Cyber-Security Considerations for the Smart Grid

Sam Clements, *CISSP;* Harold Kirkham*, Fellow, IEEE*

***Abstract*— The electrical power grid is evolving into the "smart grid." The goal of the smart grid is to improve efficiency and availability of power by adding more monitoring and control capabilities. These new technologies and mechanisms are certain to introduce vulnerabilities into the power grid. In this paper we provide an overview of the cyber security state of the electrical power grid. We highlight some of the vulnerabilities that already exist in the power grid including limited capacity systems, implicit trust and the lack of authentication. We also address challenges of complexity, scale, added capabilities and the move to multipurpose hardware and software as the power grid is upgraded. These changes create vulnerabilities that did not exist before and bring increased risks. We conclude the paper by showing that there are a number mitigation strategies that can help keep the risk at an acceptable level.**

***Index Terms*— cyber security, mitigations, smart grid, smart meters, vulnerabilities**

I. INTRODUCTION

THE SMART GRID will add a layer of control and communication to the grid in places where it does not now exist. The capability to perform control from remote locations or autonomously will allow distribution systems to be increasingly automated and transmission systems to be monitored at the regional scale. But these capabilities come at a cost: there will be an increased vulnerability to cyber attack.

As it happens, there are several sorts of attacker whose existence can be plausibly postulated. Some utility customers might attack the system with the goal of reducing their electricity bill. It may be that such an attack need communicate no further than the nearest advanced metering infrastructure (AMI) connection. Some attackers may wish to enrich themselves – by accessing the utility billing system or by blackmail. That blackmail may be aimed at the utility ("pay me or else") or even at some other customer, whose privacy has been breached through access to their power use. Yet other threats may come from someone with more nefarious motives, with the goal of shutting down the network.

This paper presents a review of some options for helping the smart grid be resistant to such attacks. It proceeds as follows. First we will highlight existing vulnerabilities in the power grid. Next, we will describe the new vulnerabilities introduced by adding smart grid technologies to the existing power grid. The paper concludes with some mitigating strategies to manage the increased risk.

Manuscript received **********. This work was carried out at the Pacific Northwest National Laboratory through an agreement with the US Department of Energy.

Sam Clements is with the Pacific Northwest National Laboratory, Richland, WA 99352 USA (phone: 509-375-3945 e-mail: samuel.clements@pnl.gov).

II. BACKGROUND

There are two important areas that need to be understood before we can proceed. The first is what we consider the difference between the today's power grid and the "smart grid." The second is how the computer systems in the power grid or, more generally, industrial control systems (ICS) differ from information technology (IT) computer systems.

The term "smart grid" seems to imply that today's electrical power grid is somehow dumb. This is not really the truth. The tens of thousands of km of high voltage lines could not be managed without extensive measurement, communication and control. It is true, however, that additional measurements could be made, and with the information from these measurements, different control strategies might be implemented. At the very top of the hierarchy of power delivery, wide area measurements could reveal system behavior on a regional scale that is presently hard to observe. At the very bottom of the hierarchy, in the customers' homes, measured data sent to the utility might help bring about improved energy use. Redistribution (in time, not space) of the customer load might enable delivery with lower losses, and operation without the use of expensive peaking generators.

The term "smart grid" can mean different things to different people, but the goals are always the same: improved efficiency of delivery and improved availability of power. Achieving these goals will require additional communications and control resources to be deployed in the power grid. It is the security of these additional resources (in the IT sense) that is the subject of this paper.

However, the grid is not just an IT application. NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security* provides excellent insight into the differences, and gives reasons why IT solutions tend not to meet the requirements of ICS environments. This publication covers differences in availability, risk, architecture, interaction with the physical world, resource constraints, communications, change management, managed support and equipment lifespan.

The challenge of attempting to list all the possible vulnerabilities of the utility control system would be daunting. Rather than make that attempt, we will focus on categories of vulnerabilities that are unique to the power grid, or are known to be relevant to industrial control systems (ICS) rather than to traditional information technology (IT) type of systems.

