Camrin Joyner

12/12/2024

Profesor Hagh

CYSE 200T

SCADA Systems Write Up

Supervisory Control and Data Acquisition systems are very important for running vital facilities like nuclear power plants, water treatment plants, and the transit systems. Even though they play an important role, SCADA systems have major flaws that can put public safety and business efficiency at risk. One of the biggest problems with these flaws is that they depend on old technologies, like older protocols for communication like Modbus and DNP3, which don't always have encryption and can be hacked or used without permission. Also, SCADA hardware like Remote Terminal Units and Programmable Logic Controllers is more likely to be interfered with or destroyed when it is out in the open, especially when it is in a remote or poorly protected area. Moving from private, closed networks to architectures that are linked to the internet has increased these risks by making SCADA systems more vulnerable to more types of cyber threats, like malware, ransomware, and denial of service attacks.

SCADA systems, on the other hand, don't do nothing when these risks happen. They have features that are meant to make them durable and less vulnerable. Inefficient architectures, like backup systems and computers with two sets of power supplies, keep operations running even if hardware or the network goes down. Human Machine Interfaces let workers see real time data and quickly react to problems by using the SCADA system's ability to gather and display complicated process data. Modern SCADA systems also have high-tech security features like industrial grade firewalls, VPNs, and application whitelisting. These protect confidential communication channels and stop software from running without permission. Having open, standard protocols for communication like Modbus TCP/IP and IEC 61850 also makes it easier for devices to talk to each other. These protocols include encryption and authentication tools to protect data security.

Even with these improvements, there are still problems. Modern security features can't be added to many older systems without major updates, which leaves them open to risk. Also, Misconceptions about the security of SCADA systems also make them less secure. For example, some people think that physical barriers or VPNs are enough to protect them. Modern technologies such as XML based web services and cloud-hosted solutions are being used by SCADA developers to solve these problems. However, these new technologies raise new worries about the security, reliability, and latency of the internet.

In conclusion, SCADA systems are necessary for managing important infrastructure, but they are also very vulnerable and need to be constantly improved and watched over. By using new technologies, following industry-wide safety standards, and putting money into modernization projects, SCADA systems can successfully lower risks and make sure that the infrastructure that supports modern society works safely and reliably.

Camrin Joyner

12/12/2024

Profesor Hagh

CYSE 200T

Works Cited

Stouffer, Keith, et al. "Guide to Industrial Control Systems (ICS) Security." *CSRC*, 3 June 2015, csrc.nist.gov/pubs/sp/800/82/r2/final.

admin, Published. "Recent SCADA Cybersecurity Breaches and Their Implications: 2024." *Process Automation Solution | Pro-Tech Systems Group*, 2 Apr. 2024, www.pteinc.com/recent-scada-cybersecurity-breaches-implications/.

cisa. "Mitigations for Security Vulnerabilities in Control System ..." *Cisa.Gov*, www.cisa.gov/sites/default/files/2023-01/MitigationsForVulnerabilitiesCSNetsISA_S508C.pdf. Accessed 13 Dec. 2024.

Devasia, Anish. "Securing SCADA Systems from Cyber Attacks - Technical Articles." *Control*, control.com/technical-articles/securing-scada-systems-from-cyber-attacks/. Accessed 13 Dec. 2024.

Micro, Trend. "One Flaw Too Many: Vulnerabilities in SCADA Systems." *Trend Micro (US)*, www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems. Accessed 13 Dec. 2024.

Camrin Joyner

12/12/2024

Profesor Hagh

CYSE 200T