# - The Aurora Power Grid Vulnerability –

*A White Paper*

**What is the Aurora vulnerability?:** Aurora is a vulnerablity to cyber attacks that could sabotage critical systems that provide electricity including the nationwide power grid. This vulnerability effects control systems that operate rotating machinery such as pumps, turbines and so on. The vulnerability of the nation's electrical grid to computer attack is due in part to steps taken by power companies to transfer control of generation and distribution equipment from internal networks to supervisory control and data acquisition, or SCADA, systems that can be accessed through the Internet or by phone lines.

The move to SCADA systems boosts efficiency at utilities because it allows workers to operate equipment remotely. But this access to the Internet exposes these once-closed systems to cyber attacks. So far, incidents of hackers breaking into control systems to cause damage or outages have been scarce although there have been a few. However, the threat of such damage makes control systems an alluring target for extortionists, terrorists, unfriendly governments and others.

Electric utilities, pipelines, railroads and oil companies use remotely controlled and monitored valves, switches and other mechanisms that are vulnerable to attack.

In a dramatic video-taped demonstration of the Aurora vulnerability recorded in 2006, engineers at Idaho National Labs showed how the weakness could be exploited to cause any spinning machine connected to the power grid -- such as a generator, pump or turbine -- to self-destruct. These attacks could easily be carried out on vulnerable equipment using the Internet.

Costs and time are frequently given as the reasons for not locking down these complex networks. Many plant operators consider it unlikely that an attacker would be able manipulate or damage control systems, as most of these systems run on obscure hardware powered by highly specialized communications standards. However, this "security-by-obscurity" defense is gradually eroding, as a number of utilities are upgrading from older, legacy systems to operating systems more familiar to the average hacker, such as Microsoft Windows and Linux.

The GAO issued a vulnerability report on May 21, 2008 regarding the Tennessee Valley Authority, the nation's largest public utility company. The GAO found that TVA's Internet-connected corporate network was linked with systems used to control power production, and that security weaknesses

pervasive in the corporate side could be used by attackers to manipulate or destroy vital control systems. As a wholly owned federal corporation, TVA must meet the same computer security standards that govern computer practices and safeguards at federal agencies. As of 5/21/2008 it apparently did not. The GAO also warned that computers on TVA's corporate network lacked security software updates and anti-virus protection, and that firewalls and intrusion detection systems on the network were easily bypassed and failed to record suspicious activity.

The task of gauging the electric sector's true progress in mitigating the Aurora vulnerability has fallen to the Federal Energy Regulatory Commission. In January 2008, FERC approved eight mandatory reliability standards to protect bulk power systems against disruptions from cyber-security breaches. The agency has the authority to fine plants up to $1 million a day for violations of those standards, but the industry has until 2010 to demonstrate compliance with the new rules.

Security experts contend that existing standards contain loopholes and don't adequately protect critical power systems. For example, telecommunications equipment is excluded, even though there are documented cases of computer worms shutting off service from control systems to substations. There are security experts in the power industry who recognize the threat from cyber vulnerabilities like Aurora, but who claim they don't have the funding or the authority to do much about it.

**FAA Air Traffic Control system vulnerability:** While not an aurora vulnerability per se, a recent USDOT report stated that the nation's air traffic control systems are vulnerable to cyber attacks. Support systems have been breached in recent months allowing hackers access to personnel records and network servers, according to a government audit.

The Transportation Department's inspector general concluded that although most of the attacks disrupted only support systems, they could spread to the operational systems that control communications, surveillance and flight information used to separate aircraft. The report noted several recent cyber attacks, including a February incident when hackers gained access to personal information on about 48,000 current and former Federal Aviation Administration employees, and an attack in 2008 when hackers took control of some FAA network servers.

Auditors said the FAA is not able to adequately detect potential cyber security attacks, and it must better secure its systems against hackers and other intruders. "In our opinion, unless effective action is taken quickly, it is likely to be a matter of when, not if, ATC (air traffic control) systems encounter attacks that do serious harm to ATC operations," the auditors said.

