A Review Paper on Security of Industrial Control Systems (ICS)

Dhruva Santosh

Abstract - Industrial Control Systems (ICS) are used to operate or automate industrial processes and are an integral part in the functioning of critical infrastructure. The ICSs are tailor-made to the needs of the industry that they are being used in. This research paper provides an overview of the threats and the vulnerabilities that plague Industrial Control Systems, the challenges we are currently facing in our efforts to secure these ICSs and the steps taken to mitigate the associated risks

Keywords – Authentication, Autonomous, Buffer Overflow, Distributed Control Systems (DCS), Industrial Control Systems (ICS), Legacy systems, Mitigation Operational Technology (OT), Supervisory Control and Data Acquisition (SCADA) systems, Threats, Vulnerabilities

1 INTRODUCTION

Industrial Control Systems (ICS) are used by many industries such as electric, power, natural gas, and various manufacturing industries for monitoring, controlling and automating processes. ICSs usually collect sensor data and operational data from the plant, processes them and relays control commands to the equipment either locally or remotely. Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) Systems fall under the category of Industrial Control Systems. DCSs provide control over the processing equipment locally using many autonomous controllers distributed throughout the production plant and SCADA systems control production systems that are widespread by utilizing a centralized system of computers for processing data. This centralized hub processes the sensor information and relays the control signals to the equipment using networking.

2 ARCHITECTURE OF DCS AND SCADA SYSTEMS

The architecture of Distributed Control System is a simple one. There consists of a control server on which a supervisory controller is run. This supervisory controller communicates with the sub ordinate controllers scattered throughout the processing plant. This supervisor sends control signals and requests data from the subordinate controllers. Once the sub ordinate controllers get the control signal from the supervisor, the sub ordinate controllers relay the required control signal to the equipment. These communications are usually done using a peer-to-peer network. To eliminate the need for wiring between each device and its respective controller, a local field bus is used for communicating between the controllers, actuators and sensors

SCADA systems usually consist of a central hub for communication and data processing called the Central Monitoring System (CMS). The CMS consists of a Control server and the communication router and is usually within the processing plant and in one or more Remote stations. CMS is responsible for collecting and logging information received from the plant or any of the Remote Stations and it is also responsible for generating signals for a particular action if an event is detected. The communication routers and the Control Server communicate with each other using a peer-to-peer network. The communication between the CMS and the controllers in the plant is usually done using cables or radio frequencies. In some cases where the remote site cannot be reached via a direct radio signal, a radio repeater is used to amplify the signal so that the signal can travel a greater distance and reach the remote site

3 THREATS AND VULNERABILITES IN CONTROL SYSTEMS

Traditionally Industrial Control Systems (ICS) were isolated and were used only to control and manage industrial systems. These isolated industrial management systems were called Operational Technology (OT). Due to the advancement of technologies, the Information Technologies and Operational Technologies are beginning to converge into an integrated network. While this convergence brings innumerable benefits, they also expose the OTs to several newer vulnerabilities which were not discovered earlier due to the isolation of OTs.

The most common vulnerabilities in Industrial control Systems are Buffer Overflows, Poor Authentication Protocols, Weak User Authentication, Poor Password

Policies and Improper Configuration and Patch Management.

3.1 BUFFER OVERFLOW

A Buffer Overflow is a condition where the software's code overruns the boundaries of the buffer it is meant to be stored in. This can cause the code to overwrite adjacent memory blocks resulting in unwanted code execution, file damage or information exposure. Buffer Overflow can occur due to poor input validation. It is essential for industries to check for poor input validation and perform boundary checks to mitigate risks from attacks like Buffer Overflow

3.2 POOR AUTHENTICATION PROTOCOLS

In ICSs, the most important layer of protection for communication with networks are Authentication Protocols. They are used to authenticate itself and the entity trying to establish a connection through the transfer of authentication data. Poor authentication protocols allow unauthorized devices to manipulate commands that are being sent from the ICSs which can disable a production plant resulting in a loss of revenue. Poor authentication protocols can also expose confidential information which is a very serious risk when it comes to critical infrastructure and industries like Nuclear, Natural Gas, Electric, Water, etc.

