Cyber Threats and Vulnerabilities in Industrial Control System

ANKITA GUPTA
M.TECH EMBEDDED SYSTEM ELECTRONICS AND TELECOMMUNICATIONS
SYMBIOSIS INSTITUTE OF TECHNOLOGY
PUNE, INDIA
Email-ankita.gupta.mtech2023@sitpune.edu.in or ORCID-0009-0006-2973-9740

***Abstract*—Industrial control system is a system which is used in critical infrastructure framework such as highways, tunnels, railways, electric utilities, water management system, mobile networks etc. ICS is a combination of various types of control systems including instrumentation devices, network and controllers used to operate and automate industrial process. This case study is basically about the characteristics and abstract architecture of industrial control system and analyzing the cyber threats and vulnerabilities status of industrial control system. ICSs are essential to critical infrastructure operations, and their successful misuse can cause in data malfeasance and also can cause significant physical damage including the loss of human lives. Nowadays cyber threats and vulnerabilities are increasingly shifting their focus from Industrial technology to Operational technology. Therefore critical industrial infrastructure owned by the government and private entities at high risk of detrimental cyberattacks that can cause loss of life and severe economic damage as well.**

***Index Terms*—Industrial control system, Cyber threats, Vulnerability analysis, ICS Security.**

I. Introduction

Industrial control system mainly used to control large number of operations of critical infrastructures such as power supply systems, water management, oil industries, transportation, manufacturing industries and so on. Initially ICS were designed to operate with specific protocols and hardware tools, without any security requirements. Nowadays, ICS are becoming more and more interconnected with Internet of things, therefore this evolution urges raising of cyber threats and vulnerabilities risk in ICS. There are various types of ICS that targeted by threat actors to carry out cyber attacks such as:

- Supervisory Control and Data Acquisition- SCADA, is a system that processes and collect data of control system that operate higher level and for significant distances. Some applications are- Pipeline systems, Microwave transmissions.
- Distributed Control Systems- DCS, are systems of specially designed computers, controllers and sensors that are dispersed through industrial plants. Some applications are- chemical plants, nuclear power plants.
- Industrial Automation and Control Systems- IACS, are combination of electronic, mechanical and elctromechanical devices that perform various tasks like controlling, monitoring and actuation processes on logical devices. It also provide real time data. Some applications are- Autotransformers, Motor controllers.
- Programmable Logic Controllers- PLCs, are electronic devices that perform various functions like input/output control, three modes control, counting and timing mechanisms, sequential control and intutive programming interface. Some applications are- Escalator and lift operations.
- Safety Instrumented Systems- SIS, are used to perform safety functions in industries. It is hardware and software based control systems which provides protection if hazardous condition is detected.
- Remote Terminal Units- RTUs, are microprocessor based industrial control systems. These electronically connect various hardware to control systems. Some applications are- Air traffic equipments.
- Human Machine Interfaces- HMIs, are hardware and software based information transmit exchange device between human and machine or computerized systems. Some applications are- Centralized control rooms.
- Intelligent Electronic Devices- IEDs, are combination of electronic devices with microprocessors such as circuit controllers that have many functions like power monitoring, controlling and metering. Some applications are- Sewage treatment plants, Food processing industries.

A. Cyber Threats

Industrial control systems generally threaten by various cyber threat vectors such as; Bot-networks, Attackers, Criminal groups, Foreign intelligence systems, Phishers, Insiders, Spammers, Spyware, Malware, Terrorists groups and Industrial spies. These threat sources make ICS's vulnerable and exploit system completely. Any kind of attack through cyber threat vectors on ICS protocols is a part of five major threat categories -

- Spoofing- In these kind of attacks a person or program successfully steal other's data by falsifying identity.
- Data Tempering- In these kind of attacks malicious actors manipulate data by means of accessing unauthorized files.
- Disclosing data- In these kind of attacks hackers usually capable of breaching data in unauthorized fashion.
- Denial of service- In these kind of cyber attacks malicious users make device unavailable to its intended user.

- Privilege Escalation- In these kind of cyber attacks hackers gain unauthorized privileged access within system.

To give a sense of the size of these attacks, following are some of the biggest cyber attacks described as below;

- In 2010, a malware Stuxnet developed by US and Israeli Intelligence to target Iran's nuclear facility. Stuxnet successfully targeted Iranian centrifuges.
- In 2010, a malware Night dragon used to target global, oil and petrochemicals companies.
- In 2012, a malware Shamoon used to target large energy companies including Saudi Aramco and RasGas.
- In 2013, a remote access Trojan named Havex developed by Russia's civilian and military intelligence services to target targeted industrial control system; energy grids and electricity firms.
- In 2014, a trojan malware developed by a Russian-based group known as Sandworm also known as Voodoo Bear to target Ukrainian's power grid.
- In 2017, ICS malware Triton/Trisis/Hatman was discovered which targeted petrochemical facilities in the Middle East.