978-1-4244-6551-4/10/$26.00 ©2010 IEEE

III. Current Vulnerabilities

Surprisingly, it is probably not possible to implement many of today's IT security mechanisms on the existing electrical power grid. We refer here to the computer system used for SCADA, the supervisory control and data acquisition systems used for system operation, not to the computer systems used for billing. The difficulty arises because most of the devices in the electrical power system were purpose-built and do not have extra capacity to perform security functions. For the most part, the utilities have wanted to own the communication systems they operated, and they have not wanted to own any more than was necessary. For many individual distribution automation functions in particular, the minimum communication system was implemented. Load management might be done by power line carrier, at a speed of a few bits per second, if "speed" is a word that is appropriate. Other functions might take advantage of a few seconds per day of time on a customer telephone. Yet others could be done via signals buried in broadcast radio.

None of these mechanisms had any headroom, and no new functions or new control points could be added. The utility distribution communications world was perennially bandwidth limited. In this environment, a rather basic data compression algorithm known as "report by exception" allowed better use of the channel. But the channels that were built could not accommodate the extra information required for (say) secure authentication.

It is also important to note that the lifespan of these systems is much longer than, say, a desktop computer. Where business-IT systems are typically on a 3 to 5 year replacement cycle an ICS is expected to last 15 to 20 years or more. This means two things. First, equipment that was built one cycle ago and is still in service is likely incapable of dealing with today's security mechanisms. Second, what are now "modern" security mechanisms will be around for one cycle, long enough to become out of date.

The protocols and communications that controlled the electrical power grid of yesterday operated on implicit trust. The danger of relying on this is trust becomes apparent when it is realized that anyone could send any command to any device on the network, and that device would do what it is told if the command was a valid command. There was no verification that the command came from a trusted entity.

So at a time of his own choosing, an attacker could send the command to open breakers in all the substations on a network to which he has access; and all the breakers would open. The protocols do not have the capability to identify who issued the command, or any way to verify that it was authorized.

Control systems are also vulnerable to spoofed data. Most of the communications are device-to-device where the status of one device causes another device to act. If the data is spoofed and a false status is sent, the second device will act in a way that it should not. For example, a level sensor might detect the state of a tank that is filling and send a message to shut off a pump or open a valve once the tank reaches a certain point. If the message to the pump is spoofed, saying it is not full when it really is, the tank will overflow. Depending on the contents of the tank, this could have a serious impact.

A non-malicious but useful example of this is illustrated by an outage created at the Hatch nuclear power plant. A machine on the company network that monitored and synced with a system on the primary control system network was patched and rebooted. The patch zeroed out some values of the system and then synced with the control system. The system interpreted the message to mean that the reservoir was empty and shut down the plant [1]. Though this was not malicious, it illustrates the consequences of bad data and the damage that insufficient integrity checking can do.

IV. New Vulnerabilities

In the past decade there has been a move in industrial control systems—including the electrical power grid—away from proprietary hardware and software to open-standard off-the-shelf products. There are significant economic advantages to the change, but with it come all the vulnerabilities of commercial-off-the-shelf (COTS) products.

As more COTS products are deployed, the control systems networks begin to look more and more like typical IT networks. A common problem is that the two responsible departments don't always talk. They come from different schools of thought, and can easily cause each other problems because they don't know how to meet each other's needs and communicate effectively. A good example of this problem is the typical IT practice of patching systems. An IT professional uneducated in control systems would look at a control system and immediately want to set up a patching server and push out patches to all the hosts. The control systems engineer knows that with patches comes the necessity of rebooting the machine. This "unplanned outage" could have catastrophic effects, as we saw above. On the other hand control systems engineers, being highly trained in running the control system, often don't have the expertise in implementing security solutions typically performed by IT personnel. So without understanding each other's need and capabilities, either side can introduce unnecessary vulnerabilities.

