Solutions to SCADA Vulnerabilities

Olga Ivanova
ECS 189M: Computer Security
June 12, 2017

1 Introduction

Life today is unimaginable without electricity. While many take it for granted, electricity is a finite resource which is delivered through an enormously complex network. To allow infrastructure expansion and keep up with increasing individual demand, power grids in the United States have been automated to become the so-called Smart Grid. The Department of Energy (DOE) defines the Smart Grid as:

> . . . a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between. Its distributed intelligence, coupled with broadband communications and automated control systems, enables real-time market transactions and seamless interfaces among people, buildings, industrial plants, generation facilities, and the electric network.[1]

The Smart Grid has many benefits over traditional power grid systems. Its two-way nature enables easier integration with decentralized renewable energy sources like household solar panels.[2] Also, real-time data helps coordinate electricity delivery, reducing the likelihood and duration of shortage-related power outages.[3]

However, the Smart Grid's connection to the Internet makes it vulnerable to cyberattacks. The December 2015 attack on Ukrainian regional electricity providers has shown that sophisticated cyberattacks can disrupt automated systems for extended periods of time.[4] This paper will propose security improvements for electric grids' SCADA systems, which were the primary exploits in the Ukranian cyberattack.

2 What is SCADA?

SCADA stands for Supervisory Control and Data Acquisition. According to the National Institute of Standards and Technology (NIST), "SCADA systems are used to control dispersed assets where centralized data acquisition is as important as control".[6] They typically consist of a master server which is connected to a number of remote field units through a TCP/IP or Ethernet connection. Field units are equipped with sensors which relay data to the master server, and often include Programmable Logic Controllers (PLCs), simple computers which respond to instructions sent by the master server.[7] SCADA networks are more complex in larger systems such as electric grids, where there may be multiple levels of subservers communicating with the main server. The main server is located within a control center, which stores data and allows real-time monitoring of field units through Human-Machine Interfaces (HMIs) and engineering workstations.[7] As with servers, there can be multiple levels of control stations. All control stations are connected to the corporate enterprise network through a wide area network (WAN); this connection also allows remote access to field stations for troubleshooting and maintenance.[8]

2.1 Special Considerations

While most SCADA systems today use the same operating systems and network devices as regular corporate IT systems, their goals and constraints are quite different.[9] For example, most Internet connections are high-throughput, but allow some jitter and delay. Links between field units and SCADA servers do not require high throughput, but delay is unacceptable because sensor data is time-critical.[9] Electrical grid systems must be running nearly all of the time, which is problematic for components that need frequent updates, like computer software. Systems must also be as fail-safe and fault-tolerant as possible, so proposed changes undergo rigorous testing before being implemented.[10] Electricity providers must weigh these issues against the benefits of improved usability and corporate connectivity.

3 Vulnerabilities

Connecting SCADA to the Internet poses cybersecurity risks which may be complicated by the constraints mentioned above. Malicious access of a SCADA server can reveal all automated aspects of power generation and delivery; China and Russia have been accused of conducting such attacks to map US infrastructure in the past decade.[11] Incursions into the central server can also be used to hijack the system, or to establish a channel for further attacks.[12] Lastly, a cyberattack on SCADA can be used to add, alter, or overwrite code on connected PLCs. This type of attack is especially dangerous: it can cause extensive damage, but becomes virtually untraceable if the original intrusion went undetected. For instance, the infamous Stuxnet worm altered PLCs associated with Iranian nuclear centrifuges, and masked its effects to appear as a technical problem with the centrifuge.[13] While Stuxnet's concealment methods were very sophisticated, the Step7 PLC programming software exploited by the worm is widely used in modern industrial control systems (ICSs), and could be used in attacks on factories and infrastructure throughout the world.[13] The 2007 Aurora Test has shown that PLCs in generators can be reprogrammed to cause potentially catastrophic damage to the electrical grid.[14]

Luckily, the unprecedented 2015 attack in Ukraine did not attempt to destroy generators. However, researchers speculate that this attack was "primarily designed to send a message", and that the perpetrators might have still greater capabilities.[5] The Ukrainian cyberattack was a meticulously planned operation which probably took place over several months and featured several incursions into the SCADA network to discover its structure. In the end, the hackers remotely accessed SCADA to take down multiple substations and even reconfigured control centers' backup supply: " ...when power went out for the wider region they wanted the operators to be blind, too".[5] To complete the damage, the hackers maliciously updated the substations' serial-to-Ethernet firmware, rendering the SCADA network inoperable, and deleted critical files from the operators' workstations to render those inoperable as well.[5] While Ukrainian providers restored power manually, such attacks could be devastating in the United States, where some power grid control systems have no manual backup.[5] Moreover, this attack could be easily modified to alter PLCs, as described above.

