Cyber Attacks on SCADA Systems

Shalini

Tata Advanced Systems Limited

Abstract: ***Energy networks are defined as critical infrastructures monitored and controlled by the ICS and SCADA Systems. The attacks like DOS, MITM mostly happen due to vulnerabilities of SCADA components (PLC, RTU, HMI, communication equipment) and the used protocols. This paper explains how SCADA systems can be hacked by the attacker and some Standards & Regulations to secure the system are provided.***

Keywords: Critical Infrastructures, SCADA systems, Attacks, Communication Protocols, Protection guidelines

1. Introduction

The SCADA (Supervisory Control and Data Acquisition) systems remotely monitor and control centralized data collection and transmission of information in critical infrastructures. These systems include power grids, water treatment systems, nuclear power plants, agricultural irrigation systems, gas pipelines systems, and other similar systems that are designed with redundancy and have fault-tolerance properties. But these countermeasures are not enough solutions as many small to large organizations are vulnerable to malicious attacks due to insecure communication.

2. SCADA vulnerabilities for Cyber Attacks

The purpose of the attacker can be from getting access to your system to terrorist activities who want to damage the petroleum pipeline. Vulnerabilities allow malicious actors like cybercriminals, terrorists, aggressive military groups to compromise the SCADA system (e. g., Power Plants). The attacker can perform various activities like espionage, damage to the system, session hijacking, system unavailability to authorized users or generating false alarm messages on the HMI operator screen. Some harmful attacks can seriously disable the system or can cause to damage the system by sending improper commands.

The communication between the corporate network and field network by wireless area network opens an entry point for the attacker. The attacker can take advantage of remote access with the help of TCP/IP networking and inject the worms like Stuxnet into these critical infrastructures. *Stuxnet was an extremely sophisticated, undetectable worm attack, discovered in 2010, believed to target SCADA systems for Iran's nuclear power plants. Once entered the network, it affects centrifuges (IoT devices that isolate isotopes of uranium) and reprograms it to damage or destroy controlled equipment. Recently on September 4, 2019, another malware named Dtrack was found by CERT in Indian Kudankulam Nuclear Power Plant (KKNPP) administrative network. The malware could possibly gain unauthorized privileges or sensitive information from connected networks.*

The cyber-warfare attacks like Dtrack or Stuxnet can disrupt power utilities or other remotely accessible critical infrastructure of a country and can impact negatively. So, to keep eye on these types of attacks and implementing prevention solutions are essential.

3. Attack Surface on SCADA Systems

Finding the attack surface area of SCADA systems can prevent the harmful attack on these critical infrastructures. Sometimes the sensors, equipment, and software act as an attack surface for SCADA systems.

As we know the insecure communication between the corporate network and field network is a prime attack surface. Necessary actions should be taken to protect data transmission between the control network and field site components. Applying the recommended security considerations for SCADA as well as for Internet of Things components (HMI, RTU, and PLC that might produce unwanted consequences if hacked, as happens in Stuxnet) can reduce the chances of the hack.

HMI: HMI provides the graphical user interface for SCADA for sensors and machines connected to SCADA systems. This interface can be the target for attackers to get control or steal critical data.

Vulnerable Software: The vulnerable applications used by the operator remotely to control the RTU and PLC can open paths to the attacker. The fig1 shows how the attacker gains access to SCADA equipment with the help of the operator's machine.

