Analysis of Cyber Security incidents in Industrial Control Systems (ICS)

Kiran Kumar Mohanraj. Author, *MSc. Cybersecurity*

***Abstract*— Industrial Control Systems (ICSs) play an important role in today’s industry by providing process automation, distributed control, and process monitoring. In this paper, we provide an overview on ICS and how it differs from the traditional Information Technology (IT) systems. The threats and vulnerabilities faced by ICS is discussed along with the real-world cyber-attacks case studies. We present a classification of existing security solutions along with their strengths and weaknesses. Finally, we provide emerging technologies which can impact ICS security.**

**Keywords- Industrial Control System, Information Technology, Threat Landscape, Information Communication Technology, Risk management.**

I. INTRODUCTION

The main focus of the traditional Industrial Control Systems (ICS) is on system functions. Information and network security were not considered at the time of its design. With the development of Information and Communications Technology (ICT) and functional requirements, more ICSs have moved from an isolated network environment to a public network for enabling the remote control and supervision of infrastructures. These control systems are critical to the operation of critical infrastructures that are often highly interconnected and mutually dependent systems [1]. This paper will look into the threats faced by the cyber physical control systems, as well as the taxonomy for cybersecurity in ICS. Furthermore, the existing practices to prevent these cyber-attacks are discussed.

II. OVERVIEW ON ICS

An ICS comprises different types of controllers used to control industrial plants as well as monitor their performance in order to assure their correct operations [2]. There are several types of ICSs. The well-known ICS is Supervisory Control and Data Acquisition (SCADA) systems. SCADA is designed for data acquisition and monitoring the production system. An ICS system consists mainly of a number of devices. One of ICS devices is a supervisory computer that communicates with the field controllers, e.g., for collecting the information from each sensor and sending control commands to the controllers. Programmable Logic Controllers (PLCs) are the logic interface between the SCADA system and sensors [3]. A Human Machine Interface (HMI) provides a Graphical User Interface (GUI) that allows a system operator to interact with the controller hardware. In order to establish the connection between SCADA and PLCs, many ICS vendors have proposed specific communication protocols (such as Distributed Network Protocol (DNP3), which is widely used in electricity and wastewater treatment plants) that can be used for various ICS environments. SCADA systems use the DNP3 protocol to monitor and control the devices on site.

Furthermore, Serial Modbus uses the high-level data link control standard to create a serial communication channel for PLCs. Moreover, Modbus-TCP uses the TCP/IP protocol to transmit data between PLCs and SCADA/DCSs [4].

III. TRADITIONAL IT SYSTEMS vs CRITICAL SYSTEMS

In the early stages, ICS was similar to IT systems, where specialized hardware and software were used to run control protocols in these systems. With the advent new technologies in IT, the cybersecurity vulnerabilities and incidents increased drastically. The ICS started adopting IT solutions to incorporate remote access capabilities because of which industrial computers and networking protocols started adopting IT systems. To deal with the security challenges in an IT system, various security practices has been designed. These solutions should be treated with certain precautions when implementing it to the ICS environment. In some cases, new solutions should be created which is specific for ICS environment [2].

The critical systems differ in many instances, including the risks and priorities faced by each system. The performance and reliability requirements of ICS and the applications differ a lot from the traditional IT support personnel. The operational environment of IT systems and ICS keeps on updating.

The NIST in its guidelines on ICS provides a comparison IT systems and critical systems which is discussed below:

1. *Performance Requirements*

ICS is usually time-sensitive and requires deterministic responses. The response is critical when there is an emergency situation or a safety incident. In ICS, the access control should not intervene with the human-machine interaction. In contrast, IT systems accept some level of delay in responses but requires high throughput. For security reasons, restricted access control is implemented in IT systems [2].

1. *Availability Requirements*

Since ICS processes are continuous, the availability of these systems is high. Outage of these systems will lead to less productivity and financial losses. To overcome these issues, exhaustive pre-deployment testing is conducted. The IT systems use strategies such as rebooting a component for testing which is acceptable [2].

