Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack

Jonathan Stidham

Can Hackers Turn Your Lights Off?
The Vulnerability of the US Power Grid to Electronic Attack
A GSEC Practical Assignment (Version 1.2e)

Introduction

There is now no reason to doubt that presently there are individuals, groups, and nations that seek actively and presently to do harm to the United States. We have seen enough evidence of this in the last few weeks with the attacks on the World Trade Center, the Pentagon, and the apparent attempt to damage or destroy either the Capitol or the White House. [1]

One of the lessons we need to take from this tragedy is that it is absolutely necessary for us to protect the critical infrastructures of the United States.

One of the most important aspects of our critical infrastructure is the National Power Grid. Without electrical power, just about everything in our Information Age society and economy goes dead: respirators, heaters, air conditioners, and refrigerators in hospitals and homes, perishable food supplies in markets, stock trading on Wall Street, financial transfers between banks, and much more, including, of course, the lights, everywhere from Manhattan to Watts.

Let me give a couple of examples. On November 9, 1965, a blackout occurred that knocked-out power to 30 million people in the Northeastern United States and Ontario, Canada for as long as thirteen hours. Runway landing lights went dark, people were trapped in elevators, traffic snarled at busy intersections that were suddenly left without signals. [2]

On May 16, 1996, an improper setting on a high-voltage circuit breaker at a single substation caused another outage. This resulted in an 8-hour blackout affecting 290,000 in Delaware, Maryland, and Virginia, but was estimated to have cost regional businesses as much as $30 million. On August 10, 1996, all major transmission lines between Oregon and California lost power. This outage affected 5.6 million users for up to 16 hours in 10 western states, and was caused by a single tree branch brushing a high-voltage transmission line in Oregon. [3, 4]

These outages (and many others) occurred without any intentionality. Indeed, what might be accomplished when intentionality is present?

Until now, we Information Security professionals have oriented our defensive strategies against the intentional electronic havoc wrought by disgruntled employees, recreational hackers (skilled and "script-kiddie"), and the relatively low-key "hacktivists" (hacker-activists trying to make a political statement). There has been good reason for this. A new PricewaterhouseCoopers survey indicates that "global corporations suffered more than $1.39 trillion in lost revenue due to security breaches this past year. A majority of those losses stem from the rapid growth in computer viruses and denial-of-service (DoS)

attacks, which together account for 60 percent of lost productivity among thousands of survey respondents." [5] These losses and the attacks causing them certainly deserve our attention.

But whether they were in our sights before or not, we should now seriously broaden our threat scope to include international terrorists. For whether they are working independently, in larger networks, and/or with the sponsorship of foreign governments, terrorists are a force with which we must reckon. We ignore this responsibility at a great potential cost.

According to a September 19, 2001 LA Times article, "In the Internet Age, when communications speed across national boundaries in nanoseconds, terrorist groups are winning the cyberspace battle, say intelligence and security experts." [6] This article goes on to describe that terrorists (including groups linked to Osama Bin Laden, the primary suspect in the New York and Washington attacks) openly solicit funds through their own websites. They make effective use of encryption to mask their communications. And they are interested in our defensive information.

In 1998, apparent terrorist/hackers tapped into a NASA/JPL computer in Pasadena and accessed data about the commercial air traffic system. The FAA then had to shut down communications for several live flights. Vulnerable information included the configuration of GPS navigation satellites (which could allow them to jam the system during a war), information on Stealth aircraft (plane locations, how they operated in difficult weather conditions), etc.

Tom Talleur, then chief of NASA's cybercrime unit, eventually traced the hackers to computers in the Persian Gulf area.

The Defense Department admits to hundreds of successful attacks on its networks in recent years. Quoting Brian Murphy, who left the Defense Department's network security unit last year to work for the security firm Riptech, the above article states that "No computer hacker has yet shut down an electrical grid or opened a dam." But then it quotes Murphy as saying:

"But our nation's critical infrastructure is both connected to public networks and vulnerable," he added. "It's open to terrorists, operating from anywhere in the world, with the motivation and skills to wreck havoc." [6]

If hackers from other countries (terrorists and others) were interested in information on our GPS satellites, Stealth aircraft, and our commercial aircraft, it would be foolish to think they would not be interested in our critical infrastructures, including the National Power Grid. So, the scope of entities that constitute a threat to our IT systems (and our critical infrastructure) must certainly now expand to include terrorists, whatever their country of origin (including the US).

