Thomas Roeseler

CYSE 200T

Professor Charlie Kirkpatrick

November 3, 2022

SCADA Systems

SCADA stands for Supervisory Control and Data Acquisition. SCADA systems refers to systems that are used to control and monitor critical infrastructure processes like water treatment and gas pipelines. SCADA systems are the centralized systems that supervise and control an entire site of a certain infrastructure. Remote Terminal Units (RTUs) connect to the sensors of whatever process the system is for which helps to convert sensor signals to digital data and send that data to the supervisory stream. Data acquisition can start at the RTU or PLC(Programmable Logic Controller) level and is then formatted in a way to let the operator in the control room make the supervisory decisions with the Human Machine Interface(HMI). SCADA systems are a target of cybercriminals because they control critical infrastructure and if a cybercriminal is able to get into those systems, bad things can happen or they think they will get paid a lot if they were to use ransomware.

Vulnerabilities with SCADA Systems

SCADA systems are a potential target for cybercriminals because they control critical infrastructure and the attacker could have intentions for money or for cyberterrorism if they were to try to poison a water treatment center like a hacker did to a water treatment center in Florida in 2021. The two major security threats to SCADA systems are unauthorized access to software and the second major threat is that there is little to no security on packet control protocol. To address these risks, SCADA vendors are developing specialized industrial VPNs and firewall solutions for SCADA networks that are based on TCP/IP. Whitelisting has also been used because of their ability to prevent unauthorized application changes. “An indispensable asset, IDS even detects policy violations. This is vital, because vulnerability sometimes stems from

scenarios other than malice,(Tiga 2019).” Network intrusion detection is important for SCADA systems because of their trouble with being able to identify any suspicious activity, which is why they need Intrusion Detection Systems. Intrusion Detection Systems help identify intruders or suspicious activity on a network which is important for security with SCADA systems because they can help find the vulnerabilities for that system.

A reason SCADA systems have vulnerabilities is because they were made to be open and easily operated, so that it could be repaired easily. SCADA systems usually fail to detect any suspicious activity or fail to give a proper response to a cyber attack if one does happen. “Believe it or not, there are systems in operation today (that shall remain anonymous for security reasons) that still have workstations sharing the same passwords. Or, in the worst case, systems do not require a password whatsoever, (Nucleus Command Systems, 2020).” There are many systems today that are 15+ years old and share passwords or don’t use passwords at all which is a big risk if they were to be the victim of a cyber attack. The older systems are more susceptible to attacks because of these vulnerabilities.

Conclusion

There are vulnerabilities that come with SCADA systems and because they are a potential target for cyber attacks, it is important to mitigate these risks. They are important because critical infrastructure affects many people in an area, so if something were to happen, it could affect thousands of people. A big reason SCADA systems have many vulnerabilities is because of the lack of monitoring with their systems. Developing specialized industrial VPNs and firewall solutions for SCADA systems is a way SCADA vendors are mitigating some of their risks. Whitelisting is also something that is being used for SCADA systems because of their ability to prevent unauthorized application changes.

References

SCADA Systems - Google Docs

Scada systems and their vulnerabilities (secpoint.com)

SCADA Security: What Makes SCADA Networks More Vulnerable to Cyber-Attacks? - Nucleus Command Systems

How To Ensure Your SCADA System Is Secure! (tiga.us)