According to the report, the FAA received 800 cyber incident alerts during the fiscal year that ended Sept. 30, 2008, and more than 150 were not resolved before the year finished. Fifty of those, the auditors said, had been open for more than three months, "including critical incidents in which hackers may have taken over control" of some computers. Officials tested Internet-based systems that are used to provide information to the public. The tests found nearly 4,000 "vulnerabilities," including 763 viewed as "high risk." The vulnerabilities including weak passwords, unprotected file folders, and other software problems.

These weaknesses could allow hackers or internal FAA workers to gain access to air traffic systems, and possibly compromise computers there or infect them with malicious codes or viruses.

**BIOS is also vulnerable to modern malware attacks:** Basic Input/Output System (BIOS), a firmware run by a computer at the time of boot-up, is increasingly targeted by malware attacks as modern hackers having administrative OS rights are effectively conducting BIOS updates or BIOS on the Internet to load customized low-level firmware. Recently, experts have shown how BIOS malware could be used to attack multiple operating systems and infect different kinds of motherboards. According to them, BIOS-based malicious software can disseminate not just on various OSs, but also by a number of hardware. These attacks are hard to identify and block. Earlier during March 2009 at the Vancouver CanSecWest security conference, researchers Anibal Sacco and Alfredo Ortega of Core Security Technologies Inc. performed a general BIOS attack that could push malware inside various BIOS types, as reported by search security on June 18, 2009.

**Terrorist attacks:** Terrorists groups could soon use the internet to help set off a devastating nuclear attack, according to research done by the International Commission on Nuclear Non-proliferation and Disarmament (ICNND). Their study suggests that under the right circumstances, terrorists could break into computer systems and launch an attack on a nuclear state triggering a catastrophic chain of events that would have a global impact. Without better protection of computer and information systems, the paper states, governments around the world are leaving open the possibility that a well-coordinated cyberwar could quickly elevate to nuclear levels. In fact, this may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb themselves. Though the paper admits that the media and entertainment industries often confuse and exaggerate the risk of cyberterrorism, it also outlines a number of potential threats and situations in which dedicated hackers could use information warfare techniques to make a nuclear attack more likely. While the possibility of a radical group gaining access to actual launch systems is remote, the study suggests that hackers could focus on feeding in false information further down the chain or spreading fake information to officials in a carefully orchestrated strike. "Despite claims

that nuclear launch orders can only come from the highest authorities, numerous examples point towards an ability to sidestep the chain of command and insert orders at lower levels," said Jason Fritz, the author of the paper. "Cyber-terrorists could also provoke a nuclear launch by spoofing early warning and identification systems or by degrading communications networks." Since these systems are not as well-protected as those used to launch an attack, they may prove more vulnerable to attackers who wish to tempt another nation into a nuclear response. Cyberspace is real, and so is the risk that comes with it. Online attacks are one of the most serious economic and national security challenges we face. However, the study suggests that although governments are increasingly aware of the threat of cyberwar with other nations, action to bolster those defenses does not alleviate the threat of a rogue group that circumvented the expected strategies for online warfare. "Just as the 9/11 attacks were an unprecedented attack with unconventional weapons, so too could a major cyber attack," it says.

**Hacking the 'smart grid':** The race to build a "smarter" electrical grid could have a dark side. Security experts are starting to show the dangers of equipping homes and businesses with new meters that enable two-way communication with utilities.

There are many benefits to upgrading the nation's electricity networks, which is why a smart-grid movement was already revving up before the recent economic recovery package included $4.5 billion for the technology. Smarter grids could help conserve energy by giving utilities more control over and insight into how power flows. But there are potential problems with moving too fast.