But, regardless of whether an attacker is a terrorist bent on destroying the US, a recreational hacker, a disgruntled employee, or a hacktivist, protecting our critical infrastructure, including and especially our Power Grid, is an absolute necessity.

The issue before us in this paper, then, is the potential and/or actual vulnerability of our National Power Grid, or portions thereof, to electronic attack. Has the U.S. power grid been hacked yet? I will address this question first.

Has the Power Grid Been Hacked?

Has the power grid ever been hacked? Well, this depends upon what one means by "hacked." If by this one means, "Has an electric power utility's networks ever been penetrated by hackers?" the answer is a definitely yes.

Schweitzer Engineering Laboratories (SEL), in their white paper "Safeguarding IEDS, Substations, and SCADA Systems Against Electronic Intrusions" [7] documents the following electronic intrusions:

1. Several times, hackers have attacked IT systems in electric utilities looking for credit information
2. A radical environmental group was caught hacking into an electric utility IT system at and undisclosed U.S. location
3. At another undisclosed U.S. electric power company, hackers subverted a company server in order to play games, eventually consuming 95 percent of the server's resources, creating an essential Denial of Service attack on the servers legitimate users
4. [Though this is not an electronic intrusion, it is worth noting here for its potential to create one.] A disgruntled ex-employee of an electric utility in Texas posted a note in a hacker journal indicating that his insider knowledge of the system could be used to shut down that region's power grid.

So, it is clear from these examples (and others to be mentioned below), that U.S. electric power utilities have been "hacked" in that their networks have been penetrated and mischief has been done. But have hackers ever actually shut down a part of the power grid, that is, cause a power outage? That question is harder for those of us outside the electric power industry to answer.

The power industry does not acknowledge that hackers have ever disrupted the US power grid to date. [4] Of course, lack of acknowledgement is not the same as an explicit denial. Underreporting or non-reporting of hacking incidents is not uncommon. A survey conducted jointly between the Computer Security Institute, the FBI, and the International Computer Crime Squad indicates that less than 17 percent of 428 respondents would report an electronic intrusion if they thought they had experienced one. And most of the respondents, 70 percent, said they feared bad publicity. [4]

This may indeed be the case with the 1995 Dallas "Phonemasters" case. [2] The Phonemasters were a group of phone "phreakers" who worked various scams across the country. A Wall Street Journal report on this case included a casual paragraph-eight disclosure that the three hackers involved "had access to portions of the national power grid." No charges related to this were filed against the defendants, who admitted other crimes. The prosecutor on the case, former Assistant U.S. Attorney Matt Yarbrough denies it. "I don't remember any example of them accessing the power grid." [2]

The electric power industry is not commenting on the question. "When it comes to saying something specific about whether anything has happened on the electric system, I don't answer," said Eugene F. Gorzelnik, the Communication Director for NERC, the North American Electrical Reliability Council. When he was asked to what degree the power grid is vulnerable to such an assault, Gorzelnik said, "I just won't answer that question. It's not something that we want to talk about in the press. It doesn't serve any useful purpose." [2, 8, 9] While Gorzelnik's statement about whether such disclosure serves any useful purpose is debatable, what is certain is that his comments were not a denial.

But, in either case, since electric utility systems have been penetrated, attacks on the power grid are certainly of realistic concern. But can the U.S. Power Grid truly be taken down?

The NSA's "Eligible Receiver" Exercise

In June of 1997, the NSA, Pentagon, FBI, etc. worked jointly on an exercise called "Eligible Receiver". This exercise was designed to see what a coordinated cyberattack could do to US military functions in the Pacific Theater and with US national infrastructure. NSA "hacker" teams posed for the exercise as North Korean cyberwarriors trying to influence US policy in the Pacific, and attacked Unclassified military computer systems throughout that area, the US 911 Emergency system, and the US Power Grid.

The hacker teams worked from different physical locations, inside and outside the US. They used COTS (Commercial Off The Shelf) software and hacker tools freely available on the Internet. They were forbidden, of course, from actually disrupting any critical infrastructure elements, but were tasked to show that they could do so.

So what were the results of this exercise?