B. Vulnerabilities

Industrial control system consist of various devices, controllers, computers, software integration systems to communicate and operate industrial processes. These functions make ICS more vulnerable to cyber threats malware from both inside and outside the control system network. Some important vulnerabilities which are common to all ICS are given as below;

- Buffer Overflows- These are programming errors where program overruns the boundary of the buffer.
- Unauthenticated Protocols- It is used by protocols to validate connectivity between devices.
- Weak User Authentication- It is a user identifier by which user identifies itself through passwords, biometrics, fingerprints and iris scans.
- Untimely Adoption of Software- It occurs when software not tested thoroughly for all input and error conditions, can lead to exploitation of ICS and invite malicious hackers.
- Misconfigurations- Systems that have been misconfigured present major security vulnerabilities.
- Third party outsourcing- Having outside personnel accessing.
- Weak Firewall rules- These are intricate part of networks. In the case of OT networks these not configured thoroughly.
- Inadequate Hardware- Mostly companies often try to save money by purchasing inadequate hardware which leads to misconfigurations and vulnerability exploitation.
- Insider threats- These threats are mainly responsible for security breaches.
- No Working Backups- This happen when critical system has failed and there is no secure copies of backup configuration for that critical system. This security gap can exploit the system by perpetrator.

C. ICS Security

In Industrial control system most of the cyber attacks have either targeted IT infrastructure or circuit breakers of OT. Therefore ICS security is essential as the defence of industrial control system from cyber threats and attacks. ICS security is also defined as Operational Technology security or OT security. Operation Technology security includes wide range of practices to reduce ICS vulnerabilities, these are following;

- Detection of organization list and details of assets its own.
- Vulnerability management of system.
- Network disturbance protection and detection.
- Terminus detection and response.
- Patch management to protect against vulnerabilities .
- Management to access services and resources.

II. Literature Survey

Some research paper review for ICS cyber security has described below;

- Research paper [6], [9], [15], [22] have different approaches to describe the cyber malware attacking behaviors. These cyber attacks have great impact for any nation's national security and economy that can make any nation vulnerable for its citizen's security. Concentrating on ICS security, each nation should implement ICS security framework to secure ICS systems from internal and external attacks. Framework steps describes as below;

1) Procedural security control.
2) Operational security control.
3) Technological security control.
4) Physical security control.
5) Regulatory security control.
6) Compliance security control.

- Research paper [2] proposed a new model for Multi-Attribute Vulnerability Criticality Analysis, MAVCA is a probabilistic model which provides a unique way to find out the issue of uncertainty in ICS network's systems vulnerability management. It also provide methodology for security strategy to prevent cyber-attacks.
- Research paper [18] has provide a survey of RowHammer vulnerability. Failure of Dynamic Random Access Memory is called as RH. By RowHammer attack it is possible to change data of attcked hardware. RH is a first example of how mechanism of circuit failure can cause vulnerabilities in system's security.

III. Analysis

Developing countries like India where democracy play a major role is highly sensitive for any major cyber attacks. Compare to global average cyber attacks, India alone witness approximately 1700 cyber attack each week on average. India's health care sector is a prime target for cyber attackers due to intrinsic vulnerabilities. In this technological advancement era

most of the countries still not a part of global conventions or forums which make other components vulnerable to major cyber threats. Creating a global framework by organizations and spreading awareness can prevent system from any hazardous attack.

IV. Result

Before advancement of further industrial revolution some strict security policies are required for any country to protect the critical infrastructure of information as well as operational technology. For security of data and systems cyber laws should be provided. According to above case study of cyber threat in ICS following steps are required;

- Cyber security policies should be endorse by country.
- Legal laws should be reviewed periodically to protect personal data from breaching.
- Detection and protection system should be up to date.
- Automatically encryption and decryption of data whenever it is required by system.
- Identifying vulnerabilities in system and providing repairing.
- Must have a backup solution.
- Securing sensitive systems from any damage.
- Prohibition of unauthorized access.
- Regular monitoring of tasks.
- Upgradation in quality training to all staffs.

V. Conclusions

Nowadays cyber threats and vulnerabilities are prime challenges that any kind of organisations need to consider while adopting advance technologies and internet of things. Modern Industrial Control Systems are very important in our life because we use it as information and communication tools to manage, monitor and improve ICS usage. These ICS systems are commonly used in critical infrastructure, if one these systems became slow down or shut down, it would have a great impact on national economy as well as national security for any country. Some Popular ICS attack incidents, like Colonial pipeline ransomware attack, Triton malware attack, Ukraine power grid trojan attack show that the impacts of major cyber-attacks can cause considerable negative effects on other connected components of entire system. To represent the concern of advanced cyber attacks before any crucial damage is done to physical system a multi-layer, data-driven cyber-attack systems are required to improvise ICS cybersecurity by providing wider attack detection.

