Name: Desmon Smith

Date: 3/21/2024

How Reliable Are Our Industrial Systems?

SCADA systems are essential to daily life and they should not have this many vulnerabilities. Companies should be working hard to come up with a way to protect these systems from hackers and itself.

What Is SCADA?

As Daneels and Salter stated, SCADA stands for Supervisory Control and DATA Acquisition (1999). SCADA is used for systems that control our day to day life. SCADA systems are used when companies need to gather and process a large amount of data (Sami, 2019). Sami stated in an article that, “SCADA systems can be found in manufacturing facilities, oil production and processing, pharmaceuticals, energy, water treatment and distribution” (2019). SCADA systems have been around for a while and they are improving everyday.

Vulnerabilities

Like any other system, SCADA does have vulnerabilities. These systems can be controlled online so they are susceptible to cyber attacks. When SCADA was first created security issues were not a concern (Manor et al., 2022). Since security issues were not a priority, it is difficult to add proper security measures to these systems. If a hacker finds a hole in SCADA’s security, it

can expose them to other vulnerabilities they can attack in the future (Manor et al., 2022). Hackers getting into the SCADA systems can be very detrimental to society and open the door for cyber terrorism. Although adding security measures to SCADA is hard, progress is being made.

In addition to security errors, there are also many implementation errors in SCADA systems. These errors include lack of input validation, invalid index array, improper control flow management, and improper limitation of memory buffer (Manor et al., 2022). The most important error is the lack of input validation because it directly leads to the other issues. Input validation is the process of software validating that inputs put into the system are correct and safe to carry out (Manor et al., 2022).

How SCADA Deals With Risks

As I mentioned previously, security was not a concern when creating SCADA. This makes SCADA systems a target for cyber attacks. With that being said, it is important to perform security checks regularly (Darshana & Srinivas, 2020). There are multiple organizations contributing to the security of SCADA systems. These organizations are mitigating risks by studying past incidents and threats (Darshana & Srinivas, 2020). Learning from your mistakes is effective, but SCADA also needs to focus on potential attacks and incidents that target vulnerabilities that have not been exposed to them yet.

Conclusion

SCADA systems were founded in a time where cybersecurity was not an issue. As we progress into the future, vulnerabilities in the SCADA system are being exposed and manipulated. SCADA controls our vital resources and these vulnerabilities are a serious threat. Different organizations are working desperately to get security systems in SCADA up to date. It is harder than expected, but we are moving in the right direction.

References

Daneels, A., & Salter, W. (1999). What is SCADA?. https://cds.cern.ch/record/532624/files/mc1i01.pdf

Darshana, U., Srinivas, S. (2020). SCADA (Supervisory Control and Data Aquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89. https://www.sciencedirect.com/science/article/pii/S0167404819302068?casa_token=-6O4xXhkfIIAAAAA:704XAcRpNBSvgo0NfnxYigt8WV7geHFPG5Gx6fDlETi7MO7KuYl_h4rsQB9q-pYkxMtyj_Kl6w

Manor, A., Abdun, M., Mohammed, C. (2022). SCADA Vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security*, 125. https://www.sciencedirect.com/science/article/pii/S0167404822004205#sec0032

Sami, A. (2019). SCADA (Supervisory Control and Data Acquisition). https://www.technologytimes.pk/wp-content/uploads/wp-advanced-pdf/1/scada-supervisory-data-acquisition.pdf