COMPUTERWORLD

Print Article Close Window

What if the smart grid has stupid security?

Richard Power

May 11, 2010 (CSO)

As I write this piece, the economic future of the Gulf coast region is dangling on a fragile thread over a fathomless abyss, as a volcanic eruption of oil threatens unprecedented and almost unimaginable consequences. Whether the cause of this tragedy is revealed to be human error, system failure, corporate malfeasance or terrorist attack, the event itself highlights the profound impact of infrastructure-related disaster.

As I write this piece, business media journalists are trying to get their minds around the story of what happened to the New York Stock Exchange recently, when the Dow plunged almost 1,000 points in less than an hour. Theories, rumors and spin abound.

Atlantic Monthly's Wire blog articulated five lessons (5-7-10), including the question: Are we ready for a cyber attack? Of course, that question (the answer to which is an emphatic NO) avoids another relevant question, "Was this a cyber attack?" And the answer to that question, as we know from the Martin Luther King Day telephone system crash (see my book Tangled Web: Tales of Digital Crime for something other than the official story), as well as some other events arising from mysterious "glitches," we may never know (or be able to admit we know).

And as I write this piece, Richard A. Clarke, whose heroic Against All Enemies opened the eyes of some (not enough) people to major governance failures related to the 9/11 attack (pre- and post-), is on a book tour for his new book, Cyber War.

In an interview with National Public Radio's Terry Gross (4-19-10), Clarke stressed the vulnerability of infrastructure: "A cyber attack could disable trains all over the country & It could blow up pipelines. It could cause blackouts and damage electrical power grids so that the blackouts would go on for a long time. It could wipe out and confuse financial records, so that we would not know who owned what, and the financial system would be badly damaged. It could do things like disrupt traffic in urban areas by knocking out control computers. It could, in nefarious ways, do things like wipe out medical records."

Also seeMichael Assante and Mark Weatherford's 4 things the roman aqueducts can teach us

about securing the power grid on CSOonline.com

You are no doubt familiar with the CBS Sixty Minutes story (11-8-09) on Cyber War that highlighted the attacks on the Brazilian power grid; and you no doubt recall when CIA analyst Tom Donohue referenced declassified information on successful cyber attacks on several non-US cities via the Internet (PC World, 1-19-08). Let's not wait for the big power grid security story of 2010. The time for truth and consequences for critical infrastructure is already here.

To get some real world answers to real world questions on power grid security, I turned to a friend and colleague, Seth Bromberger. He has been involved in security for more than sixteen years, and in cyber security for a major utility for five years. He is also on the Board of Directors of EnergySec, "a private forum of information security, physical security, audit, disaster recovery and business continuity professionals from energy industry asset owners."

Bromberger and Steve Parker, a fellow member of the EnergySec Board of Directors, recently shared their perspectives with me.

Richard Power: What is EnergySec? Who is involved? What is its mission? How is it structured? Why should people pay attention? Who should get involved?

Seth Bromberger: EnergySec is a non-profit corporation focused on information sharing and awareness as they relate to security issues in the energy sector. Our mission is to facilitate information sharing, open communication, and coordination among energy sector asset owners (utilities and others who own power generation, transmission, or distribution equipment), government agencies, academia and research institutes, and product manufacturers for the purpose of strengthening the security of critical infrastructure in the electric and energy sectors. EnergySec grew from a series of informal meetings among security professionals from several northwestern utilities into a 300+ member organization within two years. We have kept the bureaucracy to a minimum in order to ensure that the barrier to entry is low: there are six members on a board of directors who oversee general activities, such as our secure communications facilities and our annual conferences.

EnergySec is important because it really is the first true example of a public-private partnership in the energy sector. We have members from all around North America sharing security information, from vulnerabilities and suspicious activity reports to organizational and regulatory frameworks, in an open, non-competitive, and professional environment where participants have been pre-vetted according to specific membership criteria. As an example of the value of our information sharing program, we've been able to exchange near-real-time situational awareness data on several occasions so that members can implement shared protections against emerging threats and vulnerabilities. The latest McAfee DAT issues, for example, were detected by a member and relayed to the community almost an hour before McAfee started contacting large companies.

EnergySec membership is open to members of any organization with a commitment to improving energy sector and critical infrastructure security. Membership is free for asset owners and government agencies, and we have a fee-based membership program for other interested parties. There is a fairly comprehensive terms of service that helps guarantee the confidentiality of the information that is provided by the members.

More information may be found on our website, http://www.energysec.org.

Explain the differences in roles between ES-ISAC and EnergySec. Do the two interact? What distinguishes one from the other? How do they compliment each other?

Bromberger: The ES-ISAC and EnergySec have very strong ties to each other. EnergySec supports and complements existing ES-ISAC programs and can disseminate information in cases where the ISAC can't. The ISAC is run by the North American Electric Reliability Corporation

(NERC), who is also the industry regulator. There are mandatory reporting requirements for the ES-ISAC. What EnergySec seeks to do is to provide a set of forums where members can exchange information voluntarily, without fear of reprisal, and informally, without worrying about full knowledge or formal approvals. The informal information exchange results in faster dissemination of information with the understanding, sometimes, that the information can be ambiguous - but that's where the ISAC provides a complementary service. Via the NERC Hydra program, our members work with the ISAC to apply industry expertise to important announcements that are sent through formal channels to NERC and ISAC members.

Our membership therefore gets the benefit of a rapid, informal discussion of an issue, along with a chance to assist in crafting the more formal announcement that NERC and the industry require from the ISAC.

All security professionals have to come to grips, in one way or another, with the full spectrum of risks and threats, from petty cyber crime to critical infrastructure attacks, from disgruntled employees to international cyber criminals and state-sponsored cyber warriors. What is your perspective on this spectrum of risks and threats? How do you sort it out in your work? What advise do you offer cyber security professionals in the energy sector and other critical infrastructure areas?

