International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Monitoring and Detecting Security Attacks in Industrial Automation and Control System

Bhagyashri Sangewar, Bimal Shah and Dr. A. R. Buchade

Department of Computer Engineering PICT, Pune

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Industrial Automation and Control Systems (IACS) required to facilitate the safer means of information communication between smart devices such as various Intelligent Electronic Devices (IEDs). Security in Industrial Automation and Control Systems (IACS) is critical task as many of these devices are present in remote location and controlling critical plant processes. These IEDs and SCADA or other hosts uses various protocols such as Modbus, DNP3 etc. Here focus of work is to detect security attacks on IACS products. Protocols such as Modbus or basic DNP3 does not provide any security features. These creates opportunity for attacker to attack IACS devices using man in the middle, packet modification, eavesdropping types of attacks. Attack on any device is possible due to vulnerabilities in device itself or kind of protocols used. It is important to understand such communication protocols so that we can understand how attacker can affect communication mechanism to attack the device. Here as a reference we have considered Distributed network protocol version 3 (DNP3) which is nonproprietary protocol used in Supervisory Control and Data Acquisition (SCADA) system. DNP3-SA provides authentication mechanism which ensures the integrity and confidentiality between communicating devices. However, it may need to detect attacks if attacker can breach the defense mechanism of the protocol. The purpose of this project to detect attacks. This can be done by monitoring network packet of given protocol (which is DNP3 in this case) as well as by monitoring various system information. Network packets can help us to prevent the attacks while system information can be utilized to identify attack as soon as attack has taken place.

Keywords: *Industrial Automation and Control Systems, SCADA, DNP3 protocol, Secure authentication, Security*

Introduction

Disrupting services in critical infrastructures is a very important issue to consider. As disruption, either minor or major, deliberately or mistakenly caused to these infrastructures can lead to damaging highly sophisticated devices, degrade system performances and causes substantial economic losses. In addition, it could pose as life threatening situations to the society. Unfortunately, this situation has now become the target area for many malicious attackers.

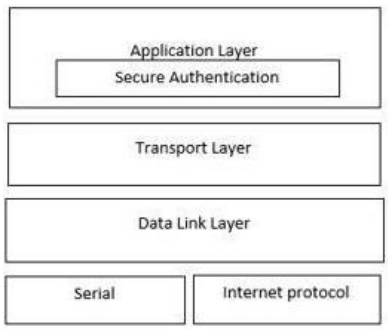

Fig.1DNP3 Layer Architecture

The products which are being used in Industrial Automation and Control Systems are vulnerable to various security attacks. In such situations monitoring the device as well network behavior will help in identifying most of the critical situations. DNP3 (Distributed Network Protocol) is a set of communication protocols used between components in process automation systems. It is primarily used for communications between a master station and IEDs (Intelligent Electronic Device). DNP3 protocol has three layers which includes data link, transport and application layer. DNP3 can be used over a variety of physical media, including serial links and IP networks. However, DNP3 is typically used with IP networks. In the network most of the attacks are possible on IP networks therefore, considering network monitoring plays and important role for security of the system.

Motivation

Initially security was not concern as Many SCADA based systems in today's operation were deployed decades ago with availability and personal safety as the

primary concerns. SCADA systems initially depended on proprietary elements but nowadays, Open communication protocol are being used in SCADA systems as well as other IACS products. The technical details of such protocols are easily accessible to everyone. Many IACS products are connected to Internet. With the acceptance of Internet into the SCADA networks the IACS products are now interconnected to achieve efficient information but vulnerable to malicious intent of attackers. Teams of sophisticated hackers are also employed by criminal organizations or terrorists to break into these systems.

Need

Cyber security is a dynamic in nature. A goal of security is to enhance the ability of systems to operate correctly, even in the presence of unexpected conditions or when subject to deliberate attempts to interfere with that correct operation. There are many different techniques that enhance cyber security and various techniques can often be used in combi-nation to provide resilience against specific sets of potential problems or vulnerabilities. Over time, new security threats will be discovered, and new methods devised to compromise existing techniques. New problems will appear that has not been previously imagined. As new techniques are developed that expose or exploit security flaws, new measures need to be developed to address those changes and maintain system security. Even if attacker is successful, system should alert user on priority that attack has taken.

Review of Literature

Y. Xu et.al [1] studied and analyzed various communication protocols such as DNP3, Modbus, IEC 60870-5-104, IEC 61850, IEC 61400-25 as well as IEEE C37.118. They have also given attacks possible on these protocols and its mitigation techniques. Most of these protocol lacks any of the authentication, authorization, encryption, availability, integrity, confidentiality. Due to lack of network security features man-in-the-middle, Denial of service, replay, injection, spoofing, eavesdropping and modification all these attacks are possible on the protocol. They have provided the solutions such as risk assessment, encryption, authentication and intrusion detection techniques.

