Name: Justin Graham

Date: 11/6/2022

SCADA SYSTEMS

SCADA systems are necessary in keeping critical infrastructure active everyday. These devices have been around for decades and have been upgraded over time to adapt to new technologies, but have also allowed for vulnerabilities within their systems that can be exploited by malicious attackers. There are plenty of reasons these devices are a high priority for attackers and this article explains some of the vulnerabilities and solutions to better secure these systems.

SCADA System

SCADA (Supervisory Control and Data Acquisition) are the systems that are used to control infrastructure processes. [These systems contain a human operator with a device that will display the processed data, a supervisory system, remote terminal units, programmable logic controllers, and a communication infrastructure that connects the remote terminal units to the supervisory system] (SCADA Systems pg. 1). In a basic definition, SCADA systems monitor and control basic processes such as opening and closing valves or turning on and off relays. However, they are very important in keeping our society running and are a clear target for hackers who want to disrupt the natural flow of things.

Vulnerabilities

One of the many problems with the control systems used in our critical infrastructures is that they were originally designed many years ago before online security was a concern. As the systems have been updated and become internet capable, the physical limitations such as processing power and bandwidth prevent the system from properly using encryptions and newer protocols. Authentication is also a concern. Tim Yardley, a technical program manager at the University of Illinois stated in his article, “In the case of authentication, it is fairly common for devices in the control space to use default passwords for access and control. Most of these default passwords are very easy to find when using search engines” (Yardley pg. 15). This demonstrates how little concern these companies have with the physical security of the SCADA devices. Other issues that are defined by the SCADA Systems article include “threats to packet access to network segments that host SCADA devices” (pg. 6). There are many situations where SCADA devices

have little to no security on packet protocols. This can allow hackers or unauthorized intruders to gain access and send information into the network and cause issues with the SCADA devices.

SCADA Risk Prevention

In order to combat the vulnerabilities in our critical infrastructures, there have been many new standards created. Some examples listed by Hardley are the “North American Electric Reliability Corporation, National Institute of Standards and Technology, and the American Gas Association” (Hardley pg. 18). Each of these companies have released new standards that are designed to increase the protection on SCADA devices. There have also been many open source projects designed for SCADA devices. Tools such as protocol specific firewalls, encryption overlays, and specialized VPNs. These devices will help combat network vulnerabilities while the new standards can help prevent physical vulnerabilities and create a more secure environment.

Conclusion

SCADA devices have been in use for decades now and will not be going away anytime soon. They could be considered the backbone of our critical infrastructures and that is why they are a target for malicious attackers. There have been some improvements to the systems with the evolution of technology but not enough to provide tight security on the systems. There needs to be more resources used to better secure and improve the SCADA systems especially with the next evolution of the devices. As more information is connected to the internet on these devices, the more security should be emphasized in protecting critical infrastructures.

References

Yardley, Tim. “SCADA: Issues, Vulnerabilities, and Future Directions .” *Usenix The Advanced Computing Systems Association*, Usenix, Dec. 2008, https://www.usenix.org/system/files/login/articles/258-yardley.pdf. Accessed 6 Nov. 2022.

“SCADA Systems.” *SCADA Systems*, http://www.scadasystems.net/.