Deputy Secretary of Defense John Hamre, speaking about Eligible Receiver in a speech in July of 1998, said: "A year ago, concerned for this, the department undertook the first systematic exercise to determine the nation's vulnerability and the department's vulnerability to cyber war. And it was startling, frankly. We got about 30, 35 folks who became the attackers, the red team … We didn't really let them take down the power system in the country, but we made them prove that they knew how to do it." [10]

Senator John Kyl, in a November 1998 interview on cyberterrorism conducted by the United States Information Agency (USIA), said about the exercise, “Well, [cyberterrorism is] surprisingly easy. It's hard to quantify that in words, but there have been some exercises run recently. One that's been in the media, called Eligible Receiver, demonstrated in real terms how vulnerable the transportation grid, the electricity grid, and others are to an attack by, literally, hackers -- people using conventional equipment, no "spook" stuff in other words.” [10]

Another Defense Department official is quoted in the Washington Times as saying, "The attacks were not actually run against the infrastructure components because we don't want to do things like shut down the power grid …. The referees were shown the attacks and shown the structure of the power-grid control, and they agreed, yeah, this attack would have shut down the power grid." [11]

“Eligible Receiver” then clearly indicates that our power grid is vulnerable. Does the electric power industry admit that this is at least a possibility?

A majority of utility industry insiders in the National Security Telecommunications Advisory Committee Information Assurance Task Force agreed that “an electronic attack capable of causing regional or widespread disruption lasting in excess of 24 hours is technically feasible. The source for such an attack could come from within the utility or from an external source.” [4]

Anjan Bose, a power-grid expert and dean of the College of Engineering and Architecture at Washington State University, speaking about electronic intrusions says, “You can black out whole cities.” Once inside the control system, “you have access to open the switches for the transmission lines … You can open the switches for the big generators. Even random switching without someone knowing the consequences could be devastating.” [12]

So, the electric power utility industry professionals and experts, while denying any successful hacker attacks have resulted in power outages, clearly admit such attacks are possible, and that their systems are vulnerable to attack.

The threat or likelihood of an electronic attack is also on the rise.

Power Grid Threats on the Rise

The 1997 Information Assurance Task Force stated that “Physical destruction is still the greatest threat facing the electric power infrastructure. Compared to this, electronic intrusion represents an emerging, but still relatively minor, threat.” [4]

Last year, 2000, another SEL white paper put the situation in slightly different terms. “Although physical destruction is still the greatest threat to the North American electric power grid, the threat of electronic computer-based intrusions and attacks is growing and needs to be addressed by the electric power industry.” [13]

A number of factors contribute to this increasing danger: [12, 13]

1. The shift from proprietary mainframe-based computer control systems to distributed systems using open protocols and standards, and the expanded use of public protocols to interconnect previously isolated networks, i.e., PC's and UNIX machines running TCP/IP.
2. Pressures within the industry to downsize, streamline, automate, and cut costs to maintain profit margins.
3. FERC (Federal Energy Regulatory Committee) filings 888 and 889, which require that utilities provide open access to transmission system information. Much of this information is available for anyone to view via the Internet.
4. Increased access and interconnectivity to remote sites through the use of dial-in modems and the Internet.
5. Instability in the electric utility job market, caused by competition and deregulation.
6. Increasing incidents of international and domestic terrorism targeted against North America.
7. Increasing numbers of countries with government-sponsored information warfare initiatives.
8. Rapid growth of a computer-literate population.
9. Widespread availability of hacker-tool libraries.
10. Formation of dozens of line energy trading networks where buyers and sellers manage real-time sales of electricity over the Internet, as a part of deregulation.
11. Increase in connectivity between utility administration networks and power-grid control networks.
12. Movement towards standardization of software, such as Microsoft and Sun operating systems and application software.

All sides are admitting vulnerabilities in our electric power systems, and that the threat of exploiting those vulnerabilities is increasing. When then are those areas of vulnerability?

Specific Areas of Vulnerability

The National Security Telecommunications Advisory Committee Information Assurance Task Force quantifies the vulnerabilities to electric utilities and the power grid in three main areas: [4]

a. The Control Center,
b. The Substation, and
c. The Communications Infrastructure

First, we will look at the Control Center. The Control Center monitors a utility's generating plants, transmission and sub-transmission systems, distribution systems, and customer loads. It primarily functions to provide centralized monitoring of power system operations, to retain historical data, and to allow for the manual and automatic control of field equipment.

The Control Center's vulnerabilities lay in its links to Corporate MIS systems, to other utilities or power pools, and to supporting vendors. Remote maintenance and administration ports can also access control Centers, creating another vulnerability. Whenever a utility's Energy Management System (EMS, which controls the flow of power through that utility's section of the power grid) is connected to a Local Area Network, there is a danger of hackers gaining access to the power grid.