1. *Risk Management Requirements*

The main focus of ICS is human safety and fault tolerance. This is done to avoid loss of lives, endangerment of public health or confidence, regulatory compliance, loss of equipment and loss of intellectual property. Whereas in IT systems, confidentiality and integrity of information is the major concern [2].

1. *System Operation*

The system operations of both the systems differ drastically. In ICS, the operating systems and networks are different from an IT network and lacks security capabilities [2].

1. *Resource Constraints*

The ICS lacks resources to implement security capabilities. Implementing security capabilities in ICS will lead to unavailability issues and production delays. IT systems have a lot of computing resources which helps in providing security to organization’s sensitive information [2].

1. *Communications*

The IT systems has standard communication protocols which are mostly a wired connection and some localized wireless connection. The ICS uses field device control and intra-processor communication which are mostly proprietary [2].

IV. ANALYSIS OF THREAT LANDSCAPE IN ICS

Since the ICS are used to control critical infrastructures and the adoption of internet technologies by the ICS, security is becoming a real issue that ICS owner and vendors are facing to. To ensure the reliability and security of control operations, it is essential to understand the security objectives and requirements. The primary security objective of ICS is to protect the confidentiality, integrity and availability (CIA) of the organization’s assets. These security objectives are high level objectives to ICS. The functional and organizational requirements for protecting ICS are discussed below.

* *Network protection*

Industrial networks should perform profiling, network traffic monitoring, and attack detections. Industrial network infrastructure must be able to ensure control operations under attacks due to the criticality of the systems that they operate [3].

* *Authentication and authorization*

Authentication is the key concept for identifying systems assets, guaranteeing that they are allowed to access another resource within the system. Authorization should be

integrated to industrial control systems to prevent unauthorized users of services to access sensitive system

resources. To implement authentication and authorization, we require cryptographic functionalities [3].

* *Secure communications and protocols*

Any communication between the three levels of ICS (field, plant and control room) should be secured, by adding security by design in communication protocol such as Modbus and DNP3. ICS require much more security requirements than IT systems due to the criticality of infrastructure that deploys ICS [3].

*A. THREAT VECTORS IN ICS*

Nowadays, ICS faces increase in cyber-attacks, most of these attacks are adopted from Internet Technologies. Zhakarya [3] proposes that there are three broad types of threat against ICS security. Firstly, attack against availability, these attacks deny the access to all the components of a systems like the ICS assets; Operator workstations, Engineering stations, communications system as well as control devices. Secondly,

attacks targeting integrity, the threat actor modifies acquired messages or control commands transiting through the three system levels as well as modifying the content of databases or control programs in PLCs or RTUs. Thirdly, attacks targeting confidentiality, the aim is to acquire unauthorized data or resources in the Industrial control network. Acquired data such as passwords, PLCs configurations may be used unintentionally to replay some ICS operations [1].

The NIST in its guidelines on ICS classifies the threats into four categories.

*(i) Adversarial*

The threat sources involved in these attacks include individual, insider, established groups, organization, third-party suppliers, etc. The main intent of these threat sources is to exploit the vulnerability to access sensitive information or communications and information-handling capabilities of organization’s resources [2].

*(ii) Accidental*

The false actions taken by the user/administrator of the organization rather than the assigned activities leads to accidental threat [2].

*(iii) Structural*

The failure of hardware and software systems namely IT equipment, operating systems or even environmental controls like temperature controls, power supply will lead to structural threats [2].

*(iv) Environmental*

These are the threats caused by natural or man-made disaster like fire, flood, etc. or by unusual natural event or infrastructure failure. These threats cause failure of critical infrastructure but is outside the control of the organization [2].

