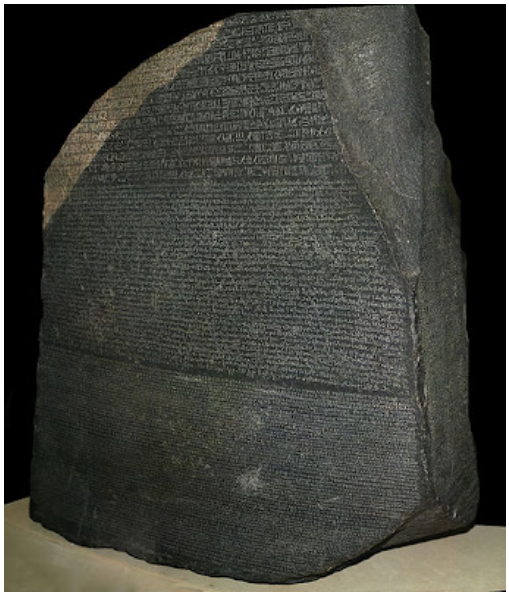
CyBlog
Security, Privacy and Mobility in the Information Age
Carnegie Mellon University CyLab

Wednesday, March 3, 2010

RSA 2010: Hacking the Smart Grid -- Myths, Nightmares & Professionalism



The Rosetta Stone Photo Credit: Hans Hillewaert CC-SA-BY-3.0 (Theme of RSA 2010)

NOTE: What do we mean by smart grid? Speaking on "Investing in Our Energy Future" at a Gridweek event on 9-21-09, Secretary of Energy (and Nobel prize winning physicist) Steven Chu offered a worthy definition: “Dynamic optimization of grid operations and resources. Incorporation of demand response and consumer participation.” (For your convenience, I have embedded Secretary Chu's full presentation at the end of this post.) Ah, but what about it's security?

RSA 2010: Hacking the Smart Grid -- Myths, Nightmares & Professionalism

By Richard Power

The implementation of Smart Grid is in the vital national interest of the U.S., and all other industrial (and post-industrial) nations; it is vital both in terms of energy security and climate security, which, of course, means Smart Grid is also vital to economic security.

Any nation that wants to compete in the 21st Century needs Smart Grid. Indeed, any nation that wants to survive in the 21st Century needs Smart Grid.

In framing the issue for this RSA 2010 session on "Hacking the Smart Grid," Gib Sorebo of SAIC (one of CyLab corporate partner, BTW), cited several Smart Grid drivers, most notably, resiliency and reliability and reduction in carbon emissions, as well as several Smart Grid challenges, including the integration and distribution of renewables, the complexity of transmission networks, how to eventually provide infrastructure for electric vehicles (hopefully much sooner than later), and yes, what to do in regard to cyber security.

A smart grid, after all, is not necessarily a secure grid.

Smart grid is full of innovation, and it is being designed and implemented swiftly (or certainly should be), and innovation and urgency only tend to exacerbate security issues.

Furthermore, the issues swirling around the cyber security of power grids, whether legacy, smart or in transition, have shifted from the theoretical to the down and dirty. A decade or so ago, talking about attacks on the power grid were mostly speculative, but a decade ago, well, that was a century ago.

Some incidents have even ended up in the headlines:

In a rare public warning to the power and utility industry, a CIA analyst this week said cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities. Washington Post, 1-19-08

A power failure has blacked out Brazil's two largest cities and other parts of Latin America's biggest country for more than two hours, leaving millions of people in the dark after a huge hydroelectric dam suddenly went offline. All of neighbouring Paraguay also lost power, but for only about 20 minutes ... The blackouts came three days after the CBS's 60 Minutes news programme in the US reported that several past Brazilian power outages were caused by hackers. Guardian, 11-11-09

So what is really happening in the space of Smart Grid cyber security?

The RSA 2010 panel Sorebo moderated consisted of Matthew Franz, Principle Security Consultant, SAIC, Matthew Carpenter, Senior Security Analyst, InGardians and Seth Bromberger, Information Systems Security Manager, PG&E.

For those of us who have firsthand knowledge of the decade-long struggle to promote critical infrastructure protection for existing systems, this few brief excerpt from their discussion offer a tantalizing, but humbling glimpse into this profoundly promising, yet clearly perilous undertaking glibly dubbed Smart Grid:

Seth Bromberger, PG&E: *The research is being done on security in these components is not necessarily new. We are talking about encryption, key management, strong authentication. These are not new concepts. The devil is in the implementation. Where you have vendors, manufacturers and product developers taking short-cuts, or implementing poorly, that's where we are finding these vulnerabilities ...*

