CYBERSECURITY

HACKING THE LIGHTS OUT

Computer viruses have taken out hardened industrial control systems. The electrical power grid may be next

By David M. Nicol

IN BRIEF

Every facet of the modern electrical grid is controlled by computers. It is our greatest example of physical infrastructure interlinked with electronics.

The Stuxnet virus that infected Iran's nuclear program showed just how vulnerable machines could be to a well-crafted electronic virus.

The grid shares many of the vulnerabilities that Stuxnet exposed; being larger, its vulnerabilities are, if anything, more numerous.

Although a sophisticated attack could bring down a large chunk of the U.S. electrical grid, security is being ramped up.

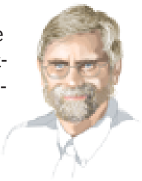
VINCENT LAFORET *Redux Pictures*

LAST YEAR WORD BROKE OF A COMPUTER VIRUS THAT HAD managed to slip into Iran's highly secure nuclear enrichment facilities. Most viruses multiply without prejudice, but the Stuxnet virus had a specific target in its sights—one that is not connected to the Internet. Stuxnet was planted on a USB stick that was handed to an unsuspecting technician, who plugged it into a computer at a secure facility. Once inside, the virus spread silently for months, searching for a computer that was connected to a prosaic piece of machinery: a programmable logic controller, a special-purpose collection of microelectronics that commonly controls the cogs of industry—valves, gears, motors and switches. When Stuxnet identified its prey, it slipped in, unnoticed, and seized control.

The targeted controllers were attached to the centrifuges at the heart of Iran's nuclear ambitions. Thousands of these centrifuges are needed to process uranium ore into the highly enriched uranium needed to create a nuclear weapon. Under normal operating conditions, the centrifuges spin so fast that their outer edges travel just below the speed of sound. Stuxnet bumped this speed up to nearly 1,000 miles per hour, past the point where the rotor would likely fly apart, according to a December report by the Institute for Science and International Security. At the same time, Stuxnet sent false signals to control systems indicating that everything was normal. Although the total extent of the damage to Iran's nuclear program remains unclear, the report notes that Iran had to replace about 1,000 centrifuges at its Natanz enrichment facility in late 2009 or early 2010.

Stuxnet demonstrates the extent to which common industrial machines are vulnerable to the threat of electronic attack. The virus targeted and destroyed supposedly secure equipment while evading detection for months. It provides a dispiriting blueprint for how a rogue state or terrorist group might use similar technology against critical civilian infrastructure anywhere in the world.

Unfortunately, the electrical power grid is easier to break into than any nuclear enrichment facility. We may think of the grid as one gigantic circuit, but in truth the grid is made from thousands of components hundreds of miles apart acting in unerring coordination. The supply of power flowing into the grid must rise and fall in lockstep with demand. Generators must dole their energy out in precise coordination with the 60-cycle-per-second beat that the rest of the grid dances to. And while the failure of any single component will have limited repercussions to this vast circuit, a coordinated cyberattack on multiple



David M. Nicol is director of the Information Trust Institute and a professor in the department of electrical and computer engineering at the University of Illinois at Urbana-Champaign. He has worked as a consultant for the U.S. Department of Homeland Security and Department of Energy.

points in the grid could damage equipment so extensively that our nation's ability to generate and deliver power would be severely compromised for weeks—perhaps even months.

Considering the size and complexity of the grid, a coordinated attack would probably require significant time and effort to mount. Stuxnet was perhaps the most advanced computer virus ever seen, leading to speculation that it was the work of either the Israeli or U.S. intelligence agencies—or both. But Stuxnet's code is now available on the Internet, raising the chance that a rogue group could customize it for an attack on a new target. A less technologically sophisticated group such as al Qaeda probably does not have the expertise to inflict significant damage to the grid at the moment, but black hat hackers for hire in China or the former Soviet Union might. It is beyond time we secured the country's power supply.

