ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

A Survey on Industrial Control System attacks and preventive measures

Amrutha Mohandas[1], Chinju K[2]

M. Tech Student, School of Computer Sciences, Mahatma Gandhi University, Kerala, India[1]

Assistant Professor, School of Computer Sciences, Mahatma Gandhi University, Kerala, India[2]

ABSTRACT: During the past decade, amazing technological advancement and automation were come in Industrial Control System, which brought greater interconnections of the control components. The increased exchange of information through these has created Cyber-Security vulnerabilities such as entry points for hackers. The Modbus TCP like modern control communication systems are based on open standards that influence Ethernet to allow interoperability between solutions from different vendors. The system using Modbus TCP do not have a defensive architecture, which can be corrected using a proper preventive mechanism.

KEYWORDS:ICS, Modbus, Snort, Tofino

I. INTRODUCTION

Now a days in industries computerized process control systems are applied in diverse range in order to improving productivity, product quality, and efficiency of a production line which also help reduce energy consumption directly or indirectly. The co-operate networks in these industries do not address the attacks, especially on process control networks due to the use of traditional information and communication technology and security techniques which is effective for vulnerabilities. This is mainly because of the communication protocols used in the control networks.

The surveys are showing that the industrial control attacks are increasing tremendously. According to IBM Managed Security Services (MSS) data Fig.1, the attacks targeting industrial control systems (ICS) are increased above 110 percent in 2016 over last year's, as of Nov. 30.[1]

In March 2016, the U.S. Justice Department claimed that Bowman Avenue Dam in Rye Brook, NY is attacked Iranian hackers. The attackers compromised the dam's command-and-control (C&C) system in 2013 using a cellular modem.[1]

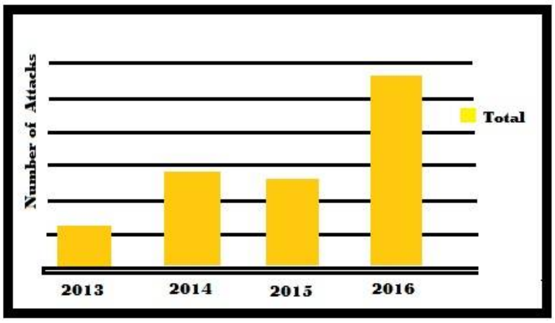

Fig.1 : Industrial Control System Attacks

A recent attack on Ukraine Power Grid happened in December 2015 is more alarming because the impact of the attack was bigger and wider. It is recognized as the first blackout caused by a malicious hack which affected 225,000 customers. [1]

Copyright to IJIRCCE
DOI: 10.15680/IJIRCCE.2018. 0609012

If a hacker can collect the login credentials of the communication network server, he can possibly gain access to the controller and then can make whatever change in the software code of the controller. Any modification to the software or firmware may have major impacts for the application which the actuator is assigned.

In case of a circuit breaker (CB) control in a substation, the hack into a controller and malfunction of a CB would cause not only a direct effect for the customers connected to the substation but also its impact will spread to other substations connected in the nation's power grid as the load of the particular substation would have to be redistributed amongst the substations. This possibility recalls the Federal Energy Regulatory Commission's finding that the U. S. could suffer a coast-to-coast blackout if just 9 out of the country's 55,000 transmission substations are knocked out on a scorching summer day [2].

The present detection and prevention measures are not effective in dealing with unknown malwares and attack vectors; therefore, a new approach for cyber-resiliency is required to secure Industrial Control Systems without fail under compromised situations.

II. Literature Survey

Charles Kim *et al.*[2] developed a representative model of the industrial control system architecture which is cyber insensitive, and in the concept of software and hardware redundancy and diversity and of utilization of unidirectional network connection, along with control data bus activity monitoring. The important and distinct advantage of this architecture includes preservation of the integrity of alerting and prohibition of communication related intrusions such as Denial of Service (DoS) attacks. Also this architecture includes the bus monitoring feature which is added to the supervisor to detect abnormal activities on the control bus.

James M. Taylor*et al.* [12] focuses on how the legacy protocol vulnerabilities can negatively affect the security of control system.For this discussion, the gave attention on the Modbus TCP/IP implementation that leverages the ubiquitous TCP/IP (Ethernet) to connect with and control end devices or remote terminal units (RTU) that control physical processes. It also focuses on the man in middle attack which affecting Modbus protocol.

PritikaMehra*et al.*[13] focuses on the comparison of open source network intrusion softwares such as SNORT and BRO.It reaches the conclusion that Snort is one of the best known lightweight IDS. Snort can easily be deployed on any node of a network, with minimal disruption to operations.