References

[1] Xiaohe Fan, Kefeng Fan, Yong Wang1, Ruikang Zhou, "Overview of cyber security of Industrial control system."

[2] Uchenna Daniel Ani; Hongmei He; Ashutosh Tiwari, "Vulnerability-Based Impact Criticality Estimation for Industrial Control Systems."

[3] Alfred Ocaka; Diarmuid O Briain; Steven Davy; Keara Barrett, "Cybersecurity Threats, Vulnerabilities, Mitigation Measures in Industrial Control and Automation Systems: A Technical Review."

[4] Ming Wan; Jiawei Li; Ying Liu; Jianming Zhao; Jiushuang Wang, "Characteristic insights on industrial cyber security and popular defense mechanisms."

[5] Rao Faizan Ali; Amgad Muneer; P D D. Dominic; Ebrahim A. A Ghaleb; Ammar Al-Ashmor, "Survey on Cyber Security for Industrial Control Systems."

[6] Phitaya Nakhonthai; Krishna Chimmanee, "Digital Forensic Analysis of Ransomware Attacks on Industrial Control Systems: A Case Study in Factories."

[7] Zahra Jadidi; Yi Lu, "A Threat Hunting Framework for Industrial Control Systems."

[8] Montri Wiboonrat, "Cybersecurity in Industrial Control Systems: An integration of information technology and operational technology."

[9] Usman Javed Butt; Maysam Abbod; Anzor Lors; Hamid Jahankhani; Arshad Jamal; Arvind Kumar, "Ransomware Threat and its Impact on SCADA."

[10] Beulah Rani I; G. Matthew Palmer; G. Jaspher W. Kathrine; S.E Vinodh Ewards, "Intrusion Detection System for Cyber Attacks in Food and Beverage Industry."

[11] Ercan Nurcan Ylmaz; Bünyamin Ciylan; Serkan Gönen; Erhan Sindiren; Gökçe Karacayılmaz, "Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect."

[12] Toshio Miyachi; Tsutomu Yamada, "Current issues and challenges on cyber security for industrial automation and control systems."

[13] Mohamed Mesbah; Marianne Azer, "Cyber Threats and Policies for Industrial Control Systems."

[14] Matthew G. Angle; Stuart Madnick; James L. Kirtley; Shaharyar Khan, "Identifying and Anticipating Cyberattacks That Could Cause Physical Damage to Industrial Control Systems."

[15] Omar EL Idrissi; Abdellatif Mezrioui; Abdelhamid Belmekki, "Cyber Security challenges and Issues of Industrial Control Systems–Some Security Recommendations."

[16] Maesschalck S; Staves A; Derbyshire R; Green B; Hutchison D, "Walking under the ladder logic: PLC-VBS: a PLC control logic vulnerability scanning tool."

[17] Alzahrani A; Aldhyani T, "Design of Efficient Based Artificial Intelligence Approaches for Sustainable of Cyber Security in Smart Industrial Control System."

[18] Aydin H; Sertbaş A, "Cyber Security in Industrial Control Systems (ICS): A Survey of Rowhammer Vulnerability."

[19] Eric Byres; Justin Lowe, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems."

[20] Kevin Hemsley; Ronald Fisher, "A History of Cyber Incidents and Threats Involving Industrial Control Systems."

[21] Joel F. Brenner, "Eyes wide shut: The growing threat of cyber attacks on industrial control systems."

[22] Zakarya Drias; Ahmed Serhrouchni; Olivier Vogel, "Taxonomy of attacks on industrial control protocols."

[23] Abdulrahman Al-Abassi; Hadis Karimipour; Ali Dehghantanha; Reza M. Parizi, "An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System."

[24] Chenyang Liu; Yazeed Alrowaili; Neetesh Saxena; Charalambos Konstantinou, "Cyber Risks to Critical Smart Grid Assets of Industrial Control Systems."

[25] Allan Cook; Richard Smith; Leandros Maglaras; Helge Janicke, "Measuring the Risk of Cyber Attack in Industrial Control Systems."

[26] Fan Zhang; Hansaka Angel Dias Edirisinghe Kodituwakku; J. Wesley Hines; Jamie Coble, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data."

[27] Eric Luiijf, "Threats in Industrial Control Systems."

[28] Maryna Krotofil; Dieter Gollmann, "Industrial control systems security: What is happening?"

[29] Xinxin Lou; Asmaa Tellabi, "Cybersecurity Threats, Vulnerability and Analysis in Safety Critical Industrial Control System."

[30] Nick Evancich; Jason Li, "Attacks on Industrial Control Systems."