Ihab Darwish et.al [2] highlights different security threats and vulnerabilities that is being challenged in smart-grid utilizing Distributed Network Protocol (DNP3) as a real time communication protocol. Two attack scenarios have been demonstrated:1. unsolicited message attack 2. Data set injection. The experimentation was done in DETER testbed platform. Intrusion detection system is used to identify the attackers targeting different parts of the system. mitigation techniques are also proposed. and they have used host-based intrusion detection agent at each Intelligent Electronic Device (IED) for the purpose of detecting the intrusion and mitigating it.

Ihab Darwish et.al [3] have created an attack detection model using the Round-Trip Time Delay (RTTD) for DNP3 transactions. They have used host-based intrusion detection technique and Naïve Bayes estimator was used to categorize network traffic by application. Likelihood distribution for both legitimate and hacked transactions are modeled using Bayesian analysis. Maximum A Posterior probability (MAP) and the loss functions are used to optimize threshold for improved attack detection accuracy. They measure the average

"Round Trip Time Delay" (RTTD) for each DNP3 transaction (Request and Response packet exchange). Then they performed a dynamic adjustment to the maximum allowed timeout by adding the safety margin "m" to the average round trip time delay RTTD.

Determination of "m" is decided experimentally in the DNP3 testbed environment during the normal DNP3 transactions and after initiating the attack. Using the retransmission strategy is their second approach in the mitigation process.

Raphael Amoah et.al [4] presents DNP3 Secure Authentication for Broadcast (DNP3-SAB), a new lightweight security scheme for broadcast mode communication. In DNP3 protocol standard broadcast scheme is proposed but they have not mentioned its security. In this paper DNP3 Secure Authentication for Broadcast (DNP3-SAB) which is a new lightweight security scheme for broadcast mode communication was proposed. The proposed scheme is modeled, validated, and varied using colored Petri Nets against the most common protocol attacks such as modification, injection, and replay. The proposed SAB uses a hash chain to solve the problem of key management. Hash values used for messages are linked together as a hash chain. The usage of a single key together with the hash chain removes need for a key per message.

Ihab Darwish et.al [5] analyzes vulnerabilities and performing penetration testing using man-in-the-middle (MITM) attacks to identify possible threats associated with smart grid. They have used game theory for theoretical modeling. The paper can analyze the outcomes of MITM for DNP3 environment. They have given pass and drop mitigation technique to reduce the impact of MITM attacks along with the selection of retransmission timer.

Jeyasingam Nivethan et.al [6] proposed the Linux based firewall for DNP3 protocol. They have added the fileting rules which are used to identify the common attacks on DNP3 protocol. The testing is done at scaled down electric power station between DNP3 master and DNP3 slave. They use the iptables open source firewall facility. The experimental results show that the proposed approach succeeded in blocking most of the DNP3 attack traffic.

Jin Bai, Salim Hariri et.al [7] find out the fact that security was not the goal while designing DNP3

protocol so attacker can easily target the device which is part of critical infrastructure. They have proposed the automatic network protection framework to detect the attacks on DNP3 over TCP/IP. They have focused on ruled based anomaly intrusion detection. The testing result shows that the system has high positive rates and very low false positive rates. As well as for testing they have used both offline and online testing.

Proposed Methodology

This project work aims to detect possible or actual attacks. The network activities can be monitored such as connections from unusual locations at unusual time, or unexpected communication sequences, monitoring certain function codes or monitoring certain fields in DNP3 headers. System information can include few parameters such as unusually slow system performance, system crashes or reboots, abnormal system performance or getting memory filled etc. While system learns from network monitoring as well as system monitoring, there will be higher chances of detection of attacks.

Network monitoring will be done by following way:
Capturing Module: This module will capture the network packets from the network using scapy python library. The packet capturing is done in live mode so that real time monitoring will be achieved. **Parsing Module:** This module will monitor the captured packets and analyze different parameters of DNP3 protocol. DNP3 protocol packet is decoded in thi s module.
Feature Selection Module: This module will extract the meaningful features which plays an important role in identifying normal packet and malicious packet and the parameters which are redundant in this process are discarded.

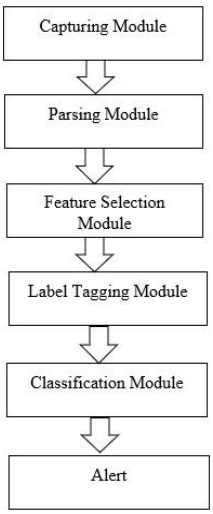

Fig. 2. Network Monitoring

Label Tagging Module: The label tagging module will add label to each packet as malicious packet or normal packet so that the algorithm will learn from the pattern of the packets and will help in taking decision in future. This module will add the automatic labels to packets based on predefined rules.
Classification Module: This module will classify the live packets as normal or malicious based on past learning and give an alert if certain suspicious condition occurs.