Matthew Carpenter: *We need pen-testing out of everybody. That doesn't mean everyone in the audience should go disassemble our firmware and look for buffer overflows. But there are so many different layers in this very complex system, and sometimes we just need critical thinking done about how we implement x, or whether this is a great feature to have. For instance, some utilities are thinking about having [an automated process by which] a person's credit report could impact whether or not that person can actually have power. This may not be the smartest choice to have automated throughout the system, without checks and balances in place. But it is actually something that has been pushed forward as a To-Do. So I can break into meters using this technology, but what about the guys who can influence credit reports? Or how about getting in between the communication of these credit reports? How can I manipulate the system? So we need everyone in the entire implementation of Smart Grid to be thinking critically about this could be abused. If I turn on this security protection, how could it be abused to cause more damage? How do I turn on anti-tampering technology in this device? OK, now what? So if I have anything higher than a 1.0 on some scale, I just shut down my entire neck of the woods? OK, maybe not the best bet. We need critical thinking done by everyone who has purview into the system, and good communication of "Well, maybe this isn't such a good idea." We need to open up that flow of communication.*

Gib Sorebo, SAIC: *For a long time, the [utility] industry has had a reputation of being tight-lipped about incidents, even about vulnerabilities that have been discovered (and, of course, it is not the only one). There have been a lot of bad feelings, recently, about some disclosures related to meters, people were branded not as terrorists, but it was almost that kind of thinking; in other words, "You guys are destroying the industry by revealing information about these vulnerabilities." And then we have the issue of everyone complaining that incidents are never reported to the regulators, or to the industry, or to whatever. Is there a middle ground? Obviously, we do not want to disclose vulnerabilities right away for an infrastructure that takes a long time to change, but where can we go with that?*

Matthew Franz, SAIC: *I am still kind of traumatized by my involvement with the disclosure of some SCADA vulnerabilities. Speaking of [being called] terrorists, I remember a utility software vendor that ... I gave a case study back in 2006 about some ... protocol vulnerabilities that I worked through the CERT process ... To paraphrase, what I was told was that by telling US CERT, i.e., giving them the details, and how to reproduce it, etc., and having US CERT release an advisory, we were arming the terrorists ... Just as a bell-weather of where we are I went to four or five of the leading meter AMI vendors this morning, and I looked for their /security site. The kind of site that Microsoft and Cisco and others have, in terms of how you go about reporting vulnerabilities, and only one of these meter vendors had the contact information, the GPG keys, etc., and that is the first step if that researcher wants to do the right thing, to get a hold of these vendors, and there is no way to do that ... The level of transparency you have is far less than Cisco or Microsoft ...*

Matthew Carpenter, InGaurdians: *We have to be more cautious than a Microsoft vulnerability disclosure. If you know me, you have probably heard me talk about responsible disclosure being a communication mechanism for vulnerabilities, but also a way to keep vendors in line. For IT, I think that makes a lot more sense. We have to be more cautious because of the impact in this arena. But we need to have fluid motion for our vulnerability research, we need to have a way to disclose to a vendor that there is an issue. We need to be able to have discourse throughout the utility space, so that effected customers have an early warning, "Hey, something's up, we've got a fix that's in the works, but just to give you some warning, when this comes out, you need to put it into test immediately, and in a certain amount of time, roll it out ... I remember hearing a vendor say, "Think about thirty days." I said, "That seems a little long, but if get a vulnerability notification, and within thirty days you have a fix out, well, you're better than Microsoft." But no, thirty days was actually the number to push out the patch from the time they clicked the button. "Whoa," I said, "we have some problems in our viewpoint into vulnerability handling." Disclosure needs mechanisms ...*

Seth Bromberger, PG&E: *You talked about making sure that the affected customers are made aware of the vulnerability. I am all for knowing ... The challenge that we have is that the lines dividing customers and non-customers are very blurry when it comes to things like critical infrastructure. I could see an argument that anyone who consumes power is a customer of the vendor whose control systems help deliver that power. From a utility perspective, I would say that the utilities are probably the customer base that the vendor would be beholden to. So when we talk about disclosing vulnerabilities ... to what end is the researcher disclosing, is it to feed ego? If so, that is probably not the most responsible way of doing it. Sending out on one of the*

public lists, information on a zero-day in a control system handling power or manufacturing is probably not the best way to people who are going to be impacted by it. And someone could argue that everyone is impacted by it, but I would challenge [by saying] that the average power consumer doesn't have any ability to effect the change and necessary remediation in those systems. So there are mechanisms the word to the right people, and again, I would say from my perspective, knowing about it is better than not knowing, so if the only way to get it out there is full disclosure, well, if it is actionable, I can take action, if I don't know about it, I can't do anything, and we can't pressure the vendors to fix it. But ultimately the utilities are in the position here of being the consumers of the product, and not necessarily the manufacturers of the product, and so the leverage we have is as a paying customer ... But it also puts us at a little bit of a disadvantage in that we need to be able to have the influence with our vendors to actually affect this change. We can't do it by ourselves.

Secretary Chu Grid Week

View more presentations from Glenn Klith Andersen.

Posted by Carnegie Mellon CyLab at 11:09 AM
Labels: Cyber Security, Cyber Security News, CyBlog, Information Security, RSA Conference, RSA Conference 2010

Newer Post Home Older Post