Ethan Massingill

Professor Davis

CSCI 570-01

04/15/2023

Power Grid Security Considerations

As technology is starting to play a vital role in every aspect of modern companies, from the smallest communication devices to large-scale industrial systems, the necessity to guard these systems increases. The rise of Internet of Things (IoT) and smart devices, such as industrial monitoring hardware, brings significant improvements including the power grid. The use of Supervisory Control and Data Acquisition (SCADA) systems has increased drastically for such tasks as remote monitoring, control of systems, and controlling distribution of power. With the benefits of the growing interconnected technology comes new challenges to keeping these systems secure from cyber attacks especially in the Power Industry due to the domino effect if a system fails leading to potential widespread blackouts which can endangers public safety. This paper will examine the impact of cyber attacks on SCADA systems in the power industry and examine the measures that can be taken to keep it secure to prevent these attacks. Likewise, we will also analyze recent cyber attacks on SCADA systems and discuss the lessons learned to prevent similar attacks in the future. This is especially relevant in today’s world as state actors have leveraged these exact attacks in wars to potentially cause great harm.

The Power Grid is one of the most important industries to protect. Everyday life is deeply connected to things that require power even in unforeseen ways. The power grid itself is an interconnected system that transcends state and local areas depending on the region. Power is needed in everyday homes for things such as refrigeration of food, cooling and heating areas, powering communication devices such as computers and cellphones, and assorted devices such as coffee makers and lighting. Likewise having reliable power is a necessity for hospital services that require equipment, emergency services such as 9-11, traffic lights, datacenters, and air traffic control systems just to name a few. Blackouts in the power gride can have drastic consequences that can affect all these areas. Likewise, a power grid failure can potentially cause a cascading effect on the power grid effecting a much larger area than just the surrounding incident for example, in 2003 the entire northeast was hit by a massive blackout that was caused by a domino effect of system failures of smaller sections failing. While the power was only out for around 2 days it effected 50 million people and cost 6 billion (Minkel). With the effects of this being so severe on modern countries it has become an attack vector by state actors in warfare. For example, in 2015 Russian hacking groups targeted the Ukraine power grid which led to widespread outages as part of the wider conflict in Ukraine since 2014 (Park, Walstrom). Furthermore, due to the need for this industry being lifeblood of others such as water, oil, and internet means that it is paramount to keep it secured and functioning properly.

Securing a SCADA system is a critical component of the power infrastructure. First it is important to understand some of the key areas in which SCADA systems are attacked. According to a study published in IEEE, the most popular attacks against the power gride include “denial of service (DoS), false data injection (FDI), insertion of worms or malware, energy theft as well as physical damage of the smart grid, e.g., causing apparatus to self-damage” (Amin). For DoS attacks this could include overflowing the communication network with traffic to jam the system up. (Amin) For FDI attacks this specifically injects false data to the control centers communication from sensors and may result in a cascading effect on systems trying to respond to the false data. (Amin) Worms and malware also play a large role where they try to wipe the software or cause it to do physical overloads of the grid to cause system damage. (Amin)

One of the first starting points to securing this system is the topology of the SCADA system itself, according to study published in *Commucations survey’s & Tutorials* “The network topology has a crucial impact on the survivability and resilience of the SCADA system.” (Pliatsios). In their study they concluded that “The point-to-point and star topologies offer more resilience against failures, compared to the bus, line, and daisy-chain. The peer-to-peer and ring offer the most resilience in case of failures, as there are multiple paths between the controller and the devices.” (Pliatsios). Another aspect they found to secure the system specifically against DoS attacks was implementing an extension of the Multipath-TCP protocol saying, “The proposed extension uses a novel stream hopping mechanism that hides open port numbers by periodically renewing the sub-flows. The experimental results indicate that the proposed protocol can effectively mitigate DoS attacks with low communication overhead.” (Pliatsios). One essential approach would also be to physically and logically isolate the public internet from the SCADA system. Doing so should be handled both by vlans, but also physically separating the systems to help foster secure environments. Anmam Sajid, a cloud computer researcher, stated that her first recommendation of the best practices for securing a SCADA system is following this policy stating that “…to segregate networks introduces security tools that surround each network and as a result effectively segregate and monitor network activities, preventing policy violations.” (Sajid). Likewise in the same study they point out another component of this is to always log and monitor the computer systems themselves stating “Activity logs are kept by nearly all computer software and devices including operating systems, network devices, applications and other intelligent programmable devices. These logs play a vital role in troubleshooting, compliance checking, forensic analysis and intrusion detections.” (Sajid). Which then in turn also bleeds into needing to secure and monitor network traffic and file integrity. Both can be early indicators that are key to preventing the spread of attacks. For file integrity they specifically suggested making sure that the Checksum methods of blacklisting and whitelisting should be handled. (Amin) Updating Firmware and patching is especially important as unpatched data could lead to vulnerabilities being exploited by the threat hackers, or unintended effects between systems. (Amin) Another important layer to this security is the training and testing of personal themselves on a frequent basis. The latest threats should be considered with this system and can reveal vulnerabilities inhouse in order to fix before the system itself is attacked this way. (Amin) Likewise educated staff is essential in combating the ever-changing threats posed from the computer security world. Access control is another important feature using the policy principle of least privilege, as it helps control exactly what users and systems have access to incase of compromise. (Amin) Finally having the proper network firewall and IDS system is essential to securing the system. (Amin) This is typically the front-line defense against such attacks and detections of them, so it is crucial to properly secure these areas. Proper placements of firewalls especially using segmentation and DMZ’s help further raise the networks security. (Sajid).