THE BREAK-IN

A YEAR AGO I TOOK PART in a test exercise that centered on a fictitious cyberattack on the grid. Participants included representatives from utility companies, U.S. government agencies and the military. (Military bases rely on power from the commercial grid, a fact that has not escaped the Pentagon's notice.) In the test scenario, malicious agents hacked into a number of transmission substations, knocking out the specialized and expensive devices that ensure voltage stays constant as electricity flows across long high-power transmission lines. By the end of the exercise half a dozen devices had been destroyed, depriving power to an entire Western state for several weeks.

Computers control the grid's mechanical devices at every level, from massive generators fed by fossil fuels or uranium all the way down to the transmission lines on your street. Most of these computers use common operating systems such as Windows and Linux, which makes them as vulnerable to malware as your desktop PC is. Attack code such as Stuxnet is successful for three main reasons: these operating systems implicitly trust running software to be legitimate; they often have flaws that admit penetration by a rogue program; and industrial settings often do not allow for the use of readily available defenses.

Even knowing all this, the average control system engineer would have once dismissed out of hand the possibility of remotely launched malware getting close to critical controllers, arguing that the system is not directly connected to the Internet. Then Stuxnet showed that control networks with no permanent connection to anything else are still vulnerable. Malware can piggyback on a USB stick that technicians plug into the control system, for example. When it comes to critical electronic circuits, even the smallest back door can let an enterprising burglar in.

Consider the case of a transmission substation, a waypoint on electricity's journey from power plant to your home. Substations take in high-voltage electricity coming from one or more power plants, reduce the voltage and split the power into multiple output lines for local distribution. A circuit breaker guards each of these lines, standing ready to cut power in case of a fault. When one output line's breaker trips, all of the power it would have carried flows to the remaining lines. It is not hard to see that if all the lines are carrying power close to their capacity,

MARK DUNCAN AP Photo (left); MARK PETERSON Redux Pictures (center); EBRAHIM NOROUZI AP Photo (right)

TIMELINE

Digital Attacks, Physical Harm

As industrial machinery goes online, the potential for wreaking havoc grows. Intrusions over the past decade show that the grid is not the only vulnerability—anything with a microchip can be a target.

Davis-Besse nuclear plant

April 2000
A disgruntled former employee of a water treatment firm uses stolen radio parts to issue faulty commands to sewage equipment in Queensland, Australia, causing more than 200,000 gallons of raw sewage to spill into local parks and rivers.

January 2003
The Slammer worm bypasses multiple firewalls to infect the operations center at Ohio's Davis-Besse nuclear power plant. The worm spreads from a contractor's computer into the business network, where it jumps to the computers controlling plant operations, crashing multiple safety systems. The plant was off-line at the time.

March 2007
Government officials simulate a cyberattack on electricity generation equipment at the Idaho National Laboratory. A video of the test, called Aurora, is later leaked to CNN.

2000 2001 2002 2003 2004 2005

then a cyberattack that trips out half of the output lines and keeps the remaining ones in the circuit may overload them.

These circuit breakers have historically been controlled by devices connected to telephone modems so that technicians can dial in. It is not difficult to find those numbers; hackers invented programs 30 years ago to dial up all phone numbers within an exchange and make note of the ones to which modems respond. Modems in substations often have a unique message in their dial-up response that reveals their function. Coupled with weak means of authentication (such as well-known passwords or no passwords at all), an attacker can use these modems to break into a substation's network. From there it may be possible to change device configurations so that a danger condition that would otherwise open a circuit breaker to protect equipment gets ignored.

New systems are not necessarily more secure than modems. Increasingly, new devices deployed in substations may communicate with one another via low-powered radio, which does not stop at the boundaries of the substation. An attacker can reach the network simply by hiding in nearby bushes with his computer. Encrypted Wi-Fi networks are more secure, but a sophisticated attacker can still crack their encryption using readily available software tools. From here he can execute a man-in-the-middle attack that causes all communication between two legitimate devices to pass through his computer or fool other devices into accepting his computer as legitimate. He can craft malicious control messages that hijack the circuit breakers—tripping a carefully chosen few to overload the other lines perhaps or making sure they do not trip in an emergency.

