The Vunlerabilites of SCADA

By: Paul CUmiskey

Critical infrastructure such as power grids, water treatment plants, oil and gas pipelines, and transportation networks are vital for a functioning society and have become lucrative targets for cybercriminals in recent years. Attackers have been carrying out cyberattacks by exploiting the legacy software that critical infrastructure uses. Most Critical infrastructure uses SCADA (Supervisory Control and Data Acquisition) to manage and monitor their systems. SCADA systems do play a large role in mitigating cyber risks.

Vulnerabilities of Critical Infrastructure

Critical infrastructure is often targeted by cybercriminals. These malicious actors can exploit **outdated systems**, **unpatched software**, or **unsecured networks.** SCADA networks have been known to be vulnerable to **Distributed Denial-of-Service (DDoS**) attacks and **malware**.

- Vulnerabilities
    - **Outdated Systems: a security risk due to the lack of security patches and modern security protocols**
    - **Unpatched Software: Leaves systems vulnerable to known vulnerabilities**
    - **(DDoS): attack aims to make an online service unavailable to legitimate users by overwhelming it**

The Causes of the Vulnerabilities

There are many reasons for these vulnerabilities, and due to the massive amount of Critical infrastructure needed, it is very difficult to address every single one. One of the very prominent issues leading to these vulnerabilities is a **lack of network segmentation**. Many infrastructure systems still rely on legacy SCADA networks that lack proper segmentation. This gives the attackers the ability to move easily throughout the network once a system is breached via lateral movement. Another flaw that leaves critical infrastructure vulnerable is **human error.** Human error in system configuration or maintenance can introduce vulnerabilities. This is amplified due to the large number of systems needed for critical infrastructure to run,

- The Reason for Vulnerabilities
    - **Lack of Network Segmentation: allowing attackers to move laterally across the network easily after gaining initial access**
    - **Human Error: An error in configuration or blatant misconduct caused by a lack of security training**

Role of SCADA Applications in Mitigating Risks

SCADA systems are made to monitor and control critical infrastructure during their daily processes. This ensures real-time visibility and efficient management. SCADA systems play a large role in risk mitigation via their **real-time monitoring and alerts**. The data logging and analysis allow for the creation of a baseline, which helps identify abnormalities and allows for effective **root-cause analysis** after incidents. SCADA systems typically include a large amount of **redundancy and failover Systems** to ensure operational continuity in case a system fails.

Lastly, SCADA vendors have been incorporating security measures such as firewalls, VPNs, and authentication; however, many legacy systems do not have these.

- SCADA's Mitigation Techniques
    - **Real-time Monitoring and Alerts: enabling prompt detection and response to threats**
    - **Root-Cause Analysis: Helps organizations unravel the complex web of cybersecurity incidents**
    - **Redundancy and failover Systems: Provides systems and networks with fault tolerance limiting potential loss during a cyber attack**

Conclusion

While the state of critical infrastructure's security is still vulnerable to many threats, SCADA systems can help mitigate some of these threats. By enabling real-time monitoring, automation, and enhanced security, SCADA systems enhance the resilience of vital infrastructure. However, continuous improvements in cybersecurity practices and system modernization are necessary to maintain robust protection against evolving threats.

Works CIted

Alanazi, Manar, et al. “SCADA Vulnerabilities and Attacks: A Review of the State-of-The-Art and Open Issues.” Computers & Security, vol. 125, Nov. 2022, p. 103028, https://doi.org/10.1016/j.cose.2022.103028.

“SCADA Systems - SCADA Systems.” Www.scadasystems.net, www.scadasystems.net/.