This danger may be the result of the utility itself connecting its own LAN to the EMS. It may come from their connecting to the EMS of another utility (whose systems are connected to their corporate LAN's and so on). It may come from a vendor that is accessing the utility's EMS for support or maintenance purposes (and whose LAN is connected to the Internet). All these access points potentially have the same vulnerabilities as any LAN connected to the Internet, giving determined hackers opportunities with which they are quite familiar.

The danger may also come from the company's own remote maintenance and administration ports, which may enable workers to dial-in to troubleshoot problems, do other administrative tasks, or even operate EMS applications. Although some of these dial-in modem pools provide limited operational options, and have access control with token-based authentication systems, others have only minimal protection. Phone "phreakers" could indeed have a field day if they know the dial-in numbers and have time to play, especially if they have any knowledge of power systems.

Second, there are substation vulnerabilities. A substation serves as a clearinghouse for power as it is stepped down from the high voltages used to transmit the power across the service area and then directed to distribution systems. Power is then delivered to residential and commercial customers. In order to provide better service to customers, reduce staffing requirements, etc., the electric power industry is automating substation operations with remote terminal units (RTU's), and a variety of intelligent electronic devices. Both the RTU's and the digital programmable devices have vulnerabilities associated with them.

RTU's collect data for the Control Center and operate as a clearinghouse for control signals to transmission and distribution equipment. Some of these RTU's have maintenance ports that can be accessed even without required dial-back connectivity. Hacker access to an RTU could result in commands given to substation equipment or reports of spurious data to the Control Center. If an RTU is knocked out, this could have significant impact on customers or systems connected to this substation.

Similarly, if a hacker dials in to a digital breaker, he/she could reset the device to any of six levels of protection, two of which might either destroy the device or cause it to shutdown for self-protection. A number of utilities visited by the Information Assurance Task Force had no type of security or access control at all on these devices. In either case, though, only a minor alarm might be generated, even though the impact of these actions might be tremendous.

Third, there are vulnerabilities in the communications infrastructure, which is used for communication between control system elements. This communications infrastructure is composed of private microwave radio and private fiber networks, and public networks for communication between control system elements. Aside from the damage of physical attacks, the private network communications can be jammed or intercepted. The Internet contains sites describing how to assemble an inexpensive microwave-jamming unit.

Public network traffic constitutes about one-third of electric utility control communications. Because of vulnerabilities associated with public network, utilities in general take greater risk-mitigation measures here, including requiring diverse routing in their leased-line contracts, providing for redundant transmission media, etc. Fortunately, this reduces the vulnerability associated with using public communication networks.

Fortunately, a successful attack on the communications infrastructure would be mostly a nuisance. If this happened, the utilities would send workers out to the key sites and have them report operating data back to the control center via cell phones and mobile radios.

The biggest fear of utilities, though, is an attack on both the electric power control system and the communications infrastructure simultaneously. This was described by one utility official as a "nightmare scenario", since all means of coordination between the control center and generation and transmission elements might be lost. [4]

We now know the general areas of vulnerability in electric power systems. How might these vulnerabilities be exploited? And how easy would it be?

Attack Scenarios

According to the National Security Telecommunications Advisory Committee Information Assurance Task Force, open sources (including the Internet, FERC filings, electric industry publications, and regional maps) would provide sufficient information to enable hackers to identify the most heavily used transmission lines and most critical substations in the power grid. Relatively simple techniques could be used to locate the appropriate dial-in ports to these points and modify settings to trigger an outage. At that point, only a detailed review of the log or eliminating all other factors would result in the detection of this type of attack. [4] This means that a "script-kiddie" that has done his homework could indeed conceivably take down at least a section of the power grid.

The following are potential attack scenarios postulated by SEL, in a previously mentioned white paper. [7] They illustrate different ways that an electronic intrusion might be accomplished toward the end of attacking the power grid.

Attack Scenario #1: Using insider information, a disgruntled employee or ex-employee, with a grudge against a generation facility or T&D provider, accesses protective equipment (either physically or electronically) and changes settings. The results are that

the equipment either (a) fails to operate when it should, causing bus, line, or transformer damage, or (b) operates when it shouldn't, causing service interruption.

