SCADA Systems

Tariq Sims

Old Dominion University

CYSE 200T

Professor Kirkpatrick

11/5/2023

Critical infrastructure systems in the water, energy, transportation, and healthcare sectors are keys to the functioning of our society. All of these systems rely on SCADA applications in which monitor processes. SCADA systems are crucial for the systematic operation of critical infrastructure as well as introduce vulnerabilities that are potentially exploited. Some vulnerabilities can include **HMIs,** which display data from multiple sensors and machinery that is connected to the SCADA system which helps users make accurate decisions that can all be implemented into the same system. HMIs can be a target for threat actors who are trying to gain control over processes or steal information. Mobile applications that can be used through tablets that support engineer's control PLCs and RTUs. Communication protocols like Modbus can control different mechanisms that are supervised by SCADA systems, but they lack a level of security capabilities to defend themselves against threats that SCADA systems attract. The role of SCADA systems in mitigating these risks includes access control, encryption, patch management, supply chain security, etc. First, SCADA systems can enforce strict access control measures which can ensure only authorized users can interact with the system. Secondly, SCADA can use encryption to protect data that is in transit which makes it harder for attackers to manipulate data. Thirdly SCADA vendors should occasionally apply security patches. Lastly, SCADA systems can add supply chain security practices that verify the integrity of software components used in critical infrastructure systems.

Resources:

SCADA Systems - SCADA Systems. (2018, July 25). SCADA Systems. https://www.scadasystems.net/

One Flaw too Many: Vulnerabilities in SCADA Systems. (n.d.). https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems#:~:text=It%20should%20be%20noted%20that,DoS)%2C%20or%20steal%20information.

ICS/SCADA Access Controls | Infosec. (n.d.). https://resources.infosecinstitute.com/topics/scada-ics-security/ics-scada-access-controls//