Name: Eric Mung'au Preston

Date: November 6th, 2022

SCADA Systems: Vulnerabilities and Mitigation Strategies

SCADA systems are a complex network of monitoring multiple infrastructure processes and intaking and sending data to a main computer for it to be managed and checked. SCADA systems are integral to maintaining organizations and avenues of critical infrastructure. So, with these systems being so significant, I feel it's absolutely necessary to take every possible precaution to make them as secure as possible.

SCADA Systems

Supervisory Control and Data Acquisition (SCADA) systems control infrastructure operations within an industrial setting. Crucial infrastructure can vary from water treatment plants and farms, to steel factories, power plants, and pipelines. Now, with SCADA systems, they consist of several crucial components that allow for immediate results. Some of these components are a Human Machine Interface (HMI), a Remote Terminal Unit (RTU), a Programmable Logic Controller (PLC), and communication and supervisory systems (Kirkpatrick, 2022).

The HMI is an instrument that provides data to a human operator on the dashboard. It links to the SCADA systems databases and provides up-to-date information on problems through simplistic graphs, symbols, and functions. The RTU is a part of SCADA system hardware and changes electrical signals from equipment to values. These values allow for the RTU to send out its own signals to gain some control of switches and pipes (Kirkpatrick, 2022). A PLC is meant to support the automation process by controlling the assembly line and reduces production costs with its efficiency (Dorjee, 2014).

Finally, communication and supervisory systems are meant to help with connection and logging. Communication systems like the internet and networks are for connecting all of these parts together for the supervisory systems. The supervisory systems are essentially multiple servers that log all of the data that's created within the infrastructure operations that also serve as a communicator between the PLC's, RTU's, and other equipment. All of these systems and machines create SCADA systems, which are fundamental in monitoring critical infrastructure and the data it produces.

Vulnerabilities in SCADA and Critical Infrastructure

With SCADA systems being so necessary within critical infrastructure, it's extremely important that there is great security across all aspects. Unfortunately, there are several holes within both SCADA and infrastructure systems that could cause severe damage if not mitigated properly.

Large threats against SCADA systems are gaining access to software via a cyber attack and lack of security when it comes to managing packets of data by having few to no firewalls to filter and manage them. Other threats include, lack of encryption, lack of updates in software, and old machinery being tough to upgrade (Lamba et al., 2017).

Additionally, simple things like using default passwords, buffer overflow, and lack of physical security are big vulnerabilities to these systems (Yadav & Paul, 2019). Most importantly, if SCADA gets compromised in any way by these issues, organizations that support critical infrastructure get compromised, and things like food, water, power, and gas supply get slowed down monumentally.

Mitigation Strategies

Whenever there are possible vulnerabilities to any system, strategies to mitigate damage and risks are pivotal. SCADA systems are no different, and there are numerous ways to make them more resilient.

A starting point would be strict password and firewall policies to help with access issues and managing packets (Chen-Ching et al., 2009). Other kinds of strategies include company wide security policies and informing, upgrading the technology, transitioning to wireless, applying encryption, and secure network protection (Fernandez & Fernandez, 2005). These are some of many tactics that can help to protect critical systems and infrastructure.

Conclusion

In conclusion, SCADA systems are crucial in supporting the critical infrastructure that organizations provide. The multiple layers of components and technology must work in unity to allow for processes to move steadily, and for data and information to be monitored and controlled. While there are unfortunate vulnerabilities within these systems, there are also just as many mitigation strategies and techniques that can help to defend against these problems, and hopefully, over time, they can become the standard for all systems and organizations within critical infrastructure.

References

Chen-Ching Liu, Chee-Wooi Ten, & Govindarasu, M. (2009). Cybersecurity of SCADA Systems: Vulnerability assessment and mitigation. *2009 IEEE/PES Power Systems Conference and Exposition,* 1-3. 10.1109/PSCE.2009.4840120

Dorjee, R. G. (2014). Monitoring and control of a variable frequency drive using PLC and SCADA. *International Journal on Recent and Innovation Trends in Computing and Communication*, *2*(10), 3092-3098. https://d1wqtxts1xzle7.cloudfront.net/35586590/Monitoring_and_Control_of_a_Variable_Frequency_Drive_Using_PLC_and_SCADA-with-cover-page-v2.pdf?Expires=1667769676&Signature=Ujydy97zoDUTcVUPhuA~1lXAVJx1lZHpRJ0jw3lrBDN6zFnK0kIDdKfdOPXeG4v03ZxokkMCEnjp1sEQ~KlXOyUgaAwz5OhFAFrHjnQeeM7hrEA02cyzkCOc1Suv4nCvMbOI6Mqr1HS-K4vN8T4hVSDlpxLDptceyC~oK4cwUj4tw3GlVWH1RViBY~4hjXZRkpjENb4vEWVH001Q-DdtY62qnoqOKE3Js2vHwLtUPhQ44Oa34cs9J1VqVHzOWC8xcqu4h0HQVzHZCclRqVNxoa-hyEz73tHe3Scv9zaWxM0IupaCRez7LcBlCnzijYWNgHG7SAsKzM5KThVc7kaQ4Q__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Fernandez, J. D., & Fernandez, A. E. (2005). SCADA systems: vulnerabilities and remediation. *Journal of Computing Sciences in Colleges*, *20*(4), 160-168. https://dl.acm.org/doi/abs/10.5555/1047846.1047872#sec-ref

Kirkpatrick C. (2022). SCADA Systems. *Google Docs.* Retrieved November 5, 2022, from https://docs.google.com/document/d/1DvxnWUSLe27H5u8A6yyIS9Qz7BVt_8p2WeNHctGVboY/edit

Lamba, A., Singh, S., Balvinder, S., Dutta, N., & Rela, S. (2017). Mitigating cyber security threats of industrial control systems (scada & dcs). In *3rd International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS–July 2017)*. http://dx.doi.org/10.2139/ssrn.3492685

Yadav, G., & Paul, K. (2019, September). Assessment of SCADA system vulnerabilities. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1737-1744). IEEE. 10.1109/ETFA.2019.8869541