CYSE 200T Write-Up: “SCADA Systems”

Herald Anacta

School of Cybersecurity, Old Dominion University

CYSE 200T: Cybersecurity, Technology, and Society

Mr. Charlie E. Kirkpatrick

November 06, 2022

Herald Anacta

November 06, 2022

The SCADA System

Since the advent of time, technological inventions and advancements have helped shape the way humans live. Water irrigation, the introduction of electricity, even the invention of aerial flights has, one way or another, made a major impact throughout human history. Today, these modern marvels are regarded as critical infrastructures that are vital to modern day society. The SCADA Systems, also known as Supervisory Control and Data Acquisition came into existence to help guide, monitor, and control industrial equipment and machineries that automate and regulate major industrial infrastructures Think of it as the brain that runs the whole show. While generally considered to be secured and safe, SCADA networks can be potential targets of cyber-attacks.

What Exactly is SCADA?

The acronym SCADA or Supervisory Control and Data Acquisition can be described as the backbone that supervises industrial processes. A SCADA (supervisory control and data acquisition) is an automation control system that is used in industries such as energy, oil and gas, water, power, and many more. The system has a centralized system that monitors and controls entire sites, ranging from an industrial plant to a complex of plants across the country (Krambeck,2019). Think of it as a centralized monitoring system that controls individual small systems that are used in every major industry.

Is it vulnerable?

There is no such thing as 100% impenetrable in the world of technology, just because something has not been hacked means it can never be hacked. One major vulnerability about SCADA systems is that, since it is usually stored and located inside a company's own building, the belief is that it is physically impossible to infiltrate it. However, the potential of unauthorized human access is always there. While unlikely to happen, there is always that slim chance that a person who has bad intentions can sneak in and access the systems.

How to mitigate the risk?

It is always important to never be complacent about anything. Always have a contingency plan. A SCADA failure will be catastrophic, that is why companies who use SCADA put an emphasis on safeguarding it. With the use of technology, SCADA systems can be controlled remotely. You can also influence and control a SCADA environment without having to directly respond to each event. Using logic-based rules, operators are able to designate the completion of certain actions when sensors detect abnormalities (Wangsness, 2022). Below are the other methods in which companies who use SCADA systems help mitigate the risk and potential vulnerabilities of the system:

- Redundancy of critical hardware to serve as back up
- Use of alarm systems
- Development of specialized industrial VPN for added protection

Conclusion

SCADA systems play a big role in maintaining society's vital infrastructures. However, it is not completely safe from cyber-attacks. Proper protocols and procedures are a must to secure these highly valuable assets. We must remember that "Prevention is always better than cure"

References

Wangsness, Cole. (2022). *What is a SCADA System and How Does it Work?*. onlogic.com, https://www.onlogic.com/company/io-hub/what-is-a-scada-system-and-how-does-it-work/. Accessed 05 November 2022

Krambeck, Donald (2015) An Introduction to SCADA Systems. allaboutcircuits.com, https://www.allaboutcircuits.com/technical-articles/an-introduction-to-scada-systems/ . Accessed 05 November 2022