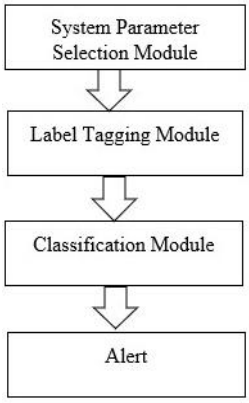

Fig. 3. System Monitoring

System monitoring will be done in following way:
System Parameter Selection Module: This module will extract the different system parameters such as system log, task history, CPU percentage and memory usage. The collected information will be stored for further analysis which plays an important role in identifying normal and abnormal system behavior and the parameters which are redundant in this process are discarded.
Label Tagging Module: The label tagging module will add label to combination of system parameters as normal or abnormal. These labels will help in taking decision in future. Automatic Label tagging will be done based on the rule set.

Classification Module: This module will continuous look for the system parameters and if any suspicious condition occurs then gives and alert.
In this way in order to determine if an attacker has violated your system or network the normal system as well as network behavior needs to be understood. The protocol which is being used for the communication between the Industrial Automation and Control System devices also needs to be analyze for further improving the accuracy of monitoring mechanism. From both system and network monitoring the alert will be generated which inform the system administrator about possible suspicious activity.

Results

Table 1. Attacks and Mitigation Techniques

Attacks	Mitigation Techniques
1. DFC (data flow control) bit	If DFC flag is set to 1 then outstation event buffer needs to check to identify whether it is full or not.
2. Unsolicited response disables	The master can stop the outstation from sending unsolicited response. The requested device history needs to check.

The above table highlights some of the possible attacks on DNP3 and how they can be mitigated.

DFC (data flow control) bit: If DFC bit set to 1 in response indicates event buffer of outstation is full. Attacker can set this bit to 1 to tell master that device is not able to process the request. That way master will not send further request to this device if continuously gets DFC= 1 in response. In that case from master side the communication pattern between the two devices needs to check to analyze how frequently the outstation device set this bit to 1 and if deviation occur between the communication pattern then it can be considered as attack. In case of outstation device if the response of DFC is set to 1 then system parameters of that device need to check to identify what causes this event buffer full condition.

Unsolicited Response Disable: In this case master device has permission to stop unsolicited responses from outstation device. If attacker maliciously send 0x21(disable unsolicited) function request in the request message, master will never receive any unsolicited response from that device in future. To avoid such attack authenticity as well as requesting device history needs to check which helps in identifying whether master had stop unsolicited response in past or not. Master device also check the pattern of the unsolicited responses of outstation device and if master has not received any unsolicited response in maximum amount of time as expected and if master has not sent any request to disable unsolicited response then attack might be taken place.

Conclusion

It is very difficult to monitor the system at remote location due to its critical infrastructure. Any kind of security attack on these devices can lead to loss of data that should not be compromised and some cases causes the system to malfunction and affect the overall plant. The monitoring system provided by this project will give the alert for suspicious activity by monitoring both system and network parameters. By focusing on both system and network activities and analyzing pattern we will be able to provide high correct detection rate and very low false positive rate.

Acknowledgment

I would like to thank my project mentor at Emerson Automation Solution Bimal Shah, Pravin Gopale, Aditya Singh and my guide Dr. A. R. Buchade for their inspiration, priceless suggestions and support for this project. I wish to express my thanks to Prof. M. S. Takalikar, HOD Computer Department, PICT, for encouragement and providing the best facilities. I thank all the people who are directly or indirectly involved in this project.

References

[1]. Y. Xu , Y. Yang , T. Li , J. Ju , "Review on cyber vulnerabilities of communication protocols in industrial control systems ", 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), 2017.

[2]. I. Darwish,O. Igbe,T. Celebi,"Smart Grid DNP3 Vulnerability Analysis and Experimentation", IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2005.

[3]. I. Darwish, T. Saadawi, "Attack Detection and Mitigation Techniques in Industrial Control System -Smart Grid DNP3", International Conference on Data Intelligence and Security, 2018.

[4]. R. Amoah, S. Camtepe, and E. Foo, "Securing DNP3 Broadcast Communications in SCADA Systems" IEEE Transactions on Industrial Informatics, Vol. 12, No. 4, August 2016.

[5]. I. Darwish, O. Igbe,T. Saadawi, "Experimental and Theoretical Modeling of DNP3 Attacks in Smart Grids", IEEE sarnoff symposium, September 2015.

[6]. J. Nivethan, M. Papa, "A Linux-based firewall for the DNP3 protocol",IEEE Symposium on Technologies for Homeland Security, 2016.

[7]. J. Bai, S. Hariri, Y. Al-Nashif, "A Network Protection Framework for DNP3 Over TCP/IP Protocol", IEEE/ACS 11th International Conference on Computer Systems and Applications, 2014.

[8]. E. Thibodeau,G. Gilchrist,P.Eng., "Introducing Secure Authentication Version 5 for DNP3", 2012 CIGR´E Canada Conference Hilton Montreal Bonaventure, September 24-26, 2012.

[9]. DNP Users Group. "Distributed Network Protocol (DNP3)" (DNP3-2012, 2012, 839 pages) IEEE Standard for Electric Power Systems Communications-

[10]. Distributed Network Protocol (DNP3). 2012. doi:10.1109/IEEESTD.2012.6327578 ISBN 978-0-7381-7292-7.