A review of Intrusion Detection with Reference to Modbus Protocol

[1] Ruhi Belgudri, [2] Dr.Y. M. Patil
Department of Electronics and Telecommunication,
KIT's College of Engineering, Kolhapur, Gokul –Shirgaon
Shivaji University, Maharashtra, India

Abstract— **An intrusion detection system is a tool that monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. Snort is IDS which allows pattern search. The present paper explains the intrusion detection system rules for Modbus (RTU/ASCII) protocol.**

Index Terms— **Intrusion detection system, MODBUS, SCADA, control systems.**

I. INTRODUCTION

The collection of tools designed to protect data and to thwart hackers is called computer security. The major requirements for security services are confidentiality, authentication, non repudiation and integrity. In many cases successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism. Having designed various security mechanisms, it is necessary to decide where to physically place it and at what layer or layers of architecture mechanisms.

II. Literature Review

North American Electric reliability Corporation Standard CIP-005-4a – Cyber Security – Electronic Security perimeter(s) defines the requirements, measures and compliance [3].

1) Requirements:

a) The responsible entity should - identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
b) Implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electric Security Perimeter(s).
c) Implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electric Security Perimeter(s).
d) Review, update and maintain all documentation to support compliance.

2) Measures:

a) The Responsible Entity shall make available - documentation about the Electronic Security Perimeter.
b) Documentation of the electronic access controls to the Electronic Security Perimeter (s).
c) Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter (s).
d) Documentation of its annual vulnerability assessment.
e) Access logs and documentation of review, changes and log retention.

3) Compliance: Includes

a) Compliance monitoring process
- Compliance enforcement authority.
- The RE shall serve as the CEA.
- Compliance monitoring and enforcement process.
- Data retention.

b) Violation security levels.

According to O'Murchu, L. Last-minute paper [4], "An in depth look into Stuxnet", explains that stuxnet is a worm that not only include malicious STL (Statement List) code PLC rootkit hiding the STL code. Stuxnet targets specific type of PLC and searches for a specific configuration. Stuxnet's versions intercept, reads and writes to the PLC and changes the code. It steals certificates from other unrelated third party companies and signs the files. It has the ability to copy and execute itself on remote computers through network shares.

As explained by Caswell, B. Bealeand, J., Foster, J. and Faircloth, J. In "Snort2.0 Intrusion Detection," [7] Snort is an IDS. In Snort, header and its options form the parts of signature. The signature based IDS operate by searching for a known identity or signature for each specific intrusion event. Snort is a signature based IDS. Similar to sniffers snort analyses all the network traffic looking for any type of intrusion.

This paper presents an extension of Snort IDS by adding a new pre-processor. Thus snort turns out into hybrid system i.e. H-snort. It meets the following requirements.

- It models the network traffic at higher level.
- It stores the information in a database to model the normal behavior of the system.
- It is totally configurable and allows adjusting the sensitivity of the system to prevent false alarms.
- It has two operation phases: training and anomaly detection.
- It is complimented with a website that allows the user to administrate and observe the network performance.

Quickdraw is a snort pre-processor. It is an application that extends snort IDS [8]. It detects security events that should be logged, extract the log event parameters, create the log event, and send the log event to a historian, security event manager or other log aggregation system. Quickdraw was developed for the protocols that use query response mode to monitor and control the process for example modbus, DNP3, Ether/IP communication standards.

According to "An intrusion detection system for wireless process control systems"[10] written by Roosta, T. Nilsson, D., Lindqvist, U. Valdes, A. , the use of wireless sensors have increased in the process control systems (PSC). This paper explains the design of a model based intrusion detection system for sensor networks used for PSC. To detect unknown attacks model based intrusion detection system can prove useful. The authors have presented design of a distributed, multi layer, model based intrusion detection system for process control systems combining legacy control components with emerging sensor network technology. Such systems use wireless sensor networks which is cost effective and reliable. This paper has focused on the problem of intrusion detection and proposed a multi layer model-based intrusion detection system for SCADA applications. They propose that combining distributed and central IDS agents, anomalies in the sensor nodes can be detected.