We have already observed that many control devices in the power grid were purpose-built to perform one function and one function only, and that many of the communications systems that have been installed are also single-purpose. The economies of continuing this practice have changed, and many multipurpose devices are now being used to perform the same function. Instead of a dedicated low-speed serial communication link there is a network card running TCP/IP connecting a device that now has an ftp server, a telnet client, and a web server embedded. These added capabilities provide ease of configuration and enhanced management capabilities, but also open new avenues to attack the system.

The mere scale of control that will come with the developing smart grid is a new vulnerability. AMI deployments are planned that will range in the millions. Homes will have smart meters that may have remote connect/disconnect switches. The intent of these switches is to limit the number of truck rolls necessary for a utility—a

customer disconnect or reconnect could be accomplished remotely, thus providing quicker service and saving the company money. The seriousness of the vulnerability comes through the large amount of central control. An example is furnished by an incident that happened in the summer of 2009 that left 18,000 homes without air conditioning for a number of hours. It was attributed to operator error. [2] It seems possible that a hacker with access to the appropriate part of the system could have done the same.

Smart meters and demand response applications will read energy usage multiple times an hour, with the goal of bringing better efficiency to power grid operations—but at the same time creating privacy concerns for the consumer. Historically, electricity usage was read once a month. At that aggregate level, no more than the amount of electricity used was revealed. Having a smart meter with two-way communication capabilities can reveal more. It is simple to see when a residence is occupied and, depending on the sophistication of the analysis tools, even what types of appliances are being used in the residence e.g. television, microwave, fans, water heater, clothes dryer, etc. Using this data attacks can be planned, from simple robbery when no one is home to more sophisticated attacks that might be able to manipulate demand response pricing signals for financial gain, or even to cause instability in the grid.

A large utility will have hundreds of substations with equipment at each site that must be managed and maintained. Implementing advanced metering infrastructures could increase this number into the tens of millions of devices. Clearly, the manner of doing business must change. There will need to be automated ways to manage and maintain all these devices and, since they will not all be on utility property, ways to detect tampering or destruction of property. These requirements greatly increase the complexity and scale. Complexity breeds vulnerability.

Along with adding complexity, smart meters dramatically increase the number of access points into a network. Where a neighborhood used to only have one access point to the utility communication and control system, via the substation, with the smart grid it will have thousands; one for each residence with a smart meter. That this is a problem is suggested by the fact that the US government has been trying to consolidate its number of access points into the Internet because it was too hard to monitor and secure. [3] There is a lesson to be learned.

Market manipulation for monetary gain is likely to become a problem if proper precautions are not taken. The young Internet in 1995 was a vulnerable but relatively benign environment compared to what it is today. Most of the malware of that era was written by individual researchers or hackers trying to prove something, not well funded organized groups whose motivations are espionage, power and financial gain. The reason these groups formed was an indirect consequence of Netscape releasing SSL v2.0 (Secure Sockets Layer). SSL enabled the encryption of sensitive communications which enabled e-commerce and the thriving Internet ecosystem we have today. The problem is that the more information that began traversing the network the more valuable it became. The increased value attracted both good and bad actors. The same is true of the smart grid. As more information becomes available it will enable markets and opportunities that were not previously possible for both good and bad ends.

Today there are those that cheat the system. Billions [4] are lost every year because of hackers. In a like manner, smart grid enabling technologies will create a marketplace for electrical power that is much more dynamic and widespread than it is today. If proper care is not taken it too may become a hostile environment similar to the Internet of today, yet it will have physical world ramifications.

V. Mitigation Strategies

A number of steps can be taken to mitigate many of these vulnerabilities. A combination of many of them will provide defense-in-depth solutions that will be much superior to any single strategy or mitigation. We will address a few of them now.

