Name: Hailey Caram

Date: June 14, 2025

SCADA Systems

Due to the dated nature of critical infrastructure systems, they are becoming increasingly vulnerable to threats and intrusion. SCADA applications can play a key role in detecting and mitigating these risks with alarms, real-time data, and process control.

Vulnerabilities of SCADA Systems

The outdated technology utilized in SCADA systems greatly increases the risk of threats and intrusion, particularly as hackers and technology continue to advance. Cybersecurity for SCADA systems is often disregarded or forgotten about. For example, default accounts, which are highly susceptible to hacks, may be left on SCADA systems (SCADA Systems, 2018). This may partly be due to the common belief that SCADA systems are not usual targets for hackers. Additionally, many SCADA systems lack effective monitoring because of this lack of caution, further increasing the risk of threat and intrusion.

There is also a general assumption that SCADA systems are air gapped or isolated from the rest of the network. This incorrect assumption leaves systems vulnerable to viruses or malware spreading throughout the network. Finally, SCADA systems employ legacy systems that are no longer supported or secure. Although SCADA systems are not often hacked, the potential for damage is critical due to the importance of the infrastructure SCADA systems support.

Mitigations

To mitigate these risks, applications such as firewalls and demilitarized zones (DMZ) can be implemented to prevent the degradation of critical infrastructure systems. This network architecture can keep unwanted direct traffic from going between the SCADA and corporate networks (NIST, 2023). Another measure administrators can take is to remove default accounts and implement strong password policies across all systems within the network. This protection is easily implemented and prevents unauthorized access to the system. Lastly, owners of critical infrastructure systems should apply an intrusion detection system to monitor and alert on any unwanted traffic coming to or from the network.

Conclusion

Although the majority of SCADA systems are outdated and vulnerable, these systems are omnipresent in our society. Some examples of the vulnerabilities to SCADA systems include a lack of network segmentation, failure to remove default accounts, and outdated protocols. To mitigate these risks, administrators should implement firewalls and demilitarized zones to decrease unwanted traffic. Additionally, removing default accounts and strong password policies help to protect against risk. Finally, an intrusion detection system should be present to monitor and alert administrators of unwanted traffic. SCADA systems are often overlooked, but the exploitation of any of these vulnerabilities has the potential to be devastating.

References

NIST. (2023, September 3). Guide to Operational Technology (OT) Security. NIST Technical Series Publications. Retrieved June 15, 2025, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

SCADA Systems. (2018, July 25). *SCADA Systems*. http://www.scadasystems.net/