Once an intruder or malware sneaks in through the back door, its first step is usually to spread as widely as possible. Stuxnet again illustrates some of the well-known strategies. It proliferated by using an operating system mechanism called autoexec. Windows computers read and execute the file named AUTOEXEC.BAT every time a new user logs in. Typically the program locates printer drivers, runs a virus scan or performs other basic functions. Yet Windows assumes that any program with the right name is trusted code. Hackers thus find ways to alter the AUTOEXEC.BAT file so that it runs the attackers' code.

Attackers can also use clever methods that exploit the economics of the power industry. Because of deregulation, competing utilities share responsibility for grid operation. Power is generated, transmitted and distributed under contracts obtained in online auctions. These markets operate at multiple timescales—one market might trade energy for immediate delivery and another for tomorrow's needs. A utility's business unit must have a constant flow of real-time information from its operations unit to make smart trades. (And vice versa: operations need to know how much power they need to produce to fulfill the business unit's orders.) Here the vulnerability lies. An enterprising hacker might break into the business network, ferret out user names and passwords, and use these stolen identities to access the operations network.

Other attacks might spread by exploiting the small programs called scripts that come embedded in files. These scripts are ubiquitous—PDF files routinely contain scripts that aid in file display, for example—but they are also a potential danger. One computer security company recently estimated that more than 60 percent of all targeted attacks use scripts buried in PDF files. Simply reading a corrupted file may admit an attacker onto your computer.

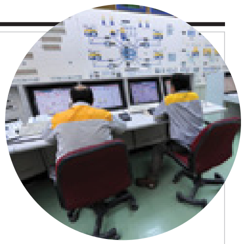
Consider the hypothetical case where a would-be grid attacker first penetrates the Web site of a software vendor and replaces an online manual with a malicious one that appears exactly like the first. The cyberattacker then sends an engineer at the power plant a forged e-mail that tricks the engineer into fetching and opening the booby-trapped manual. Just by going online to download an updated software manual, the unwitting engineer opens his power plant's gates to the Trojan horse. Once inside, the attack begins.

SEARCH AND DESTROY

AN INTRUDER on a control network can issue commands with potentially devastating results. In 2007 the Department of Homeland Security staged a cyberattack code-named Aurora at the Idaho National Laboratory. During the exercise, a researcher posing as a malicious hacker burrowed his way into a network connected to a medium-size power generator. Like all generators, it creates alternating current operating at almost exactly 60 cycles per second. In every cycle, the flow of electrons starts out moving in one direction, reverses course, and then returns to its original state. The generator has to be moving electrons in exactly the same direction at exactly the same time as the rest of the grid.

During the Aurora attack, our hacker issued a rapid succession of on/off commands to the circuit breakers of a test generator at the laboratory. This pushed it out of sync with the power grid's own oscillations. The grid pulled one way, the generator another. In effect, the generator's mechanical inertia fought the grid's electrical inertia. The generator lost. Declassified video shows the hulking steel machine shuddering as though a train hit the building. Seconds later steam and smoke fill the room.

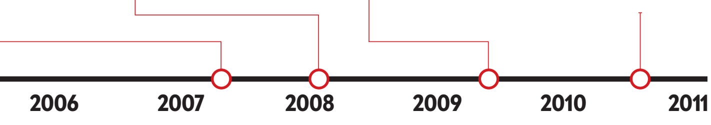
Industrial systems can also fail when they are pushed beyond their limits—when centrifuges spin too fast, they disintegrate. Similarly, an attacker could make an electric generator produce a surge of power that exceeds the limit of what the transmission lines can carry. Excess power would then have to escape as heat. Enough excess over a long enough period causes the line to sag and eventually to melt. If the sagging line comes



January 2008
A senior CIA official reveals that hackers have frequently infiltrated electric utilities outside the U.S. and made extortion demands. In at least one case, the hackers were able to shut off the power supply to several (unnamed) cities.