Utilities should carefully consider the amount and type of data they collect and then collect only the minimum required to accomplish their desired ends. In recent years, retailers have learned the value of keeping limited amounts of data. It used to be that organizations requested and retained as much information as possible about their customers–including social security numbers and credit card information–when customers made a transaction. This trend changed after a number of highly publicized computer system compromises and the theft of millions of credit card[5] and social security numbers[6], with subsequent lawsuits. Lawmakers are now holding these organizations liable for computer compromises. As a result many organizations have modified and minimized the information they collect and many are now not collecting or retaining social security numbers or credit card information. You may have noticed in most retail establishments you no longer give your card to the checker, you swipe it yourself. This is because insurance companies acknowledge the reduced risk of fraud where employees do not handle the credit cards and it reflects in the premiums they charge. It is also interesting to note that the retailer's system verifies only that there are sufficient funds/credit available on the card before approving the transaction. They never store or retain the credit card data. Utilities would be wise to think carefully about what information they need from consumers to gain the efficiencies or economies of an intended smart grid technology and then obtain and retain only the minimum information necessary.

A cultural change that needs to take place to help secure these systems is that control system engineers and IT security need to become partners. We mentioned before that each comes from a different school of thought yet as control systems are upgraded they begin to look more like IT systems. There are still fundamental differences in the requirements and constraints of the various systems, but the technologies used to obtain the various ends begin to look very similar. IT personnel have been dealing with IT security problems for many years. These same problems will begin to emerge and

become more prevalent in the control systems world. Anything that can be done to help these two organizations communicate better and more freely will help remove vulnerabilities from control systems.

Segregation between functions currently exists in the electric power grid. It was not built that way as a security feature, but as a side effect of purpose-built systems. The challenge now is to use the new interoperable systems in beneficial ways, but to still segment the network so that when one section is compromised the entire system is not affected.

As we discussed earlier the life cycle for many of these components is 15 to 20 years. Technologies that are being deployed today must have the ability to be upgraded. Optimally, this ability will exist for both the hardware and the software but more importantly in the software. New vulnerabilities will be found that need to be fixed. Without the ability to upgrade, the utility will either have vulnerable equipment for many years or have to replace equipment out of the normal lifecycle. Neither of these are attractive solutions.

Security needs to be built in. It needs to be a part of the development process from the ground up. When much of the existing power grid was built, security was not on anyone's radar. Hence security for the existing power grid must be added and it is proving very difficult. Yet even today, many devices coming off assembly lines have limited security features built in. Consumers need to start being more vocal, and demand that vendors build in security as well as test it to make sure that it is not exploitable with known vulnerabilities. Bolt-on security can only do so much, and often can do very little.

Get involved in security for the smart grid. There are a number of organizations that have significant time examining the challenges of securing the power grid and other critical infrastructure. There seem to be more every day but here are some of the big ones.

The National Institute of Standards and Technology (NIST) produced Special Publication 800-82, which was highlighted earlier. NIST is also developing the Interagency Report 7628 entitled *"Smart Grid Cyber Security Strategies and Requirements"*. This largely volunteer effort focuses on the technologies in the smart grid and the interfaces between the various components and how to secure them. It is a crosscutting addition to Smart Grid Interoperability Standards and a valuable reference for a holistic view of the challenges facing the smart grid.

AMI-SEC focuses specifically on the security of advanced metering infrastructure and smart meters. This group is very active. It has produced useful documents including *AMI System Security Requirements* [7] and *AMI Security Profile* [8] These documents provides actionable guidance on how to build-in and implement security for AMI.

The United States Department of Energy (DOE) has long been aware of the challenges, facing the energy sector. In 2005 DOE published the *Roadmap to Secure Control Systems in the Energy Sector*. This has provided a vision and guidance to the industry and driven the development of many tools and techniques that help secure control systems. A updated revision is due out soon.

The Department of Homeland Security (DHS) has the Control Systems Security Program whose mission is to coordinate efforts among federal, state, local nad tribal governments to reduce risks associated with critical infrastructure.

NERC produced the Critical Infrastructure Protection standards which are the first standards addressing cyber security for the power grid with mandatory compliance. Many have seen these standards as inadequate but they provide a good starting point. The NERC CIPs, as they are known, are under revision and the next version is anticipated to be more detailed and thorough.