*B. ICS VULNERABILITIES*

In the last two decades, ICSs have been transformed and up- graded from a proprietary and isolated architecture to an open and standard platform, which is highly interconnected with the corporate and public networks. This development has opened up new opportunities (such as remote access to networks and ICS devices) but it has also made ICSs vulnerable to a wide range of cyber-attacks. The target of the attacks is not only security policies and procedures but also ICS hardware, software, platform, and net- work vulnerabilities. Network configuration vulnerabilities (e.g., the corporate network does not configure the access control lists properly in the firewall or sends the password in plain text) can also cause a system to be attacked and shut down. The attacks on ICS systems are not new. Looking at the report from Kaspersky, in 1997, only two vulnerabilities were published. However, this index increased to 19 in 2010. Since then, the number of vulnerabilities has significantly risen, 189 ICS vulnerabilities were found in 2015. In 2015, 50% houses in Ukraine had electricity outage because of a cyber-attack against the Prykarpattyaoblenergo power company. Another system intrusion attack was discovered in Kemuri Water company when attackers infiltrated a water utility’s control system and changed the levels of chemicals being used to treat tap water. Both incidents indicate that the intruders can find the vulnerable ICS components exposed to the Internet. As the number of ICS systems available over the Internet increases every year, it is

crucial for ICS administrators to be aware of new vulnerabilities and threats, and actively improve the security of their ICS environments based on the existing technologies [3].

The table below provides the group of vulnerabilities according to where they exist.

|  |  |
| --- | --- |
| Policy and Procedure | \* Inadequate security policy for the ICS  \* No formal ICS security training and awareness program  \* Inadequate review of the effectiveness of the ICS security controls  \* Inadequate incident detection and response plan and procedures [2] |
| Architecture and Design | \* Inadequate incorporation of security into architecture and design  \* Insecure architecture allowed to evolve  \* Control networks used for non-control traffic  \* Inadequate collection of event data history [2] |
| Configuration and Maintenance | \* Hardware, firmware, and software not under configuration management.  \* Poor remote access controls  \* Passwords generation, use, and protection not in accord with policy  \* Malware protection implemented without sufficient testing  \* Intrusion detection/prevention software not installed [2] |
| Physical | \* Unauthorized personnel have physical access to equipment  \* Unsecured physical ports  \* Lack of backup power [2] |
| Software Development | \* Inadequate authentication, privileges, and access control in software  \* Improper Data Validation [2] |
| Communication and Network | \* Firewalls nonexistent or improperly configured  \* Authentication of users, data or devices is substandard or nonexistent  \* Inadequate data protection between wireless clients and access points  \* Use of unsecure industry-wide ICS protocols [2] |

*C. CYBER INCIDENTS ON ICS*

The followings are the most sophisticated attacks on ICS:

*a) Stuxnet*

Stuxnet is a worm, which was discovered in 2010. The worm aimed to possibly disrupt Iranian nuclear installations. It was programmed to infect SCADA systems, in particular, PLCs organized in groups of 164 objects, and the cascades of the Natanz plant arranged in 164 centrifuges. The attack was conducted by an insider since the facility was using air-gapped software to carry out the production. Using the exploit of four zero-day vulnerabilities, the hackers managed to gain control of the system and to spread the malicious worm to more than 10,000 hosts [5]. The main error that was made by the management system was the lack of adequate testing of the security responses, necessary to find the flaws of the systems via simulations, considering the zero/days vulnerabilities of the Microsoft Windows operating system used to spread the virus [6].

*b) Ukrainian power grid attack*

In 2015-2016, the Ukrainian power grid was attacked. The attack was due to an intruder in the company’s computer and SCADA system. Approximately 30 substations were disconnected for three hours, causing a power outage in three of its regional electricity distribution companies, Kyivoblenergo, Prykarpattyaoblenergo, and Chernivtsioblene -rgo, cutting out of power of more than 200,000 costumers. The power outages were caused by the UPS systems of the facilities, which usually provides emergency power to a load during electric fails, that impacted instead the connected load and caused the outage. Also, a Distributed Denial of Service (DDoS) attack to the call center was done so that customers were not able to report the issue [7].

