



Securing the Enterprise



CYBER THREATS GROW

BY SALVATORE SALAMONE



UTILITIES AND THE electric power grid are becoming increasingly susceptible to cyber-attacks.

More and more, companies are monitoring, managing, and controlling critical transmission and grid elements based on data collected at remote locations throughout the power grid or distribution systems. As such, the security troubles are twofold.

First, the devices that collect data and manage equipment are essentially computers, which are subject to being hacked. Second, information from these devices is transmitted over networks, thus making it possible for hackers to intercept information, or worse, issue false commands to disrupt the operation or possibly seize control of the devices.

At the heart of the problem is how to protect supervisory control and data acquisition (SCADA) systems. Safeguarding these systems is becoming more challenging because hackers are using newer techniques to break into systems.

Just last year, the Department of Homeland Security (DHS) made the unusual move of issuing an advisory urging companies to quickly install a Microsoft patch that had been issued less than 24 hours before the advisory went out.

The patch dealt with a newly found weakness called a buffer overflow vulnerability. The DHS noted: "This vulnerability could impact government systems, private industry and critical infrastructure."

The urgency behind the DHS advisory had to do with the potential harm exploits aimed at this vulnerability could cause. In particular, unpatched Windows systems could become infected by malicious software that would communicate back to a central server via an IRC or Internet relay chat channel. This would turn the infected computer into what is known as a bot, which is a computer that can be controlled by a hacker to spread spam, launch a denial of service attack, or download other malicious software such as keyloggers and spyware.

Unfortunately, there are dozens to hundreds of new vulnerabilities discovered every month. This is why Microsoft and other companies issue frequent patches to their programs. But many companies do not keep up with all the patches. This is a problem



since an unpatched system is an open door into a utility's or grid operator's network.

According to the SysAdmin, Audit, Network, Security Institute, a research and educational organization, several years ago, the Davis-Besse nuclear plant in Ohio had been off line for almost a year when the SQL Slammer worm was released and infected and disabled its safety parameter display system for five hours and its plant process computer for six hours. SANS noted that both systems had analog backups that were not affected.

Subscribe Online to *EnergyBiz*



Sensus Flex[®] Net

Flexible to meet your dynamic AMI expectations.

The Sensus FlexNet Advanced Metering Infrastructure (AMI) technology is truly based on flexibility. This comprehensive fixed network solution takes into account that **your information needs aren't static**; nor are they identical to other utilities.

FlexNet provides you with advanced metering data and demand side management capabilities.

You set the parameters – **the system responds.**

What's more, this intelligent system is available in custom packages for electricity, gas and water utilities with all meters supported on the same network. That's flexibility. **That's FlexNet.**

Discuss **FlexNet benefits**

with your local Sensus distributor.

The only truly flexible AMI system.



Contact us for literature: 1-800-METER-IT or www.sensus.com/FlexNet



Rick Sergel
AP Photo / Robin Nowacki

Making matters more challenging is the fact that hackers have changed their objectives. In the past, attacks typically showed off a hacker's technical prowess. Today's attacks are more likely aimed at committing financial fraud, stealing proprietary information, or sabotaging a company's data or its network.

"There is a shift toward more damage due to the theft of sensitive company data," said Chris Keating, director, Computer Security Institute. "This is an ominous development and underscores the need to insist that company networks be properly safeguarded."

And there is also the terrorist factor to consider. Some experts downplay the risk from terrorists, believing they would target the physical grid rather than launching a cyber-attack. But numerous news sources have reported that Al Qaeda documents found in Afghanistan in 2002 indicate an interest in cyber-attacks on the electrical grid.

INDUSTRY EFFORTS KICK IN

To address the increasing risks, the North

American Electric Reliability (NERC) last year adopted eight new cyber-security standards.

The standards cover asset identification, security management controls, personnel and training, perimeter security, systems security, incident reporting and response planning, and recovery plans.

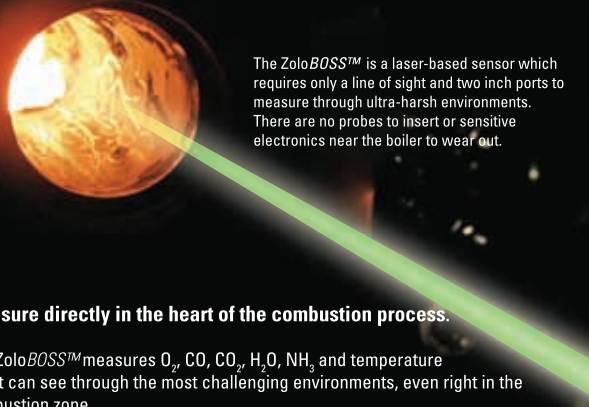
"These eight new standards provide a comprehensive set of requirements to protect the bulk power system from malicious cyber attacks," said Rick Sergel, NERC president and CEO.

The new standards replace the Urgent Action Cyber Security Standard, which NERC adopted in August 2003 to address cyber security concerns in the wake of the 9-11 attack.

Other industry efforts include the work done by the Idaho National Laboratory and the Electric Power Research Institute's Energy Information Security program. The two efforts provide guidance on best security practices that utilities, distributors, and grid operators can use to help safeguard their infrastructure and systems. ☐

Subscribe Online to EnergyBiz

Measure Where it Counts




The ZoloBOSS™ is a laser-based sensor which requires only a line of sight and two inch ports to measure through ultra-harsh environments. There are no probes to insert or sensitive electronics near the boiler to wear out.

Measure directly in the heart of the combustion process.


The ZoloBOSS™ measures O₂, CO, CO₂, H₂O, NH₃ and temperature and it can see through the most challenging environments, even right in the combustion zone.

O₂




Other sensors measure at a single point in the back-pass. Only the ZoloBOSS™ allows real-time mapping of multiple constituents simultaneously in the back-pass and the combustion zone.

CO




Make your measurement dollars count.

CO₂



Measure where no one else can.



4946 North 63rd Street, Boulder, CO 80301 USA
sales@zolotech.com 303 604 5800
www.zolotech.com

**Better Measurements
Mean Better Results**


Deep. Rich. Refined.

Start your day with the industry standard for energy news services – Energy Central Professional

Deep. Energy Central Professional delivers the most in-depth gas and power industry news, directly to your email every business day.

Rich. When you need more than news, you have unlimited access to comprehensive industry data through a secure web site or intranet connection.

Refined. You select the topics you want to receive, we deliver your personally refined news service.



in your day?

