Isaac Flores

Professor Kirkpatrick

CYSE 200T

31 October 2024

Supervisory Control and Data Acquisition

Supervisory Control and Data Acquisition is a significant aspect of industrial system safety and procedures impacting cybersecurity and monitorization demands. It simplifies and accurately presents data information in an easy humanly readable form. To go further into detail, SCADA systems are utilized by in the industrial manufacturing businesses to retrieve data, present the data collected to human personnel, and provides controlling and monitoring services. Commonly used industrial technology is often subject to attack by threat actors and its vulnerabilities and mitigation techniques should be discussed.

Industrial manufacturing technology is often at risk of falling victim to code injection attacks or structured query language attacks. These attacks send code as command to be read by hardware important to the functioning of industrial manufacturers. These malicious codes can corrupt the functionality of those systems, corrupt its data collected, and corrupt its monitoring functions. For example, some hardware may have the function of monitoring sanitation levels. A structured query language attack could cause hardware to report inaccurate sanitation levels that may endanger the sanitation standards of the assets affected. Furthermore, it is important to consider how S.C.A.D.A. systems are often used with water flow, traffic light functionality, and oil pipelines. Any of these areas could cause catastrophic damages to society if they were to be attacked.

A significant vulnerability associated with infrastructure systems is the access to physical access to hardware and software. This could occur if an unauthorized person were to gain unauthorized access to the software of system to affect its functionality. Furthermore, the use of malware could be used to gain access to software or to corrupt the proper functionality of the hardware. Another major vulnerability to infrastructure systems is malicious packet transmission. Malicious packets can have a level of control over infrastructure systems due to there not being sufficient packet defenses often found in infrastructure systems. It is important to discuss the mitigation options available for infrastructure systems.

Virtual private networking is a cyberattack mitigation tool sued to encrypt connection over the internet. This can make network transmission coming out of a network encrypted and protected from interception by threat actors. Proper firewall configuration strategies is a mitigation techniques that can protect infrastructure systems from the packet vulnerability problem. For example, properly configured firewalls can protect the infrastructure network by blocking the acceptance of specific protocols and packets. Furthermore, firewalls can also provide monitoring features. S.C.A.D.A. has sophisticated detection systems designed to detect suspicious activity that may be of significant concern. Al-Muntaser et al., (2023), state, "Statistical Approaches: Data from S.C.A.D.A. systems can be examined for patterns, trends, and abnormalities using statistical approaches" (p. 322). S.C.A.D.A. provides important statistical data necessary for proper attack vector monitorization and control.

S.C.A.D.A. is an increasingly important tool to be used in conjunction with modern infrastructure systems. Infrastructure systems are pivotal to the prosperity and functionality of modern societies. They include traffic lights, water systems, gas services, communication, and transportation. Vulnerabilities of significant concern involve unauthorized access to

infrastructure systems through the use of malware, structured query language attacks, and malicious packet attacks. S.C.A.D.A. provides mitigation techniques used to monitor suspicious activity, incident alerting, intrusion detection services, and provide statistical infrastructure system data.

Reference

Al-Muntaser, B., Mohamad, A. M., Ammar, Y. T., & Imran, A. R. (2023). Cybersecurity Advances in SCADA Systems. International Journal of Advanced Computer Science and Applications, 14(8)https://doi.org/10.14569/IJACSA.2023.0140835