*c) WannaCry*

In 2017, the WannaCry ransomware virus was used to attack Microsoft Windows operating system which infected more than 230,000 systems in 150 countries. The UK’s National Health Service (NHS) reported that computers, MRI scanners, blood-storage refrigerators and operating room equipment may have all been impacted. Microsoft issued a patch in March 2017 that would have protected computers from the WannaCry malware [8].

V. CURRENT CYBER SECURITY APPROACHES IN ICS

Multiple security counter measures have been designed for ICS following the defense in depth concept and taking into account all ICS constraints of reliability and real time responses. Various security solution for protecting the ICS is discussed below.

*a) Standards and guidelines*

1. *NIST Guidelines*

NIST guide to industrial control systems security provides typical ICS architectures and topologies, then discuss main threats and vulnerabilities of these systems. The document provides also security countermeasures to mitigate the risk associated to the ICS vulnerabilities and threats. Authors propose a complete process to apply security in ICS starting by security policies and people awareness and following by conducting risk assessment for the ICS then apply security

controls illustrated in the document. By far NIST 800-82 was the most detailed and specific guideline to secure industrial control systems for security owners. The only limitation in the specification is the miss of design guidelines for ICS providers and vendors [2].

1. *IEC 62443*

IEC 62443 formally called ISA99 Industrial Automation and Control Systems (IACS) Security; its aim is to create guidance documents on how to apply IT security in Industrial control systems including Hardware and software systems such as SCADA, DCS, PLC, HMI, networked sensors and devices. IEC 62443 is categorized into four main requirement categories; General requirements, Policies and procedures requirements, System requirements and Component requirements [3].

*b) Intrusion Detection and Prevention systems*

Since ICS are using tailored protocols such as DNP3 and Modbus for real time and reliability purposes, the traditional IDS and IPS from the IT world don’t answer the need of malicious events monitoring in the ICS. The rules and mechanisms for ICS are mainly based on attack signatures, anomaly detection, probabilistic models, system specifications as well as the behavior of ICS components. The challenge related to the introduction of such techniques in the ICS are the difficulty of managing the distribution of IDS/IPS agents in all the system components and networks in a large-scale system without decreasing the performances of the system. The other challenge that we see in the introduction of IDS/IPS into ICS is related to post detection reaction [3].

*c) Cryptographic countermeasures*

Introduction of cryptographic algorithms in the ICS design helps in ensuring the integrity and confidentiality of data in rest and in transit, authentication of messages and non-repudiation of actions executed in the control system. The use of cryptography countermeasures in an ICS environment can be very costly in term of resources consumption. Another huge problem in the application of cryptographic techniques is the storage, distribution and renewal of cryptographic embedded in the control system components [3].

*d) Risk management*

A security risk management covers the risk of equipment failure, personal safety risk, and potential cyber-attacks. Depending on the security requirements of each company, the security department will design the appropriate procedures to analyse and evaluate the risk associated with their business. The various metrics described below can be used to evaluate cybersecurity strategies.

1. *Access control management* not only determines the

users who can access the system but also sets the level of access permission. It ensures that only authenticated users can access and use specific applications, systems, and environments

1. *Risk management* is an assessment process that can be

used to evaluate the impact of attacks. Besides, it also provides the best among many alternatives to minimise the impact of uncertain events.

1. *Security metrics* are measurable properties that

quantify the degree to which the security objectives of the system are achieved. Moreover, it analyses the relevant security attributes of ICSs [1].

VI. IMPROVEMENTS TO EXISTING CYBER SECURITY APPROACHES

Although there are various security approaches which are resistant to the attacks, organizations fail in implementing and reviewing it periodically. Employees of the organization lack knowledge in cyber security aspects. In the attacks discussed above, the attacks were initiated by the employees through phishing vector. Awareness and training on ICS based information security must be provided. This plays a major part of ICS incident response which is very effective against social engineering attacks.

The emerging technologies which can impact ICS security approaches are discussed below.