In "Communication Pattern Anomaly Detection in Process Control Systems"[9] written by Cheung, S., Valdes, A. Present learning based approach for detecting anomalous network traffic patterns. The intrusion detection approach used today typically uses attack signatures to detect known, specific attacks. Learning based approach involves passively monitoring network traffic and learning network communication patterns. Thus network traffic information like connection endpoints, the rate of packet flow between endpoints and the set of hosts can be known. IDS maintain a database of recent and history of data traffic and keep updating it. The data flow patterns can then be evaluated by comparing with the previous learned historical norms. This paper evaluates two anomaly detection techniques, namely pattern based detection for communication patterns among hosts and flow based detection for traffic patterns for individual flows.

According to "A Retrofit Network Intrusion Detection System for Modbus RTU/ASCII Industrial Control Systems" written by Morris, T., Vaughn, R., Dandass, Y [1] there are four classes of intrusion vulnerabilities such as denial of service, command injection, response injection and system reconnaissance. Snort rules can be used to detect and prevent such intrusions. Denial of Service (DOS) attacks attempt to break the communication link between the remote terminal and master terminal or human machine interface. This breaks the feedback control loop and makes process control impossible.

Response injection attacks inject false responses into a control system. The control systems rely on feedback control loops which monitor physical process data before making control decisions. Command injection attacks inject false control and configuration commands into a control system. Reconnaissance attacks allow cyber attackers to reconnoitre a system before attacking.

The author further explains that, MODBUS RTU/ASCII Snort is a retrofit device intended to add Snort intrusion detection and prevention capabilities to previously installed MODBUS RTU/ASCII control systems. Snort can be run in two modes; passive or inline mode. MODBUS RTU/ASCII Snort can be placed in multiple locations within the control system network. According to the author, one Snort host between the HMI and MTU and one Snort host between the MTU and radio link provide the most intrusion detection or prevention coverage.

The paper, "On SCADA Control System Command and Response Injection and Intrusion Detection written by, Gao, W., Morris, T., Reaves, B., Richey, D. explains intrusion detection system [6]. SCADA process control systems are typically isolated from the internet via firewalls. The authors have developed a set of command injection, data injection, and denial of service attacks which leverage the lack of authentication in many common control system communication protocols including MODBUS, DNP3, and EtherNETIIP.

Response injection attacks inject false responses into a control system. Since control systems rely on feedback control loops which monitor physical process data before making control decisions protecting the integrity of the sensor measurements from the physical process is critical. False response injection can be used by hackers to cause control algorithms to make misinformed decisions.

Command injection attacks inject false control commands into a control system. Hackers can use command injection attacks to overwrite RTU programming and remote terminal register settings. Denial of Service (DOS) attacks disrupt the communication link between the remote terminal and master terminal or HMI.

In this paper the authors used the captured exploit network traffic in combination with captured traffic from the SCADA control systems running normally to train and validate a neural network based intrusion detection system which leverages knowledge of the physical properties of the controlled system to detect false response injection attacks.

According to, "A Memory-Efficient Parallel String Matching Architecture for High-Speed Intrusion Detection" written by, Hongbin Lu, , Kai Zheng, , Bin Liu, , Xin Zhang, and Yunhao Liu[11]. The ability to inspect both packet headers and payloads to identify attack signatures makes network intrusion detection system (NIDS) a promising approach to protect Internet systems. Most of the known attacks can be represented with strings or combinations of multiple substrings; therefore string matching can be used to detect attacks.

Firewalls performs packet filtering on packet headers only and fail to identify attacks that use unsuspicious headers. The network intrusion detection system (NIDS) is able to discover whether hackers or crackers are attempting to break in or launch a denial of service (DOS) attack by inspecting both packet headers and payloads to identify attack signatures. Most of the known attacks can be identified using string matching represented by string or multiple combinations of strings. NIDS needs to scan both the headers and the payloads of each incoming packet for thousands of suspicious strings. The attackers can easily overload the string-matching operations with knowledge of the rule set. The authors propose a memory efficient multiple-character-approaching scheme consisting of multiple parallel deterministic finite automata (DFAs), called transition-distributed parallel DFAs (TDP-DFA).

