Juwon Marquis Brunson
CYSE 200T
11/9/2025

Vulnerabilities of SCADA Systems

Supervisory Control and Data Acquisition Systems are integral to the successful operations of critical systems such as power plants, electrical systems, and aerospace/transport facilities. While they are revolutionary in their field, they are also a security risk due to the nature of analog vs digital upgrades. APTs have shown they can infiltrate and fake data while changing SCADA programs without user knowledge.

History

Supervisory Control and Data Acquisition (SCADA) Systems were used in the 1950s-1960s to monitor and control large-scale industrial processes. They relied on analog technology when first invented and rapidly grew in technology as the 70s created microprocessors, leading to upgrades in systems. Another innovation that allowed SCADA to grow was the creation of what is called Human Machine Interfaces (HMI), which allowed operators to visually see and interact with the data that the SCADA is controlling.

Due to all of these changes, almost all SCADA systems have undergone changes from analog to digital, raising their attack surface, including the integration of Internet of Things (IOT) technologies. In the 21st century, SCADA systems are now starting to integrate Artificial Intelligence into their systems as well as cloud computing.

Concerns

As highlighted with our course and some of the changes in technology like Artificial Intelligence, IOT, Cloud Computing, and digital vs analog controls, we can assume that there are attack vectors needing to be addressed for these changes. Most importantly will be the change from analog to digital. This change alone is huge in how you conduct security, as you will go from a more physical security control to one that is forced to implement extensive barriers to data access, such as MFA, biometrics, utilizing the CIA triad, and NIST standards.

The major concern faced is that of Advanced Persistent Threats (APTs). There has

already been evidence of China and Russia breaking into our most critical systems, such as when China used its APTs Volt Typhoon and Salt Typhoon to infiltrate power grids, telecommunications networks, and transportation systems with the “apparent goal of prepositioning for potential wartime disruption (Dutta). The advancement of technology is always a good thing, but we need to bring it to the forefront of our security concerns and policies to protect our greatest resources, which are almost all controlled by SCADA systems.

Conclusion

The introduction of SCADA systems has been a revolutionary change and improvement to the analog systems we used in place of them back before the 1950s and 60s. They have allowed more efficient and safer usage of integral systems important to American technologies. As was shown with the American and Israeli intelligence attack on the Iranian nuclear power plant, the targeting of a critical software, hardware, or 3rd party system can lead even American power plants to vulnerabilities. If a similar attack occurred on American power plants simultaneously, it would hamper, if not destroy, our war efforts and create a global catastrophe if a meltdown occurs.

Resources

“History of SCADA.” *SCADA Info*, www.scadainfo.com/history-of-scada/.

“Using SCADA to Protect Critical Infrastructure and Systems | Cyberpaul.” *Odu.edu*, 6 Dec. 2020, sites.wp.odu.edu/cyberpaul/2020/12/06/using-scada-to-protect-critical-infrastructure-and-systems/.

Dutta, Tushar Subhra. “Chinese Hackers Attacking Critical Infrastructure to Sabotage Networks.” *Cyber Security News*, CybersecurityNews, 14 Apr. 2025, cybersecuritynews.com/chinese-hackers-attacking-critical-infrastructure/.