*a) Quantum Computing safe ICS design*

Quantum computing advances can impact the security of ICS, many existing encryption algorithms will become easily compromised. Systems must be designed with cryptographic agility, by increasing the cryptographic key sizes and cipher algorithms to handle the advances in quantum computing [9].

*b) Blockchain for supply chain and Identity management*

Blockchain is a new technology that has promise to solve many problems in the area of identity management. Because of its distributed nature, it can be used for enhancing supply chain security of ICS by tracking the components during transit across all supply chain phases [9].

*c) Advanced security Hardware accelerator*

Hardware based accelerators have the advantage of low power consumptions and increased security but comes with the disadvantage of difficulty in upgrading, especially if a new vulnerability is found. There is also need to look at energy-efficient cryptographic algorithms that can be run on battery-operated backed-up devices, while requiring very little maintenance [9].

*d) Advanced Security Analytics for ICS*

The complex threat landscape and attack patterns create new opportunities for research activities around real-time security analytics and advanced machine learning algorithms, that have the potential to detect newer attack patterns and anomalies with very high levels of accuracy [9].

*e) Converged Edge Computing*

There is a new line of infrastructure products/solutions, like Hewlett Packard Enterprise’s Converged Edge computing hardware that converges OT functionality with traditional IT capability. The benefit of this convergence results in greater security, higher performance and lower operating expenditure, through lower space and energy requirements [9].

VII. CONCLUSION

Over the years, cyber-attacks on ICS systems have been on the rise. Not surprisingly, ICS systems are becoming more vulnerable to security threats that compromise confidentiality, integrity, and availability of these systems. In this paper, we have provided an overview of the nature of ICS and its threat landscape. We also provide an overview of existing ICS cybersecurity approaches. Although these solutions provide best practices to improve the security quality and an effective way to measure security strategies, they have some practical challenges like resource constraints, etc. The emerging technologies which have potential to improve the security of ICS has been discussed.

VIII. REFERENCES

[1] M. R. Asghar, Q. Hu, and S. Zeadally, “Cybersecurity in industrial control systems: Issues, technologies, and challenges,” *Comput. Networks*, vol. 165, p. 106946, 2019, doi: 10.1016/j.comnet.2019.106946.

[2] K. Stouffer, J. Falco, and K. Scarfone, “GUIDE to industrial control systems (ICS) security,” *Stuxnet Comput. Worm Ind. Control Syst. Secur.*, pp. 11–158, 2011.

[3] Z. Drias, A. Serhrouchni, and O. Vogel, “Analysis of cyber security for industrial control systems,” *2015 Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. SSIC 2015 - Proc.*, 2015, doi: 10.1109/SSIC.2015.7245330.

[4] X. Fan, K. Fan, Y. Wang, and R. Zhou, “Overview of cyber-security of industrial control system,” in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, 2015, pp. 1–7, doi: 10.1109/SSIC.2015.7245324.

[5] R. Naraine, “Stuxnet attackers used 4 Windows zero-day exploits,” 2010, [Online]. Available: https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/.

[6] T. M. Chen and S. Abu-Nimeh, “Lessons from Stuxnet,” *Computer (Long. Beach. Calif).*, vol. 44, no. 4, pp. 91–93, 2011, doi: 10.1109/MC.2011.115.

[7] J. E. Sullivan and D. Kamensky, “How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid,” *Electr. J.*, vol. 30, no. 3, pp. 30–35, 2017, doi: https://doi.org/10.1016/j.tej.2017.02.006.

[8] J. M. Ehrenfeld, “WannaCry, Cybersecurity and Health Information Technology: A Time to Act,” *J. Med. Syst.*, vol. 41, no. 7, p. 10916, 2017, doi: 10.1007/s10916-017-0752-1.

[9] G. Karpagam, B. V. Kumar, J. U. Maheswari, and X.-Z. Gao, “Smart Cyber Physical Systems: Advances, Challenges and Opportunities,” *CRC Press*, 2020.