Report

McAfee
An Intel Company

SMARTER PROTECTION FOR THE SMART GRID

ENERGY SECURITY

CONTENTS

Prime Target: The Energy Grid

If a rogue state, terrorist, or malcontent wanted to debilitate a major city or even an entire country, how could it make a widespread, immediate, and lasting impact? Quite simply, by striking at the facilities that produce and distribute the electrical power that everything else depends on.

Anything from the lights and appliances in your home to heart monitors in hospitals to air defense systems—anything could be compromised by a single, targeted attack on the energy grid. Only today, the weapon of choice is not a rocket launcher, but rather, malicious software code—malware that is skillfully designed to destroy, disrupt, or take control of the complex systems on which the grid runs.

There was a time when "energy security" meant chain link fences and barbed wire around substations and transmission lines, and natural disasters were more of a threat than man-made ones. Today, however, the safe and reliable flow of energy from supply to demand is increasingly dependent on automation and interconnected embedded systems. And it will inevitably become even more so, as the "smart grid" envisioned by energy producers and policymakers takes shape.

The problem is that the very thing that makes the grid smart—the ability of myriad embedded systems to communicate with each other, often using a combination of legacy and proprietary equipment alongside more modern solutions—has created a duality where communications over serial, wired and wireless Ethernet, cellular, and dial-up modems being used with a combination of common TCP/IP and proprietary protocols. This has expanded the attack surface, making it vulnerable to cyberthreats. Open systems invite hacking. More malware was detected on computer networks in 2011 than in all previous years combined, with critical infrastructure being a prime target. All of this begs the question in many minds: can a system with so many points of entry, like a house with all the doors and windows left open while the owner is on vacation, really be called "smart"?

The good news is that we are getting smarter about identifying, finding, and fixing vulnerabilities, and technology is increasingly effective at detecting and thwarting attacks. The challenge is that cybersecurity investments—and cybersecurity consciousness have not kept pace with either the sophistication of embedded technology nor the shrewdness and tenacity of attackers. And in spite of energy being perhaps the most regulated sector on the planet, "compliant" doesn't always translate to "secure."

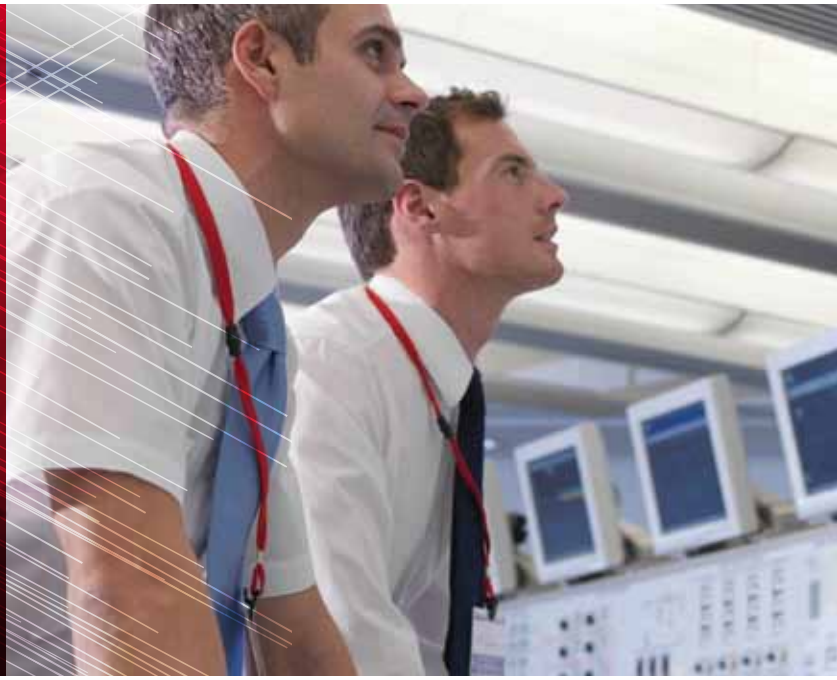
Securing the energy grid will require action on three fronts: technical, cultural, and political. McAfee and our partners in industry and government are making great strides on the technical front to mitigate the threats, whatever their origins or intentions. Addressing the cultural and political issues is a broader challenge calling for a broader awareness. In this paper we will look at how and why the energy grid is vulnerable to cyberthreats, what is being done to counter these threats, and what more needs to be done to make our energy systems as secure as realistically possible.