Some people minimize the more serious threats, and overemphasize those low-level threats that are, frankly, easier to detect, easier quantify and easier to mitigate. In our current environment (and it will likely worsen before it improves), this kind of denial kind be very dangerous.

Bromberger: Our industry faces the same threats and risks as most other critical infrastructures, and we have different ways of analyzing the impact of these threats and risks. My perspective is that the analysis of threats should focus on the impact and likelihood (probability of occurrence) to the organization in terms of prioritizing resources.

To help clarify, consider these two graphs.

Figure 1 shows a desired state for an arbitrary set of threats: the threats with the higher impact on the organization have a lower probability of occurring.

Figure 2 shows a suboptimal curve: there is a subset of threats that have a high impact relative to their probability of occurring. This indicates that resources should be applied to decrease either the impact of those threats or their probability of occurrence.

When one looks at the problem in these terms, some interesting conclusions may be drawn. For instance, there are some threats that have a sufficiently high impact, but are outside of a single organizations ability to mitigate. An example in our industry might be the detonation of a nuclear device by an adversary, and its associated impact on the electric grid. If this threat is to be mitigated, it will require a combined effort among several organizations, including government, academia, and asset owners, to come up with a cost-effective, scalable, relevant solution. (The observant reader will have discovered that the organizations listed in the example are all part of the EnergySec membership base.)

Before we can have a discussion about whether or not we're applying the correct emphasis to a set of threats based on their "seriousness", we have to have agreement on what makes a threat serious or not. Historically, this has been one of the biggest challenges in any industry, since this knowledge is typically generated and held at classified levels within the U.S. Government. As an industry, and via organizations like EnergySec, we're making progress in exchanging information that will be helpful to specific companies and the sector as a whole, while ensuring the proper confidentiality and sensitivity of that information.

In the late 1990s, many of us started pushing hard on critical infrastructure protection. There was

some momentum. But in some ways, I suggest that elements of the critical infrastructure, e.g., the financial system and the power grid, are less secure than they were a decade ago. The systems were insecure but also outmoded, and of course, the push to modernize has outdistanced the push to secure (as it always will).

I am not asking to ascribe to my characterization, but to offer your own: generalizing, what are the facts on the ground in regard to the cyber security of the power grid and for critical infrastructure as a whole? Moving forward? Too slowly? Going around in circle?

Steven Parker: As a whole, the power grid is more secure today than it was a decade ago. There has been a tremendous amount of work done over the past several years towards improving the security of the systems operating the power grid. In addition to the general increase in awareness of security issues, this effort has been supported, in part, by the CIP standards. The work to comply with CIP has given cover (and funding) to security professionals working hard to improve security.

The response to the CIP standards has improved security, but in many cases, such improvements are merely a side-effect of a focus on compliance. At best, a compliance focus can only take you where the standards go. The current CIP standards are focused only on the most critical transmission facilities, and ignore the areas that will be of greatest concern as we move toward a smarter more distributed power grid.

Ultimately, security cannot be legislated. Regardless of the quantity, quality, and scope of security standards, the job of securing infrastructure falls to those who own and operate it. Although there are pockets of security excellence within the electric industry, it is clear that the need for cyber security is not universally understood and accepted.

Also see Ira Winkler's I was wrong, there probably will be an electronic Pearl Harbor

The interconnected and interdependent nature of the power grid amplifies "weakestlink" vulnerabilities, so this is a big issue. Since there are strong economic reasons for the rush to new "Smart Grid" technologies, it is likely that functional advances in technology will outpace advances in security practice for the foreseeable future. There is a good chance that the next decade will give back the gains made over the last one.

There is a lot of talk about Smart Grid. But there more one inquires, the more one realizes that this is a buzz word that has come to mean many different things to many different people. What does it mean to you in its broadest sense and in its most specific sense? What new security issues does it bring into focus? What perennial security issues does it exacerbate?

Parker: In its broadest interpretation, the term Smart Grid simply refers to modern information technologies being applied to existing processes in the electric sector such as meter reading, automatic generation control, and transmission and distribution system operation. However, there is a deeper meaning, an underlying vision, which will be transformative in ways we cannot possibly predict.

Just as the Internet can be seen simply as a collection of technologies for the exchange of information, the Smart Grid can be viewed as merely a system for the movement of energy. However, just as the Internet has transformed the way information is produced and consumed, the Smart Grid may transform the way energy is generated, distributed, and used. As envisioned, the Smart Grid will enable realtime, market-based responses to energy supply and demand on a micro-level, down to individual appliances. New telemetry devices will monitor conditions across the grid in real-time, providing sub-second response time to disturbances. The ability to monitor and respond automatically will enable generating units and transmission facilities to operate with much smaller tolerances, improving efficiency.

These changes will increase dramatically the attack surface and will enable new and innovative ways to disrupt the flow of energy. In the past, the security of the grid was based on isolation and obscurity. In the future, the ubiquity of Smart Grid elements will make physical and electronic isolation impossible. Instead of needing to attack a control center or major transmission substation, it may be possible to create grid disturbances via mass compromise of Smart Meters or Smart Grid enabled appliances. The Smart Grid will also introduce new risks related to financial fraud, privacy, and even extortion.

Richard Power is a Distinguished Fellow at Carnegie Mellon CyLab and a frequent contributor to CSO Magazine. He writes, speaks and consults on security, risk and intelligence issues. He has conducted executive briefings and led professional training in forty countries. Power is the author of five books. Prior to joining Carnegie Mellon, Power served as Director of Security Management and Security Intelligence for the Global Security Office (GSO) of Deloitte Touche Tomatsu and Editorial Director of the Computer Security Institute.