III. Communication Protocols Used In Industrial Control Systems

The given below table includes some of the communication protocols that is most widely used in the Industrial Control Systems .These protocols will be considered with no distinctions being made with the sectors in which individual protocols are most predominant [3].

Protocol	Encryption	Authentication	Main Vulnerabilities
CIP	No	No	identity theft , traffic capture, injection of malicious traffic and to manipulate the transmission route
Modbus	No	No	denial of service attack, Man in middle attack, brute force attack
DNP3	Only secure DNP	Only secure DNP	Passive-network reconnaissance, man in middle, clear object attack

Profibus	No	No	denial of service, susceptible to nearly any type of Ethernet based attack
Profinet	No	No	susceptible to Ethernet and IP vulnerabilities
Power Link Ethernet	No	No	denial of service (DoS)

Among these protocols Modbus is the oldest industrial control protocols introduce in 1979 by the company Modicon [4]. It is uses serial communication to interact with programmable logic controllers. Substantial growth of Modbus has occurred in the 1990s with the aim of achieving greater incorporation with modern systems. For this a version for TCP/IP networks named Modbus/TCP, appeared in 1999. This step has made Modbus as one of the most extensively used protocols in industrial control system [5].

Modbus has become a de facto due to the simplicity and robustness it have [6]. Modbus doesn't include any security mechanism as it was designed to be used in highly controlled environments. Therefore, it lacks authentication .All that is necessary for the Modbus session is an address and function code that are valid. Using a network sniffer, this is information can easily be obtained over the Internet. Equally, Modbus does not allow encryption of information [5]. Hence, Modbus nether encrypts traffic nor verifies the integrity of the messages or authenticates master and slave devices [2]. The injection of malicious code into these elements like remote terminal units (RTUs) or PLCs is possible because Modbus is designed for programming these control elements. Even though Modbus control networks are still being used in the process control systems [3].

IV. Preventive Measures For Vulnerability In Modbus

An IDS (Intrusion Detection System) evaluates each and every packet against known attacks by monitoring the traffic flow across the networks and creates alerts based on those results. It identify intrusions and configuration errors harmfully affecting the network, including malware and virus infection, hackers penetrating into the system security, and employees violating access policy or accidental leaking of information. An IPS (Intrusion Prevention System) executes real-time responses to detect and prevent vulnerability exploit. For the unique business needs, system administrators structures rules with in the IPS. This stops immediate threats affecting by monitoring and evaluation of threats. The intruders that might go unnoticed by firewalls or anti-virus software can catch by an IPS [7]. IDS solution Snort, and the IPS Tofino TCP Enforcer LSM are highly worthwhile for improving the security in Modbus protocol [3].

A. SNORT as IDS

SNORT is created by Martin Roesch in 1998.It is a free and open source network intrusion detection system. On Internet Protocol (IP) networks Snort performs real-time traffic analysis and packet logging. It also executes protocol analysis, content searching, and content matching. For detecting probes or attack, operating system finger attempts, common gateway interface, buffer overflow, server message block probes and stealth port scan, this program can be used [8].In a network the Snort IDS can be placed before the firewall,Fig.2.

DOI: 10.15680/IJIRCCE.2018. 0609012

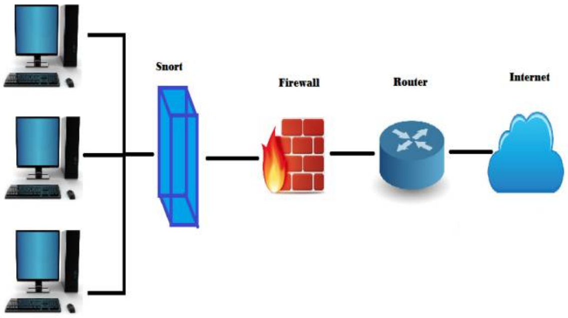

Fig.2: Intrusion Detection System Snort

It has three main mode of configuration; viz, sniffer, packet logger, and network intrusion detection. The network packets are read by sniffer mode and display them on the console in a continuous stream. The network packet to the disk is logged by packet logger mode. The network traffic is monitored by network intrusion detection mode and which analyse it against a rule set defined by the user and there perform a specific action based on what has been identified [9].

Snort can be configured on hardware platforms and operating systems like Linux, OpenBSD, FreeBSD, NetBSD, Solaris (both Sparc and i386), HP-UX, AIX, IRIX, MacOS, and Windows. Snort helps to fix a number of network problems and intrusion detections. But it cannot be used to detect intrusions on very high speed networks .Snort can easily be deployed on any node of a network, with minimal disruption to operations [8].