Tom Moore
Vice President, Embedded Security
McAfee

The threats: extortion, espionage, sabotage.

The goals: financial gain, data theft, shutting down facilities.

The suspects: organized criminal enterprises, commercial competitors, and even governments.



The Worm Turns, The Alarm Sounds

The story of Stuxnet is like that of a sensational crime that generates a flurry of media attention and speculation when it happens, but eventually fades from the news even though the mystery remains unsolved.

The Stuxnet worm first came to the public's attention in 2010, when it attacked several facilities around the world, including Iran's nuclear enrichment infrastructure, taking control of programmable logic controllers (PLCs) that control the automation of mechanical processes and disrupting centrifuges and turbines. Since then, more advanced variants of the malware have been reported in various places globally. In a 2010 survey on critical infrastructure security by McAfee and the Center for Strategic and International Studies (CSIS), nearly half of the respondents from the energy sector said they had found Stuxnet on their systems.[1]

Stuxnet set off an alarm that continues to reverberate throughout the energy sector today. Security experts who deconstructed the worm deemed it to be of a level of sophistication that could only be achieved with a multimillion dollar budget and "nation-state support." Regardless of its origin, its intention was unequivocal: sabotage.

More recently, an apparent descendant of Stuxnet called Duqu has been reported in energy facilities in at least eight countries. Perhaps authored by the creators of Stuxnet, or at least using the older worm's source code, Duqu has not been used in any actual attacks to date—although it is capable of doing damage—but rather appears to be probing for sensitive information and weaknesses that could be exploited in future attacks.

1 *In the Dark: Crucial Industries Confront Cyberattacks,* McAfee and the Center for Strategic and International Studies, 2011

The Varied Threat Landscape

While the physical destruction of facilities, with potentially deadly consequences, is a genuine concern, many cyberthreats are subtler in intent. Beginning in 2009, a series of attacks were launched against the global energy, oil, and petrochemical sectors. Masquerading as everyday system administration tools, the virus gained access to web extranets, desktop PCs, and servers, capturing usernames and passwords, and extracting sensitive proprietary data and internal communications. Dubbed "Night Dragon," the goal of the stealth attack appears to be the theft of intellectual property—a form of espionage, whether corporate or state-sponsored.

The most prevalent cyberthreat reported by the global energy sector is extortion. Criminals gain access to a utility's system, demonstrate that they are capable of doing damage, and demand a ransom. In the McAfee/CSIS study noted earlier, one in four power companies globally said they had been victims of extortion. In some countries, the incidence is alarmingly epidemic—80 percent in Mexico, for example, and 60 percent in India. And the sums of money paid out are equally staggering—hundreds of millions, by some estimates.

The threats: extortion, espionage, sabotage. The goals: financial gain, data theft, shutting down facilities. The suspects: organized criminal enterprises, commercial competitors, and even governments. One of the challenges in confronting cyberthreats to the energy sector is that they take many forms, have disparate goals, and originate with a variety of sources. It makes it difficult to know which systems are at risk, which require protection, at what level, and at what cost.

The Department of Energy's Pacific Northwest National Laboratory (PNNL) is part of a research network charged with studying cybersecurity (among other energy-related issues), developing policy recommendations and partnering with industry to bring technology solutions to market. "We need to better understand the threat landscape, whether it's international, domestic, external, or even posed by insiders," says Philip Craig, a researcher in the lab's National Security Directorate. "We tend to learn about threats and impacts as they happen, unfortunately. We have to turn that around."

How Did We Get Here?

How did we wind up with a system of energy production and distribution so vulnerable to attack? Ironically, the answer lies in well-intentioned efforts to modernize energy distribution and make it safer, cleaner, more efficient, less costly, and open to more alternative forms of production.

