Vulnerabilities Common in Critical Infrastructure Systems and Their Mitigation

Gregory S. Oehm

School of Cybersecurity, Old Dominion University

CYSE 200: Cybersecurity, Technology, and Society

Prof. Lida Haghnegahdar

November 3, 2024

Introduction

SCADA systems, or supervisory control and data acquisition systems, play an important role in much of the nation's critical infrastructure. These systems assist in the coordination and operation of many kinds of facilities, including those that specialize in energy generation, agriculture, transportation and shipping, and manufacturing, among numerous others. Through the use of sensors, Programmable Logic Controllers, and Remote Terminal Units, alongside interfaces, SCADA systems are able to control the function of industrial devices (*SCADA Systems*, 2024). However, a number of vulnerabilities can often be found in these systems. The security controls present in industrial control systems may be lackluster or nonexistent, while their connection to other devices provides a way for others to attempt to gain access to them, often made worse by individuals unaware of or apathetic to the need for the security of this infrastructure. Given that the facilities SCADA systems are utilized in are generally necessary for towns, cities, or even the country as a whole to function properly, great care should be taken to ensure that the vulnerabilities present within them are mitigated to a reasonable extent. Otherwise, threat actors may be able to gain access to these systems, potentially causing damage to them, thus resulting in significant harm to the overall population.

Networks

An important factor to consider in the security of critical infrastructure systems is its connection to the larger network within the organization. This connection to a wider network naturally brings with it a number of vulnerabilities. Any vulnerabilities present in other departments or divisions could lead to their SCADA systems being compromised. SCADA systems do not need to be directly connected to the Internet for attackers to gain access, merely connected to any device that can be accessed. Should any part of the organization's network be

connected to the Internet, the possibility arises for attackers to, through a large-scale attack, damage the organization's critical infrastructure without the need to gain physical access to the organization's individual servers, controllers, and units. SCADA systems often lack the ability to filter out malicious packets, so any threat actor who has the ability to send packets to these devices may be able to control them, whether through the organization's network or some other way (*SCADA Systems*, 2024). The way in which an organization's systems are structured, therefore, can result in multiple vulnerabilities that must be mitigated in some form. Simply disconnecting SCADA systems from the rest of the network might be viable, but certain controls might also be put in place to reduce the risk that an attack will cause damages to the organization. The implementation of intrusion prevention systems and firewalls, alongside segmenting the network can each limit the reach of malicious traffic (IEEE, 2024). Unique VPNs, too, might be used to mitigate these threats (*SCADA Systems*, 2024). Taking these steps can limit the scope of an attack, hopefully preventing it from reaching the critical infrastructure present in the organization's facilities.

Updates and Quantity of Devices

Another vulnerability often found in critical infrastructure systems, and perhaps one of the most important, is that the hardware and software that makes up SCADA systems generally have poor security in place. This is partially due to the infrequent security improvements these systems tend to receive, with updates occurring rarely, in some situations. There are a variety of possible reasons for this, such as patches and updates interrupting normal operations, for a time. In any case, many critical infrastructure systems have out of date software or hardware (IEEE, 2024). These issues are exacerbated by the huge number of devices that make up critical infrastructure systems. Further, both the high number of devices and the relatively large area in

which they may be located can make implementing security improvements an incredibly difficult task. Hundreds or even thousands of devices may be in use in some facilities, each of which may have severe vulnerabilities. Any compromises that occur can cause attackers to gain access to a massive number of devices necessary for the facility to function correctly. Though it may be difficult, ensuring that patches are implemented often across all relevant devices, perhaps by setting aside a regular timeframe in which infrastructure systems can be updated, can reduce the ability for attackers to gain a foothold in the organization's systems.

Impact of Users

Though the tangible security measures in place are certainly crucial, the human element of organizations should not be overlooked. Users in an organization often contribute to successful attacks, whether intentionally or unintentionally. Phishing attempts are not uncommon, and can lead to important information, including usernames and passwords, being exposed to those outside the organization relatively easily. This information could then be used to attack critical infrastructure. Sharing information with those not authorized to know it, even within the organization, can pose a significant risk to the security of its systems. A lack of care may also lead to employees utilizing previously used or weak passwords, or unknowingly installing malware onto the organization's systems. Ultimately, the best way to mitigate the vulnerabilities related to the users in an organization is to inform them of possible threats. If users are aware of the ways in which attackers can gain access to a system or network, they may be less likely to volunteer information. Implementing policies related to specific actions that should or should not be taken, and requiring compliance with them, can allow the organization to take the necessary steps in order to reduce the vulnerabilities that employees or other users might bring into the equation.

Conclusion

Threats to the systems that make up much of the nation's critical infrastructure are perhaps more dangerous than those targeting almost all other facilities. The possibility exists for attacks on these systems to lead to significant physical destruction and harm. Consequently, steps should be taken to reduce the chances that these attacks will succeed. Limiting the ability for attackers to access SCADA systems remotely, implementing the proper countermeasures on these systems and networks, and educating the humans who interact with these systems can each go a long way in mitigating any potential threats.

References

IEEE. (2024). *Cybersecurity of critical infrastructure with ICS/SCADA systems*. IEEE Public Safety Technology. Retrieved November 1, 2024, from https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-systems

SCADA systems. (2024). SCADA Systems. Retrieved November 1, 2024, from https://www.scadasystems.net/