3.3 WEAK USER AUTHENTICATION

Whenever a system is accessed, the system must verify if the user trying to access the system is an authorized user. This check of user identity is called Authentication. Generally, there are two types of authentication systems namely Knowledge Based Authentication System and Identity Based Authentication System. In the Knowledge Based Authentication System, the system verifies the authenticity of the user based on something they would know like a password or a PIN. This type of authentication system is very weak as it is prone to brute force attacks and can easily be bypassed. This type of authentication can be strengthened by using more effective password policies, account lockout policies, etc.

However, in the case of Identity Based Authentication Systems, the security is extremely strong as they use biometric reading to authenticate users. Biometric data can include but are not limited to Iris Scans, Retina Scans, Fingerprint scans and Voice Recognition. This data cannot easily be imitated or bypassed and hence this type of authentication is used in high security scenarios.

Weak User Authentication can allow unauthorized users to alter or manipulate control signals that are controlled by the ICSs or steal sensitive data that are stored in the network.

3.4 POOR PASSWORD POLICIES

A password policy is a set of rules that govern how strong your passwords should be by establishing a set of rules and restrictions. A password policy might contain the minimum number of characters that must be in password or the number of days until the password expires for a new password to be set. A strong password policy is essential for any industry's security posture as weak passwords are extremely easy to crack or bypass.

3.5 IMPROPER CONFIGURATION AND PATCH MANAGEMENT

Misconfiguration of software can cause security holes in the system which can be exploited by malicious actors. The improper implementation of patch management can also result in issues with security as patches ensure that any security risks associated with the software are fixed and they also ensure that the software suns smoothly.

4 CHALLENGES IN SECURING CONTROL SYSTEMS

There are many challenges when it comes to securing Industrial control Systems but the challenges that are most prominent are Availability, Legacy Systems and Commercial off-the-shelf (COTS) products

4.1 AVAILABILITY

The systems that are governed by these ICSs typically control power, gas and other critical infrastructure. These industries need to be run 24x7 and if one of these systems goes offline, it can have a negative impact on millions of people. Updating these systems is especially hard as the organizations that support these critical infrastructures cannot allow these

systems to go offline as updating systems often causes systems to shut down or restart.

4.2 LEGACY SYSTEMS

ICSs traditionally were built to last. The systems that are running in industries are older and more vulnerable to malicious actors. It is difficult to secure older hardware and software as they were installed in the pre internet era. The older systems were not designed for connectivity and have weaker authentication protocols which have a negative impact on the security of industries

4.3 COMMERCIAL OFF-THE-SHELF (COTS) PRODUCTS

Commercial Off-The-Shelf (COTS) Products are mass produced and are made readily available to the public. They are cheaper then bespoke solutions which are tailor made to suit the needs the needs of industries. Organizations that support these industries have sought to cut costs and started using COTS products which exposes the industries to more threats associated with these COTS products

5 CONCLUSION

This study has been conducted by referring to publications from NIST and GAO. This paper presents an overview of how ICSs work and their threats and vulnerabilities and the difficulties in securing them. As the convergence of IT and OT advances, the risks involved in the security of ICSs will also significantly increase and the industries should be prepared to mitigate these risks in the future.

6 REFERENCES

[1] GAO-04-354, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, U.S. GAO, 2004, http://www.gao.gov/new.items/d04354.pdf.

[2] Falco, Joe, *et al*., IT Security for Industrial Control Systems, NIST IR 6859, 2003, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=821684

[3] Stamp, Jason, *et al*., Common Vulnerabilities in Critical Infrastructure Control Systems, Sandia National Laboratories, 2003, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.132.3264&rep=rep1&type=pdf.

[4] Stouffer, Pillitteri, *et al*., Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2, 2015, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[5] https://www.lanner-america.com/blog/5-common-vulnerabilities-industrial-control-systems/ (2017)

- *Dhruva Santosh is currently pursuing his Undergraduate Degree (B.Tech) in Computer Science and Engineering at Dayananda Sagar University (Campus 3), Bangalore, India Phone: +91 9632573311 Mail: work.dhruva16@gmail.com*