Attack Scenario #2: Using a war-dialer (a program to control a modem for automated attacks), a disgruntled customer scans hundreds of phone numbers above and below the utility's publicly available phone numbers, looking for answering modems. When a connection is found, multiple returns, question marks, "HELP," and "HELLO" are entered to probe the connection and look for clues as to the kind of connection. Once a login dialog is acquired, the intruder uses social engineering to determine login information, or launches a dictionary-based or brute-force password attack. When the connection is complete, the intruder is "inside" the IED, controller, or SCADA system. Data can then be altered or destroyed, communications can be blocked or rerouted, and settings can be changed deliberately or randomly. The state of the equipment and service is in jeopardy.

Attack Scenario #3: A disgruntled customer, ex-employee, foreign agent, or terrorist uses a port scan or ping-sweep program to identify active system ports and/or network IP addresses belonging to a public utility. When an active connection is found, multiple returns, question marks, "HELP," "HELLO," and "LOGIN" are entered to probe the connection and look for clues as to the kind of connection. Once a login dialog is acquired the intruder uses insider information, social engineering, or a password attack to gain access to the system. Once again, all data, communications, and settings are vulnerable, so equipment and service is jeopardized.

Attack Scenario #4: An employee with access to computer information services is duped into installing or running a computer "game" or otherwise seemingly innocuous application by a friend, ex-employee, supervisor, vendor, or virtually anyone with legitimate connections to the employee's company. The installed computer application contains a Trojan horse program that opens a backdoor into the computer network. The inventor of the Trojan horse program is automatically notified that the backdoor is open, gains access to the system to retrieve and exploit inside information enabling him or her to access SCADA systems and protective equipment. The computer information system (e.g., control commands and metering data) and all systems subordinate to it are now in jeopardy.

Attack Scenario #5: An employee, inside service provider, or vendor representative with privileged information is approached by an unscrupulous competitor, foreign agent, or terrorist. The employee is bribed or duped into sabotaging systems and settings or creating access mechanisms the agent could use for subsequent activities that jeopardize equipment and services.

Attack Scenario #6: An unscrupulous competitor, foreign agent, terrorist or network service provider uses public information and social engineering to obtain network traffic patterns for TCP/IP packets moving between supervisory stations and remote protective equipment or metering equipment. A network analyzer or "sniffer" is attached to the network line to show the content of all data packets between the supervisory and remote

equipment. The unencrypted data packets contain control and settings information that can be used in subsequent attacks on either the SCADA system or the protective equipment.

In evaluating the "worst-case" scenario, if more than one individual directed attention to more than one section of the power grid, the US could really be in trouble. SEL, in the same white paper, states, "Finally, note that the most insidious form of electronic attack–a coordinated many-on-many attack–is also the hardest to diagnose and establish culpability. A few individuals determined to disrupt power services could launch a coordinated attack on electric power systems, using the same techniques that crippled U.S. E-commerce sites in February 2000." [7] The US could be attacked from multiple sites across the world, experience at true Distributed Denial of Service attack on the power grid, and might never be able to determine (at least electronically) who initiated the attack.

Vulnerability Summary

We have now seen that the national power grid is indeed vulnerable. This vulnerability is increasing as deregulation and market forces lead power companies to do away with proprietary systems in favor of COTS implementations, and to connect administrative and organizational networks with the networks that coordinate the flow and distribution of electricity. Present points of vulnerability include access through the Internet or modems into the utilities' LANs and thus their power control systems, dial-in access to substation RTU's and digital programmable devices, and communication interruption via the utilities' reliance upon easy jammed or interrupted private networks or public networks.

So what is to be done about all this? What are the options for vulnerability mitigation?

We will now take a look at a recent attempt to hack into the California power system and use it as an illustration of what not to do, and then proceed to describe what electric utilities can do to prevent, or at least minimize, electronic intrusions.

An Analysis of the Cal-ISO Brake-in

Cal-ISO, the California Independent System Operator, balances in the flow of electricity across the state of California, and makes power purchases to match demand (sometimes at the last minute). This is the organization responsible for assisting the utilities in avoiding blackouts. The California power grid for which Cal-ISO is responsible is tied to the transmission grid for the entire Western United States.