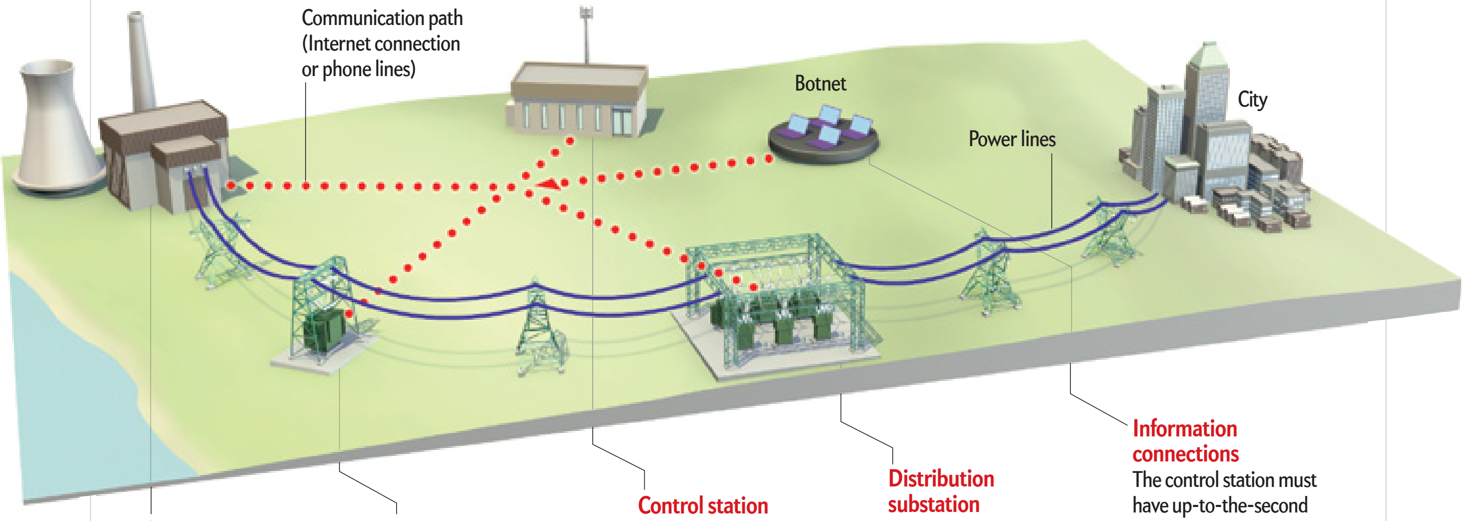
April 2009
The *Wall Street Journal* reports that cyberspies from "China, Russia and other countries" have penetrated the U.S. electrical power grid and left behind software that could be used to disrupt the system.

October 2010
Security officials in Iran, Indonesia and elsewhere report the discovery of the Stuxnet virus, a piece of malware designed specifically to interfere with industrial control systems made by Siemens.



Holes in the Grid

The modern electrical grid involves an intricate balance between the amount of energy needed by society and the amount generated at power plants. Dozens of components orchestrate the flow of electrons over distances of hundreds of miles, aligning the alternating currents and making sure no single component gets stretched beyond its limits. Any one of these parts might suffer from the attention of malicious actors. Here are some of the most troublesome choke points and the ways they might be compromised.



Generating station
It does not matter if the fuel is coal, uranium or even solar—electricity going into the U.S. power grid must alternate at 60 cycles a second, and it must enter perfectly aligned with the rhythm of the rest of the grid. An attacker might send instructions to a generator that throws its output off by a half-step, the electrical equivalent of throwing your car into reverse while heading down the highway at 50 miles per hour. The generator—like your car's transmission—will end up a smoking heap.