Energy system operators have historically been concerned with three technology domains. The first is the industrial control systems (ICS) that run turbines, generators and other heavy-duty equipment. Individual ICS systems typically perform a few specific tasks that do not require a lot of processing power. Overseeing the ICS are the system control and data acquisition, or SCADA, systems. These systems don't actually run equipment but enable operational teams to monitor and manage the ICS through consoles known as "human-machine interfaces," or HMI. The third domain is the provider's organizational IT network—its internal databases and business applications.

In years long past, these three domains operated discretely, physically separated by "air gaps" with no direct connection to each other. If data from one domain was needed in another—for example, measurements of consumption required for financial forecasting—it was manually transferred on a disc. It was, of course, inefficient, and as companies became more networked, they eagerly eliminated the manual steps and began automating the delivery of data across domains.

"Data plays a big part in business decisions," points out Ernest Rakaczky, program director for control system security at Invensys Operations Management, a provider of automation solutions to the global manufacturing and infrastructure sectors. "In energy, the movement of the end product is based on capacity and availability. Operators needed to know these things in real time, and the demand for information drove tighter connectivity between the business and process control networks."

Bridging the air gaps between IT, SCADA, and ICS meant that an intruder could gain access to all three domains simply by entering any one of those. And once operators became reliant on the Internet—which allows administrators to telecommute and field workers to reprogram systems from remote locations through their smartphones—they essentially opened all their systems to the outside world.

Another source of vulnerability is the age of much of the infrastructure. An estimated 70 percent of the existing energy grid is more than 30 years old. In the effort to update it and integrate it with more modern installations, connecting aging systems to the Internet without the benefit of encryption, security has largely been an afterthought. "The legacy system is a real challenge," says the PNNL's Mr. Craig. "The way we've connected our rural infrastructure has created a lot of opportunities for access, both physical and cyber."

Embedded Technology: The Brains of the Smart Grid

The third and perhaps most alarming cause of vulnerability is the proliferation and increasing interconnection of embedded software and devices directing the flow of energy. These devices are constantly communicating with each other, performing calculations, making decisions, sending instructions, and reporting to central control systems, based on the data they generate and share. While each of these built-in computers is typically single-function with a very specific task, more and more are being built with off-the-shelf rather than proprietary software, making them increasingly generic—and therefore vulnerable. As such, they are the prime targets of intruders seeking to gain control of or disrupt the delivery of energy.

At the 2011 Black Hat Security Conference, a gathering of information security professionals that also attracts a number of hackers, a team of researchers revealed that they had found several critical infrastructure control devices connected to the Internet simply by searching for them on Google. Once an embedded device is located, anyone who can figure out its IP address can send commands to it.

"If we set out to design a 'perfectly bad system' of energy delivery, so bad that its failure would have catastrophic consequences, what might it look like? First, it would all be interconnected, so that failure in any one area would affect all others. Second, it would connect real things made of concrete and steel, not just silicon, so that failure would cause real physical damage—fires or explosions. And third, we'd connect it to the Internet, knowing that intruders could get into it because they've already tried and succeeded. I'm not saying anyone set out to build it that way, but this hypothetical 'perfectly bad system' sounds awfully close to what we're calling the smart grid."

—Jason Healy, director of the cyberstatecraft initiative at the Washington-based Atlantic Council

Some see the headlong rush towards a more automated energy grid as an invitation to disaster. Jason Healy, director of the cyberstatecraft initiative at the Washington-based Atlantic Council, poses this question. "If we set out to design a 'perfectly bad system' of energy delivery, so bad that its failure would have catastrophic consequences, what might it look like?" he asks. "First, it would all be interconnected, so that failure in any one area would affect all others. Second, it would connect real things made of concrete and steel, not just silicon, so that failure would cause real physical damage—fires or explosions. And third, we'd connect it to the Internet, knowing that intruders could get into it because they've already tried and succeeded. I'm not saying anyone set out to build it that way, but this hypothetical 'perfectly bad system' sounds awfully close to what we're calling the smart grid."

