the Availability Digest

www.availabilitydigest.com
@availabilitydig

Are Our Power Grids Vulnerable?

December 2013

According to many studies by experts in the field, the American power grid is aging and vulnerable to collapse. The threat of natural disasters and terrorist activity make the collapse of the power system a growing likelihood.

The North American power system experienced the granddaddy of all outages in August, 2003, when an overheated transmission line in Ohio sagged, contacted trees, and failed.[1] Its load was transferred to other overheated lines, which then failed. A software bug in the monitoring system prevented the power controllers from seeing the failures. Soon, the Ohio power system called on its neighbors in the electric power grid for power and overwhelmed them to the point of failure. The failures cascaded until the entire Northeast U.S. and parts of Canada were without power for two days.

Studies show that from 1965 to 1988 – a period of 20+ years – there were three major failures of the nation's power grid system. From 1989 to 2009 – a 20 year period – there were 54 such failures. Most of these failures were weather related.

However, the danger of weather is now being compounded by the danger of cyberattacks. Thousands of cyberattacks hit the U.S. power grids every day. So far, they have been stopped by firewalls and other intrusion-prevention systems. However, a pair of researchers has discovered a vulnerability in the power monitoring and control systems that could be exploited to take down major portions of the power grid in the U.S. and elsewhere. In addition, a recent exercise called GridEx II demonstrated the damage that determined terrorists could inflect on power systems.

The DNP3 Protocol Vulnerability

The security vulnerability has to do with an old serial communications protocol, DPN3, that is still in active use in power monitoring and control systems. These systems are called Supervisory Control and Data Acquisition (SCADA) systems and are in common use to link supervisory personnel in control centers to remote power generation and transmission facilities and to electric substations that distribute the power. Via the SCADA systems, controllers can determine the state of every device in the field and can execute controls to manage the power flow and to work around failures before a repairman can be dispatched.

A SCADA system comprises a master station located at the central control facility and Remote Terminal Units (RTUs) located in the field. The master station periodically polls each of its RTUs to determine changes in the state of the power system. If it detects a problem – for instance, an increase in power demand approaching the capability of the power system – it can execute commands to mitigate the

[1] The Great 2003 Northeast Blackout and the $6 Billion Software Bug, *Availability Digest*: March, 2007. http://www.availabilitydigest.com/private/0203/northeast_blackout.pdf

problem. For instance, in this case, the master station (either automatically or under manual control) might command a brownout.

The communication system between the master station and its RTUs must be very robust and reliable. In the earlier days of SCADA systems, telephone lines and microwave transmission systems were used for communication. One problem was that every vendor had its own protocol, so that a master station manufactured by one vendor could not communicate with RTUs from another vendor.

To solve this problem, in 1993 the DNP3 (Distributed Network Protocol) was adopted by the industry. The protocol was designed to provide reliable communications in the adverse environments to which the electric utility systems are subject. The DNP3 protocol is used by most of the top five power utilities.

However, it was not designed to be secure from hackers. Malware was unknown at the time. As this security problem became recognized, much work was done to add Secure Authentication to the DNP3 protocol. However, the implementation of these features is not yet very widespread. Rather, cybersecurity regulations have focused on IP communication protocols that are being used by newer SCADA systems. DNP3 is generally excluded from these regulations.

A pair of researchers recently discovered the vulnerability in the DNP3 protocol. Via this vulnerability, they could crash the RTU software that monitors a substation. The controllers in the central control facility would then be blinded from knowing the status of the substation. The researchers further determined that an attacker at an unmanned substation could crash other substations, thus causing a widespread power failure.

To determine the extent of this vulnerability, the researchers tested the DNP3 communication software of sixteen vendor systems. They were able to break every one. In the case of one vendor, the researchers found that they could introduce malware into the RTU from afar, which would allow the RTU to be infected with other malware, such as Stuxnet, which disabled Iranian centrifuges in 2010.[2]

The researchers compiled a report about the DNP3 vulnerabilities and submitted it to the Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), whose responsibility it is to notify vendors of vulnerabilities and to issue public advisories.

Disappointedly, DHS has been slow to respond. It took ICS-CERT four months to issue advisories, and it has as yet to issue any mandates. During this time, the researchers have found the vulnerability in nine additional vendor systems.

Some vendors have eliminated the vulnerability. However, many systems with the vulnerability are still in service.

Though the researchers currently charge for their security test software, they have said that they will release a free version in March, 2014, so that all vendors can check their systems for the vulnerability.

GridEx II

Meanwhile, the power utility industry is taking the possibility of terrorism causing major power failures very seriously. Recently, it engaged in an industry-wide exercise dubbed GridEx II. A crew of about forty specialists from the North American Electric Reliability Corporation (NERC), operating out of a facility in Washington, D.C., led the attacks. NERC is the institution that oversees and regulate\s the reliability of the North American electrical grids.

NERC injected computer viruses into grid control systems, simulated bombed transformers, and substations, and knocked out dozens of power lines. DDoS (Distribute Denial of Service) attacks were

[2] Stuxnet – The World's First Cyberweapon, *Availability Digest*; March 2011.
http://www.availabilitydigest.com/public_articles/0603/stuxnet.pdf

also made on several control computers. The tests involved 210 U.S. utility companies as well as some in Mexico and Canada that are part of the U.S. power grid. 10,000 electrical engineers, cybersecurity specialists, utility executives, and FBI personnel grappled with the unseen enemy for 48 hours and tried to keep the power grids functioning.

Though no actual operating equipment was affected, the simulated result was not good. Control computers were tearing the system apart. DHS's National Cybersecurity and Communications Integration Center specialists took calls from electric industry technicians all over the country to assist them in recovering from cyberattacks. Hundreds of major transformers and transmission lines were damaged or destroyed. Tens of millions of Americans were out of power. The viruses injected into the control computers kept technicians in the control centers from knowing the status of critical equipment, requiring the dispatching of several trucks with linemen to investigate. In many cases, attempts by the linemen to enter power facilities were stymied by police officers who had locked down locations because of shooters.

All communication by email or phone was logged to assess whether participants could reach other parties such as police, cybersecurity centers, and other power companies and provide the appropriate information. The game controllers purposely injected some "fog of war" confusion into the communications. In an earlier test two years ago, it was found that communication was good with neighboring power systems, but it was poor with national organizations. Therefore, it was difficult for anyone to get an overview of what was happening. It will take several weeks of analysis to determine whether communication has improved.

The purpose of the exercise was to pose problems that were hard to solve and to expose areas that needed improvement. The drill participants would not disclose the locations that were attacked for security reasons. The chosen sites were those that insiders thought would be vulnerable.

Summary

The rate of major power outages is increasing as the U.S. power system has aged. Though weather has classically played the major role in power outages, terrorism is becoming a greater concern. The GridEx II exercise has demonstrated that terrorist attacks, both physical and cyber, can today cause major damage to the electric grid. This concern is compounded by the discovery of security vulnerabilities such as was found in the DNP3 protocol in installed equipment

It is probable that power utilities around the world are subject to these same challenges. It is incumbent upon all utilities to gage their exposure to terrorism and to introduce appropriate protective policies.

Acknowledgements

The information for this article was taken from the following sources:

Electrical Grid is Called Vulnerable to Power Shutdown, *N.Y. Times*; October 18, 2013.
Apocalypse: Threat of massive grid shutdown increasing in face of terrorism, natural disasters, *Gazette*; November 11, 2013.
Attack Ravages Power Grid. (Just a Test.), *N. Y. Times*; November 14, 2013.