Transmission substation
Electricity coming out of generating stations comes at very high voltages—the better to avoid losses from electrical resistance en route. Transmission substations are the first step in bringing this voltage down. Many older stations have dial-up modems so that technicians can dial in and perform maintenance. Hackers can use these devices to access and change critical settings.

Control station
The grid's nerve centers, control stations monitor conditions throughout. They are also where supply meets demand. When demand goes up, prices follow, and a utility might activate more power capacity to provide additional supplies. Although the operations center of a control station is not supposed to be connected to the Internet, its business center must be. A hacker might burrow into the business side and use links between that side and operations to infect critical control systems.

Distribution substation
The last step before electricity goes into homes or businesses, these substations might combine power coming in from a few different power stations and send it out on dozens or hundreds of smaller lines. Newer stations might be equipped with wireless communications equipment—either radio signals or Wi-Fi. An intruder who hides just outside a station's walls could intercept traffic and mimic legitimate instructions.

Information connections
The control station must have up-to-the-second information about what is going on at every step of the process for technicians to make smart decisions about what to do next. Hackers with access to thousands of ordinary computers—a so-called botnet—could direct these machines to send messages that interrupt the flow of ordinary network traffic. Such a denial-of-service attack would mean that control operators would be making decisions based on old information—something akin to driving a car using the information you had 10 seconds ago.

into contact with anything—a tree, a billboard, a house—it could create a massive short circuit.

Protection relays typically prevent these shorts, but a cyberattack could interfere with the working of the relays, which means damage would be done. Furthermore, a cyberattack could also alter the information going to the control station, keeping operators from knowing that anything is amiss. We have all seen the movies where crooks send a false video feed to a guard.

Control stations are also vulnerable to attack. These are command and control rooms with huge displays, like the war room in *Dr. Strangelove*. Control station operators use the displays to monitor data gathered from the substations, then issue commands to change substation control settings. Often these stations are responsible for monitoring hundreds of substations spread over a good part of a state.

Data communications between the control station and substations use specialized protocols that themselves may have vulnerabilities. If an intruder succeeds in launching a man-in-the-middle attack, that individual can insert a message into an exchange (or corrupt an existing message) that causes one or both of the computers at either end to fail. An attacker can also try just injecting a properly formatted message that is out of context—a digital non sequitur that crashes the machine.

Attackers could also simply attempt to delay messages trav-

Illustration by George Retseck

eling between control stations and the substations. Ordinarily the lag time between a substation's measurement of electricity flow and the control station's use of the data to adjust flows is small—otherwise it would be like driving a car and seeing only where you were 10 seconds ago. (This kind of lack of situational awareness was a contributor to the Northeast Blackout of 2003.)

Many of these attacks do not require fancy software such as Stuxnet but merely the standard hacker's tool kit. For instance, hackers frequently take command over networks of thousands or even millions of ordinary PCs (a botnet), which they then instruct to do their bidding. The simplest type of botnet attack is to flood an ordinary Web site with bogus messages, blocking or slowing the ordinary flow of information. These "denial of service" attacks could also be used to slow traffic moving between the control station and substations.

Botnets could also take root in the substation computers themselves. At one point in 2009 the Conficker botnet had insinuated itself into 10 million computers; the individuals, as yet unknown, who control it could have ordered it to erase the hard drives of every computer in the network, on command. A botnet such as Conficker could establish itself within substations and then have its controller direct them simultaneously to do anything at any time. According to a 2004 study by researchers at Pennsylvania State University and the National Renewable Energy Laboratory in Golden, Colo., an attack that incapacitated a carefully chosen minority of all transmission substations—about 2 percent, or 200 in total—would bring down 60 percent of the grid. Losing 8 percent would trigger a nationwide blackout.

WHAT TO DO

WHEN MICROSOFT LEARNS of a potential security liability in its Windows software, it typically releases a software patch. Individual users and IT departments the world over download the patch, update their software and protect themselves from the threat. Unfortunately, things are not that simple on the grid.