Building in Security from the Ground Up

In today's existing energy production and distribution systems, whether legacy or the first wave of smart grid, little if any thought was given to security at the time of design and installation. Power providers have been more concerned with energy availability—ensuring a steady supply of energy—and want to have easy access to systems for maintenance and repairs in the event of a blackout. The irony, of course, is that the opportunities for tampering with or seizing control of distribution system pose a significant threat to availability, and the cost of replacing a damaged generator far outweighs the investment required to protect it.

"Stuxnet should have been the wake-up call," says Mr. Healy. "Now that we know the Internet has been 'weaponized,' what do we need to do before we push too far and too fast on the smart grid? We have to bake security in from the beginning."

The rash of probes and threats reported in recent years has stirred up a sense of urgency around cybersecurity, but there are still many barriers to be overcome—technical, cultural, and political.

Securing the Target

There is increasingly widespread agreement with Mr. Healy's point that security needs to be built into grid components at the planning and design phase. In particular, because the grid relies so heavily on embedded systems, which makes them ripe targets for intruders, it is imperative to integrate security solutions natively in these devices.

A wide range of technologies already exists for achieving that goal, from antivirus and anti-malware protection to firewalls, advanced encryption, and application blacklisting and whitelisting. Whitelisting refers to technology that ensures that an embedded device will accept commands only from a known, recognized, authorized, and trusted application. If a piece of malware succeeds in getting through the system interfaces and into the device itself, its commands will be ignored and the intrusion will be reported. To mitigate vulnerabilities and thwart attacks, McAfee addresses endpoint, network, and data security within the grid as part of a cohesive security solution.

In the face of ever more sophisticated rootkits, which are designed to hide the presence of malware and enable deep penetration into a targeted system, McAfee and its parent company Intel have jointly developed a technology called McAfee® DeepSAFE™ technology. Where traditional security solutions are software-based and function above the operating system, McAfee DeepSAFE technology represents the first hardware-assisted solution that works beyond the operating system to detect malware deep in the computing stack, below the rootkits, strengthening the protection of the device.

Situational Awareness

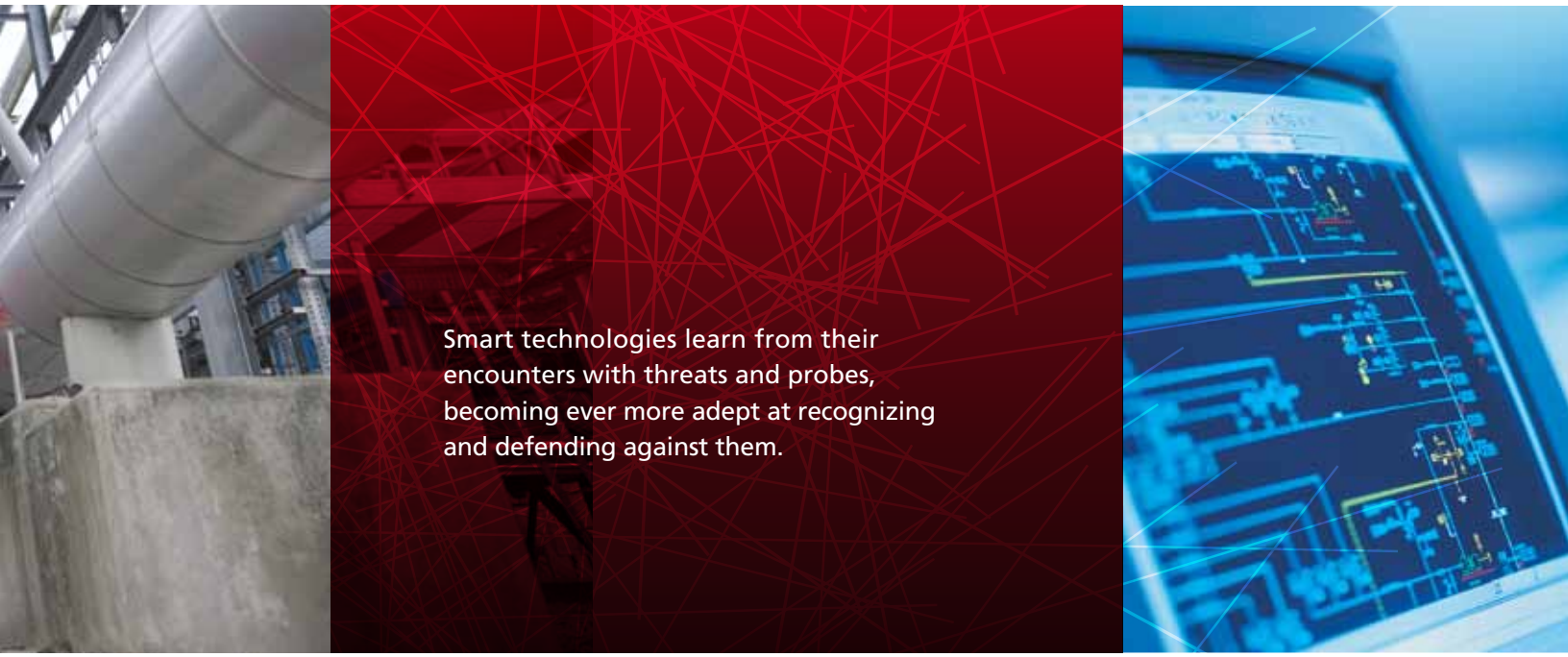
Once designed and installed, embedded systems also need to be monitored and managed. Situational awareness is another critical element of network security and another area where technology has made significant strides. Today's more sophisticated situational awareness technology not only gathers data from the various embedded devices in a network, but is also capable of analyzing and interpreting that data at a very granular level to determine whether something is amiss. Because the power providers' three technology domains identified earlier—IT, SCADA, and ICS—are interconnected and interdependent, situational awareness and visibility across all three are essential.

