Tia Warren

Vulnerabilities in Critical Infrastructure Systems

Critical infrastructure is vital to ensuring public safety, but SCADA systems are running on limited, old, unsecured hardware that has many vulnerabilities that need to be monitored.

SCADA Systems & Network Security

SCADA systems do require networks to communicate from the PLCs and RTUs to the main supervisory system so the data can be reported to operators, which opens an avenue for attack. If the SCADA network isn't properly disconnected from the internet, a country leaves itself open to remote attacks; the risk of threats like MITM, DoS, and replay attacks is especially likely to occur in cloud-based SCADA systems (Wali & Alshery, 2024). On the other hand, there's a commonly believed myth that SCADA systems are secure as long as they're not connected to the internet, but even non-ethernet communications can be attacked, like when in 2000 more than 100 Australian wastewater pumps were hijacked with a radio transmitter (Alanazi et al., 2023). Furthermore, RTUs and PLCs lack the hardware necessary for modern network encryption and send packets in cleartext; hence the push to use VPNs to transfer data (Google Doc). Some ways to reduce these risks are using software to perform frequent asset inventory, using IDSs and firewalls, creating baselines, and increasing scalability to have redundant systems (Alanazi et al., 2023). By using defense-in-depth and the monitoring capabilities of SCADA systems, operators can catch unusual activity quicker.

SCADA Systems & Access Control

As stated previously, some SCADA systems are making attempts to use VPNs, but an attacker with physical access to the network could evade security methods and wiretap or send commands across a LAN anyway (Google doc). Restricting physical access is vital to securing SCADA systems too; for example, the Stuxnet worm started from a malicious USB drive, which calls for security around removable media (Alanazi et al., 2023). By using removable media and/or having access to terminals,

attackers can unleash malware to spread throughout the system and collect data, which can then be exfiltrated after a period of time. This means insider attacks are a threat too and should be mitigated by using proper authentication and authorization methods via RADIUS servers, physical keycards, and using concepts like the principle of least privilege for employees (Alanazi et al., 2023). Another factor to consider is verifying that the hardware and firmware of devices is secure, which requires patching when available, performing maintenance on devices, doing integrity checks, and secure coding (Wali & Alshery, 2024). Secure coding can be assisted if the software is open source, such as the IEC61850 and IEC 60870 SCADA protocols, because there are more eyes available to find vulnerabilities and loopholes that need to be closed (Alanazi et al., 2023).

Conclusion

There are many threats that critical infrastructure faces, but SCADA systems can be paired with other techniques to reduce the likelihood of those threats being exploited. Disconnecting from the internet isn’t enough on it’s own; SCADA systems need to be properly monitored, evaluated, and controlled to keep systems safe. Restrict access to only those who need it, keep track of your inventory, set up ways to be alerted when something is wrong, update systems, and verify that the hardware itself isn’t modified.

Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security*, *125*, 103028. https://doi.org/10.1016/j.cose.2022.103028

Wali, A., Alshehry, F. (2024). A Survey of Security Challenges in Cloud-Based SCADA Systems. *Computers*, *13*(4). 97. https://doi.org/10.3390/computers13040097

Scadasystems.net. (n.d.). Using SCADA to Protect Critical Infrastructure and Systems. https://docs.google.com/document/d/1VnMlL2YmcW5Jg4MdDa1dt5fJpmQM0KVH/edit?usp=sharing&ouid=104340411282924033419&rtpof=true&sd=true