Whereas the power grid uses the same type of off-the-shelf hardware and software as the rest of the world, IT managers at power stations cannot simply patch the faulty software when bugs crop up. Grid control systems cannot come down for three hours every week for maintenance; they have to run continuously. Grid operators also have a deep-rooted institutional conservatism. Control networks have been in place for a long time, and operators are familiar and comfortable with how they work. They tend to avoid anything that threatens availability or might interfere with ordinary operations.

In the face of a clear and present danger, the North American Electric Reliability Corporation (NERC), an umbrella body of grid operators, has devised a set of standards designed to protect critical infrastructure. Utilities are now required to identify their critical assets and demonstrate to NERC-appointed auditors that they can protect them from unauthorized access.

Yet security audits, like financial audits, cannot possibly be exhaustive. When an audit does go into technical details, it does so only selectively. Compliance is in the eye of the auditor.

The most common protection strategy is to employ an electronic security perimeter, a kind of cybersecurity Maginot line. The first line of defense is a firewall, a device through which all electronic messages pass. Each message has a header indicating where it came from, where it is going, and what protocol is used to interpret the message. Based on this information, the firewall allows some messages through and stops others. An auditor's job is partly to make sure the firewalls in a utility are configured properly so that they do not let any unwanted traffic in or out. Typically the auditors would identify a few critical assets, get a hold of the firewall configuration files, and attempt to sort through by hand the ways in which a hacker might be able to break through the firewall.

Firewalls, though, are so complex that it is difficult for an auditor to parse all the myriad possibilities. Automated software tools might help. Our team at the University of Illinois at Urbana-Champaign has developed the Network Access Policy Tool, which is just now being used by utilities and assessment teams. The software needs only a utility's firewall configuration files—it does not even have to connect to the network. Already it has found a number of unknown or long-forgotten pathways that attackers might have exploited.

The DOE has come out with a roadmap that lays out a strategy for enhancing grid security by 2015. (A revision due this year extends this deadline to 2020.) One focus: creating a system that recognizes an intrusion attempt and reacts to it automatically. That would block a Stuxnet-like virus as soon as it jumped from the USB stick. But how can an operating system know which programs are to be trusted?

One solution is to use a one-way hash function, a cryptographic technique. A hash function takes a fantastically huge number—for example, all the millions of 1s and 0s of a computer program, expressed as a number—and converts it to a much smaller number, which acts as a signature. Because programs are so large, it is highly unlikely that two different ones would result in the same signature value. Imagine that every program that wants to run on a system must first go through the hash function. Its signature then gets checked against a master list; if it does not check out, the attack stops there.

The DOE also recommends other security measures, such as physical security checks at operator workstations (think radio chips in identification badges). It also highlights the need to exert tighter control over communication between devices inside the network. The 2007 Aurora demonstration involved a rogue device tricking a generator's network into believing it was sending authoritative commands. These commands eventually led to the destruction of the generator.

These worthwhile steps will require time and money and effort. If we are going to achieve the DOE roadmap to a more secure grid in the next decade, we are going to have to pick up the pace. Let us hope we have even that much time.

MORE TO EXPLORE

Roadmap to Secure Control Systems in the Energy Sector. Jack Eisenhauer et al. Energetics Incorporated, January 2006. www.oe.energy.gov/csroadmap.htm

Security of Critical Control Systems Sparks Concern. David Geer in *IEEE Computer*, Vol. 39, No. 1, pages 20–23; January 2006.

Trustworthy Cyber Infrastructure for the Power Grid. Multiuniversity research project funded by the U.S. Department of Energy. www.tcipg.org

What Is the Electric Grid, and What Are Some Challenges It Faces? U.S. Department of Energy. www.eia.doe.gov/energy_in_brief/power_grid.cfm

SCIENTIFIC AMERICAN ONLINE
For an extended look at the history of electronic attacks on physical structures, visit ScientificAmerican.com/jul2011/lights-out