B. Tofino Modbus TCP Enforcer LSM as IPS

The Tofino Modbus TCP Enforcer Loadable Security Module (LSM) is acting as a content inspector for Modbus communications, which check every Modbus command and response against a list of ‘allowed’ commands defined by your control engineers. If it is not on the ‘allowed’ list, or any attempt to access a register or coil that is outside the allowed range, is blocked and reported. It makes sure that the only Modbus commands your control devices receive are approved commands from approved computers. The remote programming and corrupted messages are prevented and blocked by Tofino Modbus TCP enforcer LSM, making your control system safer and more reliable [10].

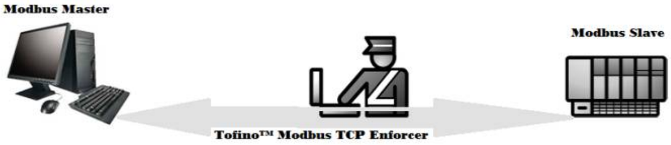

Fig.3: Tofino Modbus TCP Enforcer

Fig.3 shows the Tofino Modbus TCP Enforcer is placed between Modbus Master and Modbus Slave.All the requirements of control networks are secured by Tofino. It can be installed in front of critical PLCs, RTUs and other devices without any pre-configuration. There are no requirements to change the architecture or addressing the existing control networks. The control systems engineer can edit and test firewall rules that specify which devices in the network are allowed to communicate with each other, and what will be its protocols by using the Tofino’s central management platform softwares. Any mismatch to these rules is immediately blocked and reported to Tofino central management platform. By providing advanced security for critical Modbus devices, the optional Tofino enforcer allows to specify which Modbus function code and register address may be accessed on each protected Modbus slave. Simple editing and testing of firewall rules and Modbus traffic inception and content filtering are the main features of Tofino [11].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

V. CONCLUSION

Enhancing technological advancement in the Industrial Control Systems increases the chance of intrusion into such systems. Attacks happening in the ICS are increasing each year all over the world. These vulnerabilities occur due to the weakness of the communication protocols used for information exchange. Modbus is one of the oldest protocol which is popularly used for the communication among industrial control systems. As this protocol neither checks integrity of message nor authenticate the message or even it doesn't encrypt messages, there is a loop hole for the hackers to infiltrate into the system. An IDS like Snort or an IPS like Tofino can be supplement to the protocol as a solution for this problem.

REFERENCES

1. https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/

2. Charles Kim Electrical Engineering and Computer Science Howard University Washington DC,"Cyber-resilient industrial control system with diversified architecture and bus monitoring",IEEE, 978-1-908320-63/6/$31.00,2016.

3. Miguel HerreroCollantes and Antonio López Padilla,"Protocols and network security infrastrutures",Spanish national cyber security institute

4. MODBUS TCP/IP [available online] http://www.modbus.org/specs.php

5. James M. Taylor, Jr National Strategic Research Institute University of Nebrsaka, James M. Taylor, JrNational Strategic Research Institute University of Nebrsaka," Enhancing Integrity of Modbus TCP Through Covert Channels",IEEE,978-1-5386-2887-4/17/$31.00,2017.

6. Zakarya DRIAS Ahmed ,"Taxonomy of attacks on Industrial Control Protocols", SERHROUCHNI Olivier VOGEL in 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS).

7. https://www.rokasecurity.com/ids-vs-ips/

8. PritikaMehra Post Graduate Department of Computer Science and Applications, Khalsa College for Women, Amritsar, Punjab, India. International Journal of Advanced Research in Computer and Communication Engineering, "A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems",Vol. 1, Issue 6, August 2012.

9. SNORT Users Manual 2.9.11 ,The Snort Project ,August 31, 2017

10. https://www.tofinosecurity.com/products/Tofino-Modbus-TCP-Enforcer-LSM

11. http://www.modbus.org/viewdevice.php?id=742

12.James M. Taylor, "Enhancing Integrity Of Modbus Tcp Through Covert Channels",Jr National Strategic Research Institute University of Nebrsaka,IEEE,978-1-5386-2887-4/17/$31.00,2017 .

13.PritikaMehra,"A Brief Study And Comparison Of Snort And Bro Open Source Network Intrusion Detection Systems" International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 6, August 2012.

Copyright to IJIRCCE

DOI: 10.15680/IJIRCCE.2018. 0609012