SCADA Write-up

Cali J. Zuk

Department of Cybersecurity, Old Dominion University

CYSE 200T

Professor Charles Kirkpatrick

November 3rd, 2024

Introduction

SCADA or Supervisory Control and Data Acquisition systems have long been a critical aspect of our national infrastructure. SCADAs can be thought of as a version of command and control or CnC software for industrial control systems (ICS). These systems aggregate data across different technological layers of an industrial system and allow for easier human control of these systems through a HMI or Human Machine Interface (*SCADA Systems*, n.d.). They are the main system facilitating the control of vital national infrastructure such as traffic lights, water delivery, electrical transmission, gas transmission, etc. If a SCADA fails or falls into the wrong hands, it could not only threaten profits and national security, but could also kill people who are depending on the regular flow of electricity, gas, and water. This paper will first describe the cybersecurity threats facing these systems and then go over proposed remediations for these threats.

Threat Overview

SCADA systems face many threats as a result of two factors, their lack of security and the massive damage an attacker can do by compromising them. The lack of security stems from the fact that these systems were never designed with cybersecurity in mind. The first two generations of SCADA systems both had no cybersecurity built in (Smurthwaite & Bhattacharya, 2020). The reason for this are that the developers believed that the obscurity of these systems, combined with the niche software and physical isolation of facilities employing their use meant that those controls were not required (Smurthwaite & Bhattacharya, 2020). This lack of security from the beginning has resulted in the two thorniest issues in securing these systems, the first being a struggle to implement systems to verify authorization, the second being a lack of protection for data being transmitted between different layers of the system (*SCADA Systems*, n.d.). As these technologies have matured, they have begun to incorporate more remote management features which has given them a similar threat surface to the wider IoT ecosystem. SCADA systems are also often comprised of a mixture of older systems subject to first and 2nd generation security problems with modern systems connected to the internet (Nazir et

al., 2017). This mixture creates a uniquely difficult environment to secure as systems that were designed to be air-gapped and never exposed to the internet are being connected with newer systems that are always connected to the internet.

Proposed Resolutions

How to best secure these system is subject to much discussion; some proposed solutions are to expand deployment of Network Intrusion Detection System (NIDS), Network Intrusion Prevention System (NIPS), government regulations mandating software and hardware upgrades, contracting with 3rd parties to penetration test vital infrastructure, and expanding the use of machine learning systems to automatically detect suspicious behavior before human analysts (Nazir et al., 2017). NIDS and NIPS would work to stop attacks at the perimeter before they gain access to vital low level systems. Stronger regulations and the enforcement of those regulations would help ensure that old hardware and software gets phased out. Conducting penetration tests and vulnerability scans would aid ICS security professionals in remediating risks and threat vectors before cybercriminals are able to find them (Nazir et al., 2017). Expanding the use of machine learning systems would enable automatic remediation of heuristically detected intrusions well before a human analyst could do the same. Another strategy worth mentioning that has seen success is the use of honeypots to divert would be attackers away from critical system if an intrusion occurs. These honeypots would also allow researchers and analysts to examine the pathology of an attack against a SCADA system and further add to the limited body of real world research (Nazir et al., 2017).

Conclusions

The reality of the current state of SCADA security is not good, these critical systems are often left in place to age and chug away well after replacement is justified (Smurthwaite & Bhattacharya, 2020). Furthermore, these older generation systems are often layered over with newer technical systems that add more cracks to the systems. Improving the cybersecurity posture of these critical systems is critical, and it will take time, money, and effort that many utilities have demonstrated a

hesitance to provide. From California's ancient power grid causing the lethal Camp Fire (*Camp Fire*, n.d.) to Texas with a failure to weatherize the Texan Interconnection (Communications, 2021). If these utilities refuse to maintain the lifeblood of their businesses are any indication, securing SCADAs against attack will only come after severe compromises that may kill people. Information Technology in many companies is seen only as a cost center, and the people who own and run utilities have shown that they see everything as a cost center.

Works Cited

Camp Fire: By the Numbers. (n.d.). FRONTLINE. Retrieved November 5, 2024, from https://www.pbs.org/wgbh/frontline/article/camp-fire-by-the-numbers/

Communications, J. T. of U. (2021, March 2). *Cold Collapse: A Look Inside the Texas Energy Grid Failure | WWU News | Western Washington University*. https://news.wwu.edu/cold-collapse-a-look-inside-the-texas-energy-grid-failure

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, *70*, 436–454. https://doi.org/10.1016/j.cose.2017.06.010

SCADA Systems. (n.d.). SCADA Systems. Retrieved November 3, 2024, from https://www.scadasystems.net/

Smurthwaite, M., & Bhattacharya, M. (2020). Convergence of IT and SCADA: Associated Security Threats and Vulnerabilities. *IOP Conference Series. Materials Science and Engineering*, *790*(1), 12041-. https://doi.org/10.1088/1757-899X/790/1/012041