Several months ago, at the height of California's present energy crisis, hackers attacked the computers at the headquarters of Cal-ISO, which oversees most of the state's electricity grid. These attacks lasted for at least 17 days, beginning as early as April 25 of this year, and were not detected until May 11. The attacks were ongoing while rolling blackouts swept the state on May 7 and 8, affecting over 400,000 utility customers. Cal-

ISO officials insist the hacking attacks had nothing to do with the blackouts suffered in the state. "It did not affect markets or reliability," according to Stephanie McCorkle, a Cal-ISO spokeswoman. [14]

But an LA Times source, familiar with the attack and the ISO's internal investigation, said, "This was very close to being a catastrophic breach." [14]

The details of this incident read like a virtual "How **Not** To" list of security tips. According to this internal ISO report, investigators discovered that hackers gained access to two Solaris Web servers, systems that were part of a development network. This development network was not behind the ISO network's firewall; the servers were connected directly to the Internet. The systems were not hardened; in fact, they were installed with the default settings, and were thus vulnerable to all sorts of attacks. No audit logs were sent to other systems; they were only available on the systems themselves. The hackers gained access, apparently, through a Solaris vulnerability that was discovered in March of this year.

After gaining access to these web servers, the hackers installed an elementary "root kit" (a set of tools designed to gain root access). Investigators found evidence that the hackers were trying to compile software to get them from this development network into the more sensitive areas of Cal-ISO's network. But since the local logs were the only source of information (and could easily have been modified), investigators were not able to discover further details. [15]

So what can we learn from this event? How could it have been prevented? And how can other utilities avoid not just this scenario, but protect their systems from attack and thus avoid hacker attacks on the U.S. power grid?

Best Practices for the Protection of the Power Grid

Obviously, the Cal-ISO attack in its apparent form was possible because the Cal-ISO system administrators (and possibly the network engineers who designed the network) did not follow some very fundamental security best practices. They did not harden servers that were attached to the network. They placed these systems outside the firewall. Audit logs were not sent to a centralized auditing server, or at least to other locations, and could thus be easily altered on the compromised machines. A comprehensive approach is needed to address the security concerns of the electric power industry.

An accepted, industry-wide approach to information security known as "Defense in Depth" provides the electric power industry the guidance needed to secure their systems. This approach, developed and refined in the IT world as a whole, now applies fully to utility networks, as they have embraced the technology of IT world (Microsoft and Sun systems and applications, communicating via TCP/IP).

A full description of the Defense in Depth strategy is beyond the scope of this paper, but is detailed in an NSA white paper, "Defense in Depth A Practical Strategy for Achieving

Information Assurance in Today's Highly Networked Environments." [16] Defense in Depth seeks to achieve information assurance through application of the following security services:

1. Availability
2. Integrity
3. Authentication
4. Confidentiality, and
5. Non-repudiation

These services are applied based upon the Protect, Detect, and React paradigm. This means that organizations do not simply set up protection mechanisms. They expect attacks to occur, and include attack detection tools and procedures that allow them to react to and recover from these attacks.

This strategy also seeks to balance three primary elements to achieve information assurance:

1. People
2. Technology, and
3. Operations

The People focus requires appointment of a senior level manager (like a Chief Information Officer), effective Information Assurance procedures, assignment of roles and responsiblities, commitment of resources, and the training of critical personnel (such as users and system administrators). It also includes physical and personnel security measures to control and monitor access to facilities.

The Technology focus includes many things, from security policy to configuration management to intrusion detection products that have been validated by a reputable third party. It means Defense in Multiple Places, ensuring that all points and classes of attacks are addressed, whether from inside or outside, and have protection mechanisms deployed to face them. This means using encryption and traffic flow security internally to resist passive monitoring, and Firewalls and Intrusion Detection Systems (IDS) to resist active attacks on the network.

The Technology focus also means Layered Defenses, because it is recognized that all technologies have weaknesses. So the wise network planner employs multiple layers of defenses, such as pairs of nested Firewalls and IDS, for critical LANs. This approach should also employ strong key management and public key infrastructures that support all of the above technologies. All servers should be hardened with industry-standard best practices before they are installed on the network.

For the electric utility industry in particular, in light of the extensive use of remote management of switches and RTU's, the strongest modem security available should be implemented, including encryption. Telecom Firewalls should be installed, so that calls coming from unauthorized numbers are tracked and immediately dropped. War Dialers should be used to track whether employees are installing modems on their computers,

giving an open door to outsiders (depending on the modem's configuration). VPN technology should be extensively used as well for access to corporate LAN's. Access by other utilities, vendors, on-site employees and telecommuters should be audited with audit-reduction tools, so logs can be easily reviewed on a daily basis.