An example of a recent attack, and one of the most significant for cyber security of SCADA systems specifically in the US, occurred on the North American Electric Reliability Corporation grid in 2019. Thankfully this attack did not cause black outs and was labeled as “low-impact”. However, the attack itself took several hours to fix and is alarming for what could have happened. According to tech journalist Catalin Cimpanu the network perimeter firewalls “were mysteriously going down for periods of up to five minutes. The firewall reboots continued for hours, prompting the power grid operator to start an investigation.” (Cimpanu). However, it was discovered that the vulnerability itself being exploited was an outdated firmware on the firewall that was being attacked, causing it to reboot. The Cimpanu states that,

“The operator blamed its failure to apply the firewall security updates on the lack of a proper firmware review process to vet security updates before being deployed. Work was being done on standardizing such process, but the procedure had not been ready in time, resulting in a bottleneck of firmware updates not being reviewed and deployed.” (Cimpanu).

While not having a major intrusion this attack shows how critical it is to have proper firmware review policies and to regularly check security updates. The power grids system fully recovered after this was patched. Another incident that happened recently was in 2022 near the start of the Ukraine war a Russian state hacking agency, called Sandworm, tried to shut down key sectors of Ukraine’s power grid (Tidy). This attack was like the 2015 attack which took place during the first conflict with Russia there, however the 2015 attack caused blackouts unlike this one. Not much is known about this attack for the public, likely due to the ongoing conflict, however it used a worm payload that attempted to wipe windows and linx systems inside the power grid using the Industroyer2 malware specifically designed to destroy SCADA power grid systems. (WeLiveSecurity). It also carried the Caddywiper which is destructive malware used to wipe windows computers found within the network to try to slow down the recovery process. (WeLiveSecurity) The worm itself is unleashed to try to collect and look for SSH servers in order to spread the Caddywiper. (WeLiveSecurity) News reports state that the attack was foiled before it was able to effect the systems so it was likely detected properly. (Tidy)

As far as securing the network on packet tracer further I would start with adding more layers of firewalls separate on the Wind Turbine system and make sure that my Smart Devices are segmented properly. I would want to make sure that the protocol used for the industrial monitoring equipment uses multipath-TCP to protect against DoS attacks. I would also want to add a strong IDS system for monitoring the network. It would help also to move all public and wifi devices to a separate network disconnected from the SCADA system. Likewise including regular firmware and life cycles for all devices on the network that way older devices are maintained properly and cycled out so that they are not exploited as an attack vector like was the case with the power grid in the United States. From a network perspective I believe a cloud monitoring system with offsite monitoring could also further increase security as it would help decentralize the IDS and firewall systems away form the critical infostructure. For the network also adding secure VPN tunnels for the staff could help secure the network further.

This project was a lot of learning. Going into it I only knew a slight amount of SCADA system design and security from previous network and security class including this one. However, I believe it has really shown me just how both vulnerable and important maintaining these systems are. I think especially as we see things like the Ukraine war playing out it becomes important to see just how much the cyber security side of industry systems are for facing threats such as the Russian hacking groups. This project helped strengthen my network security implementation and thought process of placement with packet tracer and really had me dive into some of the research done in this area. I believe this is growing to become a massive important field in cyber security itself as this can have drastic consequences if a system fails compared to just a company losing money or data. Power grids themselves going out can be life or death for people and this has really allowed me to understand how securing those systems works and how important this side of cyber security is.

# Works Cited

Amin, Mahmoud, et al. “CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review.” *IEEE Access*, vol. 9, 2 Mar. 2021, pp. 38571–38601., doi:10.1109/access.2021.3063229.

Cimpanu, Catalin. “Cyber-Security Incident at US Power Grid Entity Linked to Unpatched Firewalls.” *Security*, ZDNET, 9 Sept. 2019, www.zdnet.com/article/cyber-security-incident-at-us-power-grid-entity-linked-to-unpatched-firewalls/.

“Industroyer2: Industroyer Reloaded.” *WeLiveSecurity*, 26 Mar. 2023, www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

Minkel, JR. “The 2003 Northeast Blackout--Five Years Later.” *Scientific American*, Scientific American, 13 Aug. 2008, www.scientificamerican.com/article/2003-blackout-five-years-later/.

Park, Donghui, and Michael Walstrom. “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks.” *The Henry M. Jackson School of International Studies*, 15 Mar. 2021, jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

Pliatsios, Dimitrios, et al. “A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics.” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, 2020, pp. 1942–1976., doi:10.1109/comst.2020.2987688.

Sajid, Aman, et al. “Cloud-Assisted IOT-Based SCADA Systems Security: A Review of the State ...” *SPECIAL SECTION ON THE PLETHORA OF RESEARCH IN INTERNET OF THINGS (IoT)*, IEEE Access, 21 Apr. 2016, ieeexplore.ieee.org/document/7445139/authors.

Tidy, Joe. “Ukrainian Power Grid 'Lucky' to Withstand Russian Cyber-Attack.” *BBC News*, BBC, 12 Apr. 2022, www.bbc.com/news/technology-61085480.