4 Solutions

4.1 Caveats

The solutions proposed in this section will fall within certain guidelines. Firstly, they will attempt to maintain the SCADA networks' current functionality. For instance, one of the largest cybersecurity risks for modern electrical grids is the built-in capability to remotely access SCADA from the corporate network. Without remote access, serious damage could only be accomplished by directly uploading a complex standalone worm like Stuxnet. However, this proposal assumes that electricity suppliers understand the risk posed by remote access, and that they continue to provide it because its benefits outweigh the currently small possibility of a crippling SCADA hijack.

Secondly, this proposal will explore SCADA security through the lens of the 2015 Ukrainian incident. This attack was the first of its kind, which means that more threats will probably be discovered; however, the proposed changes should mitigate at least a few zero-day vulnerabilities. Also, the compromised electrical grids' security level was representative of current standards in the United States,[5] which makes this incident a good general model for infrastructure cyberattack scenarios.

4.2 Preventing Intrusions into the Corporate Network

Access to an electrical provider's corporate network can be obtained through a practice called spearphishing. This is a targeted form of phishing, where hackers create sites or send out communications which appear to be legitimate, but actually introduce malicious software. The 2015 attack employed the old-school method of hiding a Trojan in a Microsoft Word macro.[5] Since access to the wider Internet is often restricted in corporate settings, phishing attacks are likely to use email. These attacks can be prevented by educating employees about phishing, with the emphasis that an intrusion could compromise not only the employee's workstation, but the entire system. Mail filtering could also be expanded to prohibit all emails with links and suspicious attachments like word documents with enabled macros.

4.3 Preventing Credential Theft

Even if the corporate network is breached, precautions can make stealing credentials for the SCADA network more difficult. Specialized anti-virus software can search for malicious keyloggers, and outgoing network monitors can alert to anomalies, such as when a keylogger tries to relay its data to the hacker.

Another valuable approach is to strictly compartmentalize various user and group permissions, which can be especially difficult in Windows operating systems and authentication servers. Microsoft employees note that Windows Domain Controllers, which manage user access to various resources, are often configured with higher-than-necessary permissions.[15] For example, the Ukrainian power grid attackers obtained VPN credentials for the SCADA network from the corporate Windows authentication server.[5] Credential theft from authentication servers can be prevented by ensuring that all non-system administrator users can only access the server for authentication.[15]

4.4 Two-Factor Authentication

The Ukrainian SCADA servers did not use two-factor authentication, so hackers were able to enter just by obtaining VPN credentials. Multi-factor authentication with card scanners or biometric identification would create an enormous impediment for unauthorized remote users, but having several authentication layers may also hinder the system's responsiveness in emergency situations.[9]

References

[1] Roger R. Campbell, “The Smart Grid and Cybersecurity— Regulatory Policy and Issues”, Congressional Research Service (2011): 3.

[2] Eric D. Knapp and Raj Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*, edited by Joel Langill (Waltham, MA: Syngress, 2013), 7.

[3] Knapp and Samani, *Applied Cyber Security and the Smart Grid*, 11.

[4] Kim Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”, *Wired*, March 3, 2016, accessed May 20, 2017, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[5] Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”, *Wired*.

[6] Keith Stouffer et al., “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security”, National Institute of Standards and Technology Special Publication 800-82 (2006): p.2-6.

[7] Stouffer et al., “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security”, p.2-4.

[8] Stouffer et al., “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security”, p.2-7.

[9] Stouffer et al., “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security”, p.3-1.

[10] Stouffer et al., “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security”, p.3-2.

[11] Susan Gorman, “Electricity Grid in U.S. Penetrated by Spies”, *The Wall Street Journal*, April 8, 2009, access May 29, 2017, https://www.wsj.com/articles/SB123914805204099085

[12] Knapp and Samani, *Applied Cyber Security and the Smart Grid*, 26.

[13] Nicolas Falliere, “Exploring Stuxnet’s PLC Infection Process”, *Symantec Official Blog*, September 21, 2010, https://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process

[14] Mark Zeller, “Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator?” (paper presented presented at the 64th Annual Conference for Protective Relay Engineers, College Station, Texas, April 11–14, 2011).

[15] “Avenues to Compromise”, *Windows IT Center*, last modified May 31, 2017, https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/avenues-to-compromise