The Operations focus keeps the security posture strong on a day-to-day basis. It includes updating the security policy, logging any changes to configuration baselines, installing all required service packs and virus updates, and updating access control lists and user accounts according to staffing changes. It also includes performance of security assessments and penetration tests, both by internal and external personnel, to assess the continual "security readiness". It should also include dry runs of recovery from disasters and tracking of attacks.

Conclusion

In this paper I have addressed the question of the vulnerability of the U.S. power grid. I have addressed longstanding and immediate threats to the power grid, and have shown why these threats are increasing. I have detailed the specific areas of vulnerability, and have suggested an overall strategy to deal with these areas called "Defense in Depth." I have also described some specific actions for the electric power industry appropriate for these vulnerabilities.

The question of the U.S. power grid is not something merely of interest to the electric power industry, however. It is something relevant to every U.S. citizen, and because of the interconnectedness of the world economy, the entire world. Because of this, those of us outside of the power industry must make sure that utilities are acting to secure their systems. This means all of us must focus political attention and influence (calling senators and representatives) to make sure that the utilities are following through on security measures appropriate for critical infrastructures.

References

1. “September 11: Chronology of terror,” CNN On-line article, http://www.cnn.com/2001/US/09/11/chronology.attack/index.html

2. Poulsen, Kevin, “Lights Out,” May 25, 2000, http://www.landfield.com/isn/mail-archive/2000/May/0191.html

3. Hotz, Robert Lee, Clifford, Frank, “A Glitch in the System”, The Los Angeles Times, Aug. 14, 1996

4. The President’s National Security Telecommunications Advisory Committee Information Assurance Task Force Electric Power Risk Assessment, March 1997, http://www.securitymanagement.com/library/iatf.html

5. “Viruses Drive Breaches to Nearly $1.4 Trillion in Costs,” Security Wire Digest, Vol. 3, No. 73, September 24, 2001, http://www.infosecuritymag.com/current_daily.shtml#2d

6. Piller, Charles, Wilson, Dave, “The Terrorists are Winning the Cyber War,” Los Angeles Times, Sep. 19, 2001, http://www.latimes.com/templates/misc/printstory.jsp?slug=la%2D091901techspy

7. Oman, Paul, Schweitzer III, Edmund O. Robert, Jeff, “Safeguarding IEDS, Substations, and SCADA Systems Against Electronic Intrusions,” Schweitzer Engineering Laboratories, WA, USA, 2001, http://www.selinc.com/techpprs/6118.pdf

8. Simons, John, “Unplugged! The Biggest Hack in History,” Wall Street Journal Interactive Edition, Oct. 1, 1999, http://www.zdnet.com/zdnn/stories/news/0,4586,2345639,00.html?chkpt=hpqsnewstest

9. U.S. Department of Justice, United States Attorney's Office, Northern District of Texas, Dallas, TX, September 16, 1999, http://www.usdoj.gov/criminal/cybercrime/phonmast.htm

10. The Crypt Newsletter Archives, http://www.soci.niu.edu/~crypt/other/eligib.htm

11. Gertz, Bill, “Eligible Receiver,” The Washington Times, April 16, 1998, http://csel.cs.colorado.edu/~ife/l14/EligibleReceiver.html

12. Piller, Charles, “Power Grid Vulnerable to Hackers,” Los Angeles Times, Aug. 13, 2001, http://www.latimes.com/business/la-000065693aug13.story

13. Oman, Paul, Schweitzer III, Edmund O. Frinke, Deborah, “Concerns about Intrusions into Remotely Accessible Substation Controllers and SCADA Systems,” Schweitzer Engineering Laboratories, WA, USA, 2000, http://www.selinc.com/techpprs/6111.pdf

14. “Hackers Victimize Cal-ISO,” Morain, Dan, Los Angeles Times, Jul. 9, 2001, http://www.latimes.com/news/la-000047994jul010.story

15. Lemos, Robert, “Humans Opened the Door for Calif. Power Hack,” ZDNet News, Jul. 13, 2001, http://www.zdnet.com/zdnn/stories/news/0,4586,5092679,00.html

16. “Defense in Depth A Practical Strategy for Achieving Information Assurance in Today’s Highly Networked Environments,” [Note: This link was denied by my company’s content filter, but should be visible to others with unfettered access; let the viewer beware] http://www.antioffline.com/deviation/w2000/defense_in_depth.pdf