The risks are similar to what happens when computers are linked over the Internet. By exploiting weaknesses in the way computers talk to each other, hackers can seize control of innocent people's machines. In the case of the power grid, better communication between utilities and the meters at individual homes and businesses raises the possibility that someone could control the power supply for a single building, an entire neighborhood, or worse. For example, a computer worm could give miscreants remote control of the meters, which would let them take advantage of a utility's ability to, for example, disconnect someone's power for not paying his bill. A key vulnerability has been found in devices made by an unnamed manufacturer. But once infected, a worm could spread to other manufacturers' products that use the same communications technologies and can be used to remotely disconnect people's power.

To get the computer worm going, a hacker might have to get physical access to one of the meters in order to program it with malicious code. That could start a chain reaction in which the worm spreads meter to meter over the grid's communication network. This hack might also be done remotely, if the traffic on the network isn't encrypted.

More than 50 million smart meters are expected to be deployed by U.S. electric utilities by 2015, according to a list of publicly announced projects kept by The Edison Foundation. More than 8 million have already been deployed.

**How a Phishing Attack Exposed an Energy Company to Hackers:** The following is an unsubstantiated report that was published on the Internet. The report declines to identify the energy company involved so I will take these "facts" with a grain of salt. However, the described attack and it's aftermath is certainly plausible so I will include it here as a potential attack vector that needs to be defended against.

Using a Microsoft zero-day vulnerability and a bit of social engineering, hackers compromised a workstation and threatened critical SCADA systems. It began with an e-mail sent to an employee at an energy company, and ended with a security breach that exposed critical systems to outside control. The attack began to unravel April 3, 2007. That's when a fraudulent user account, complete with administrative privileges, was detected by the energy company. Tracing backwards, it turned out that random administrative accounts were being added in the internal network because another machine inside their corporate network had been compromised due to a successful phishing attack. The reason why I am repeating this story is to underscore that fact that the number one security risk to networks is people.... in some cases, employees can be fooled into going to a web site that has been infected with malware and once that happens, it's all over but the crying. But in this example, the attack was even less sophisticated than that.

The employee machine sat on the same segment where the SCADA (Supervisory Control And Data Acquisition) controllers were. This, of course, was a fundamental network security gaffe. Soon, evidence appeared that the attackers had leapfrogged off this network and broken into the domain controller. The source of the breach? A relatively simple phishing attack. The phishing e-mail contained a pitch for a new health care plan, something that caught an employee's eye. The e-mail claimed to be about benefits for a family with two or more children, and the employee had three. The message also contained a malicious .chm file attachment. When the employee opened the attachment, it reached out to a server in the Asia-Pacific region and pulled out a malicious executable that gave the attackers a foothold on the employee's machine. This particular attack took advantage of MS07-029, a Windows DNS (Domain Name System) vulnerability that at the time was unpatched. This, of course, is also a fundamental network security gaffe. Strike three! You're out... Using the vulnerability as an entry point, the attackers ended up with control of the employee's account. With the level of access they gained, the attackers could potentially control, view and modify everything related to the business.

Our advice? Put a proxy in place for Web browsing, obviously. But more critical

is the subject of segregation. No workstation sharing a critical network segment such as SCADA should be connected to the Internet. Patch management, employee security training and the other preventative measures described in this series of white papers are also vital to protecting your network. HTH….

**About the Author**

Frank Saxton is a computer network security engineer and Easyrider LAN Pro principle. Home-based in Portland, Oregon, Frank has been designing remote diagnostic and network enterprise monitoring centers since the late 1970s. Prior to becoming a professional systems engineering consultant in 1990, Frank had a 20 year career in computer systems field engineering and field engineering management. Frank has a BSEE from Northeastern University and holds several certifications including Network General's Certified Network Expert (CNX). As a NOC design engineer and architect, Frank works regularly with enterprise-class monitoring tools such as HP Openview Operations, BMC Patrol and others. In his enterprise security audit work, Frank uses sniffers and other professional grade monitoring tools on a daily basis.