Advances in cybersecurity technology can be likened to a body's immune system, which builds up resistance to a virus the more it is exposed to it. Smart technologies learn from their encounters with threats and probes, becoming ever more adept at recognizing and defending against them.

Towards a Stronger Cybersecurity Culture

While cybersecurity can be embedded into the devices that run the grid, it also needs to be embedded in the consciousness of the people who operate it. "A cultural transition needs to take place," says Mr. Rakaczky of Invensys. "People in the power business need to think about system security the way they think about personal safety. When you walk into any plant today, you can tell that safety is the number one priority. Everyone takes responsibility for it. The culture of safety is well defined. The culture of cybersecurity has to get to that same level, and it's not there yet."

Before Stuxnet, energy providers were reluctant to discuss the possibility of security breaches for fear of calling themselves to the attention of hackers—or inviting stricter regulation. Much of that reluctance seems to be abating as more parties embrace the idea of information sharing and incident disclosure as a means of combating



cyberthreats. Meanwhile, regulation and industry standards have indeed become drivers of cybersecurity, or at least compliance with regulations governing security. Power providers in North America rely heavily on ICS and SCADA vendors to make sure their systems are compliant with the North American Electrical Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) standards. Some critics, however, argue that compliance in many instances is a case of "checking off boxes," and tighter regulation does not in itself make for tighter security.

"The number one focus in compliance always seems to be around that one snapshot in time—the audit," Mr. Rakaczky says. "Compliance can't guarantee that security measures will never be breached. But compliance and practical security measures can serve as the foundation for a culture where everyone feels like they have an equal stake in security, and the security program is part of the plant's normal way of life."

Thinking beyond regulation, government and policymakers have many more tools in their arsenal to help advance the cause of cybersecurity in the energy grid, including positive incentives to encourage innovation and investment in research and development. As the PNNL's Mr. Craig explains, "One of the unique characteristics of the lab is that we are leveraging the federal investment to develop hardware and software that address cyberthreats, which is then licensed to companies that have the resources to deploy it commercially."

Whether from criminals, hacktivists, or governments seeking advantage over their adversaries, threats to the energy infrastructure or any critical infrastructure are not going away. A smarter, cleaner, and more efficient system of energy distribution is in everyone's interest, everywhere, but without a strong security component, all of its purported advantages become meaningless. Technology innovation, spurred by public policy and embraced by an industry governed by a culture of security, is the key to making it happen.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

http://www.mcafee.com

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

45500rpt_embedded-energy_0612