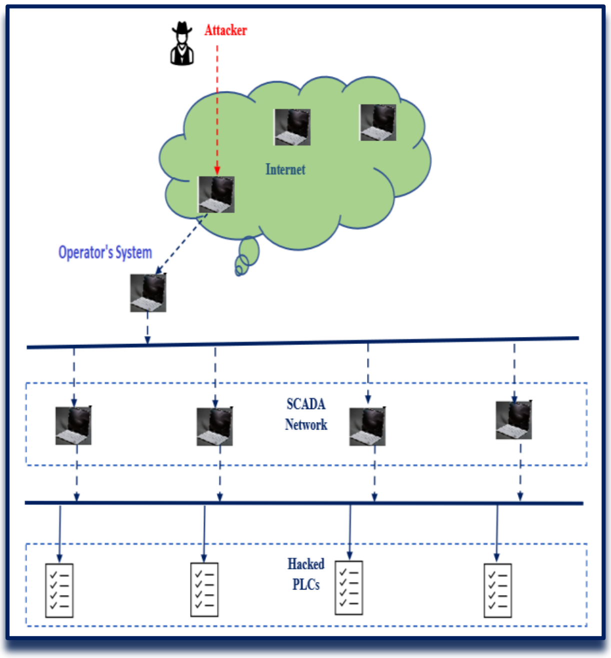

Figure 1: Hacked SCADA system

Communication Protocols: The communication protocols help to control SCADA systems. The vulnerabilities in these protocols can malfunction the SCADA system and can modify the PLC or RTU data.

Communication Equipment: the other technologies help to work SCADA system in real-time. Ill-equipped components can be an attack vector for critical infrastructures.

4. Protection of Critical Infrastructure from Cyber Attacks

Some companies in the market offer vulnerability assessment and audits of the infrastructure to discover the bugs quickly and efficiently and secure the network from hackers. They Follow the Standards and Regulations set up by the government for following for protect National Critical infrastructure. Some guidelines with solutions are given below:

- Guidelines for Security and Privacy Controls with the access control mechanism, Events Recovery, Industrial Automating& Control Systems for Industrial Control System Security Policies Planning.
- Implementation of strong network segmentation and segregation through boundary protection devices like a firewall and routers forthe boundary of different zones like control zone, and Demilitarized zoneto safeguard sensitive information from unauthorized actors. Use different infrastructure for the internal and external networks.
- Industrial Control System Security Awareness Program for Training System's Engineers, Technicians, Administrators, and Operators.
- Critical Infrastructures Interdependencies Analyzation, Protection, Penetration Testing, Incident Management, Assessing the Security Controls, Security Countermeasures of Safety Instrumented Systems (SIS) for Establishing and Conducting Assets, Vulnerability management. Conducting audits and PT regularly for ensuring network security.
- Guide to Placement and Use of Intrusion Detection and Prevention Systems (IDPs).
- Training Employees: Most of the attacks happen due to the employee's lack of training. An untrained employee can react to the message sent by the attacker. Employees should be trained regarding social engineering and phishing attacks. Employees should also be aware to secure their passwords.
- Biometric Data Specification for Personal Identity Verification, Recommendation for Pair-Wise Key Establishment Scheme, Recommended Security and Privacy Controls, PIV Card Application and Middleware Interface Test Guidelines to maintain Authentication and Authorization, and the Use of VPNs and Encryption for Securing Communications.
- Guide to Secure Legacy IEEE 802.11 Wireless Networks, The NIST Handbook to secure Wireless Network Connections.
- Guide to Secure Virtual Network Configuration for Virtual Machine (VM) Protection to Establish a Secure Topology and Architecture.
- Cyber Security Procurement Language for ICS for Ensuring Security when Modernizing and Upgrading.
- Use of access control mechanism to access system components. The access control will prevent attacks from the rogue employee.
- Arrangement of redundancy to take over the system in case of attack happen.

References

[1] Tom Ball, "Top 5 critical infrastructure cyber-attacks", 18 Jan 2018.

[2] Anish Devasia, "Securing SCADA Systems from Cyber Attacks", July 01, 2020.

[3] William T. Shaw, "SCADA System Vulnerabilities to Cyber Attack", Cyber Security Consulting.

[4] Trendmicro, "One Flaw too Many: Vulnerabilities in SCADA Systems", December 16, 2019.

[5] Bonnie Zhu, Anthony Joseph; Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems" 2011. Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, CA, USA.