SCADA Systems Write Up

Asher Embry

CYSE 200-T

Our critical infrastructure is vulnerable because insecure legacy hardware is now connected to the modern internet. Supervisory Control and Data Acquisition (SCADA) systems which manage this infrastructure act as the primary monitoring tool to control and mitigate these risks.

Infrastructure's Critical Vulnerabilities

Critical infrastructure such as the power grid and water treatment was built on Operational Technology (OT), designed for physical reliability and not digital security. Because of this design focus, much of our critical infrastructure has weaknesses due to their inherent weaknesses. Some of these weaknesses according to an article from IEEE about cybersecurity in SCADA systems are a lack of encryption and authentication, open access networks, and internet-facing environments (Skrodelis, Kelle, & Romanovs, 2024).

Bringing internet connectivity to critical infrastructure is very efficient and useful, but it also exposes those systems to cyber threats. If a system is attacked, the risk is more than just data theft, it can result in real world physical harm. According to Claroty, this can include controlling the water supply, power supply, or harmful malfunctions in nuclear reactors (The Claroty Team, 2024). The most critical vulnerability is the connection between insecure hardware and the open internet.

The Role of SCADA Systems

SCADA applications are interfaces used to operate and manage utilities. Because of their connection to physically control infrastructure, they are now a critical defense to protect the underlying systems. These systems provide centralized real-time monitoring to detect anomalies like a valve opening or a pump turning on at an unexpected time. They also mitigate risk when set up to enforce strict user authentication and logging all actions taken. When used as a secure gateway, SCADA systems can segment networks and protect physical infrastructure from a digital threat. With the rise of AI in the current era, it is also being integrated into SCADA systems to detect threats in real time (Skrodelis, Kelle, & Romanovs, 2024).

Conclusion

Critical infrastructure's primary vulnerability is the connection of insecure legacy hardware to the internet. SCADA systems are now used as an essential tool to defend these systems, perform accurate monitoring, and segment the network to defend physical components.