According to, "A Transfer Function based Intrusion Detection System for SCADA Systems" by, Stephen Papa, William Casper, Lockheed Martin, Suku Nair[2]. Most SCADA and industrial control systems have a limited and deterministic set of behaviors that result with a relatively small amount of variability during normal system operation. To cause system failures, an attacker may modify automatic controller commands, operator commands and sensor measurement data within the system. The authors have proposed a Transfer Function based Intrusion Detection System (TFIDS) to detect these intrusions. Normal operational behaviors can be modeled and integrated into the TFIDS with alarm filtering and reporting rules. Trust anchors within the system are required to collect some of the signals, ensure the signal integrity when delivered to the TFIDS, and to host the TFIDS if physical attacks are a concern.

By providing malicious control commands, malicious maintenance commands, performing a playback, or by performing a man-in the- middle (MITM) attack, an attacker can modify the systems operation. To detect MITM attacks or other attacks that modify normal system operation of SCADA systems this paper proposes the use of a Transfer Function based Intrusion Detection System (TFIDS). For this paper a transfer function is a model that is based on a known relationship between a set of input signals and one or more output signals. One or more transfer function models within the TFIDS are each designed to process a set of signals to create estimates of signals for comparison purposes. Creation of the transfer function models can be based on design knowledge of the control system, or by modeling the system based on data collected during its operation when attacks are not present.

In "Intrusion Detection in SCADA Networks"[7], the authors Rafael Ramos Regis Barbosa and Aiko Pras, focus on the development of a novel flow-based intrusion detection system. Based on the assumption that SCADA networks are well-behaved, the authors believe that it is possible to model the normal traffic by establishing relations between network flows.

Many of modern SCADA networks are connected to both the company's corporate network and the Internet. The HMI is a commodity PC. This paper describes the research proposal to address the problem of intrusion detection in SCADA networks. Based on the assumption that the traffic in these networks is well-behaved, the authors plan to build models for the network traffic based on relations between network flows, and detect attacks as violations of these models.

III. ACKNOWLEDGMENT

I take this opportunity to express our sincere and deep regards to our guide Dr. Y. M. Patil Sir for his constant guidance and encouragement. I am grateful for his cooperation. I would like to thank all our concerned lecturers and friends who supported and helped us.

REFERENCES

[1] Morris, T., Vaughn, R., Dandass, Y. A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems. Proceedings of the 45th IEEE Hawaii International Conference on System Sciences (HICSS – 45). January 4-7, 2012. Grand Wailea, Maui.

[2] A Transfer Function based Intrusion Detection System for SCADA Systems Stephen Papa, William Casper, Suku Nair Lockheed Martin Aeronautics, Fort Worth Texas & Southern Methodist University, Dallas Texas, 2012 IEEE

[3] North American Electric Reliability Corporation. Standard CIP–005–4a - Cyber Security – Electronic Security Perimeter(s). January 2011.http://www.nerc.com/files/CIP-005-4a.pdf

[4] O'Murchu, L. Last-minute paper: An indepth look into Stuxnet. The 20th Virus Bulletin International Conference. September 29 – October 1, 2010, Vancouver, BC, Canada.

[5] Falliere, N., Murchu, L., Chien, E., W32.Stuxnet Dossier, Version 1.3. Symantec Security Repsonse. November 2010.

[6] Gao, W., Morris, T., Reaves, B., Richey, D. On SCADA Control System Command and Response Injection and Intrusion Detection, in the Proceedings of 2010 IEEE eCrime Researchers Summit. Dallas, TX. Oct 18-20, 2010.

[7] Intrusion Detection in SCADA Networks Rafael Ramos Regis Barbosa and Aiko Pras University of Twente Design and Analysis of Communication Systems (DACS) Enschede, The Netherlands, 2010
[8] Peterson, D. "Quickdraw: Generating Security Log Events for Legacy SCADA and Control System Devices," Conference for Homeland Security, 2009. CATCH '09. Cybersecurity Applications & Technology, pp.227-229, 3-4 March 2009
[9] Cheung, S., Valdes, A. Communication Pattern Anomaly Detection in Process Control Systems. IEEE International Conference on Technologies for Homel and Security. Waltham, MA. May 11-12, 2009.
[10] Roosta, T. Nilsson, D., Lindqvist, U. Valdes, A. An intrusion detection system for wireless process control systems. 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp866-872, Atlanta, GA, 2008.
[11] A Memory-Efficient Parallel String Matching Architecture for High-Speed Intrusion Detection Hongbin Lu,Kai Zheng, Bin Liu, Xin Zhang, and Yunhao Liu, OCTOBER 2006.