The Industrial Control Systems Joint Working Group (ICSJWG) is the reincarnation of the Process Control Systems Forum (PCSF), whose goal is to bring together all the different parties who have a stake in securing critical infrastructure from federal and state governments to utilities, vendor, and researchers.

There are also a number of groups and standards bodies working on updating communication protocols and standards or designing new ones to add security features to the electric power grid and other control systems. Some of these protocols and standards are Secure DNP, IEC 61850, ISA 99, ISA 100 and the Secure SCADA Communications Protocol (SSCP)

Finally the last strategy we suggest is that utilities break from their traditional mold and consider utilizing third party communication companies. Implementing smart grid technologies will require increased communication capacity. Traditionally utilities would design, build and maintain their own communications infrastructure. This is expensive both in capital expense as well as time and effort to maintain. In the past decade broadband communications have seen significant growth. Leased lines used to be the only way to have broadband like capacity. Today there is DSL, cable, 3G and 4G cellular, WiMax and metropolitan area Wifi that can provide the data rates necessary to handle the larger amounts of data needed to implement most smart grid technologies. The companies that run these networks have also learned valuable lessons on how to secure their networks and mitigate many of the problems that come from having a highly exposed network. Utilities should seriously consider outsourcing some of their communication need before deciding to do it on their own.

VI. Concluding Remarks

This is an exciting time to be involved in the electrical power industry. There are so many changes on the horizon it is difficult to tell what the future holds. One thing is for sure, there are serious cyber security concerns and problems that must be addressed. It is important that we look at the vulnerabilities we are introducing, and implement sufficient controls to reduce them to an acceptable level or risk. Decisions made now will affect the electrical power grid and industrial control systems for decades to come.

REFERENCES

[1] B. Krebs "Cyber Incident Blamed for Nuclear Power Plant Shutdown", *washingtonpost.com,* Jun. 2008 [Online]. Available:http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html, [Accessed: Jan. 27, 2010]

[2] "Duke Energy Accidentally Shuts Down A/C At 18,000 Homes.", wlwt.com, Jul. 28, 2009. [Online]. Available: http://www.wlwt.com/money/20200998/detail.html. [Accessed: Jan. 27, 2010].

[3] United States Office of Management and Budget: "OMB Memorandum M-08-05 Implementation of Trusted Internet Connections". [Online]. Available: http://www.whitehouse.gov/omb/memoranda/fy2008/m08-05.pdf [Accessed: Jan. 27, 2010].

[4] Gartner Group. "Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks". Gartner.com [Online]. Available: http://www.gartner.com/it/page.jsp?id=565125. [Accessed: Jan. 27, 2010].

[5] J. Vijayan "Heartland data breach could be bigger than TJX's" computerworld.com Jan. 2009 [Online]. Available: http://www.computerworld.com/s/article/9126379/Heartland_data_breach_could_be_bigger_than_TJX_s, [Accessed: Jan. 27, 2010].

[6] RBS WorldPay. "RBS WorldPay announces compromise of data security and outlines steps to mitigate risk." Rbslynk.com, Dec. 23, 2008 [Online]. Available: http://www.rbslynk.com/RBS_WorldPay_Press_Release_Dec_23.pdf. [Accessed Jan. 27, 2010]

[7] AMI-SEC, "AMI System Security Requirements" ucaiug.org, [Online]. Available: http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/1.%20System%20Security%20Requirements/AMI%20System%20Security%20Requirements%20-%20v1_01%20-%20Final.doc. [Accessed, Jan. 27, 2010]

[8] AMI-SEC, "AMI Security Profile v1.0" ucaiug.org, [Online]. Available: http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAP-SG)/AMI%20Security%20Profile%20-%20v1_0.pdf. [Accessed: Jan. 27, 2010]

Sam Clements received his undergraduate degree in Business Information Systems from Utah State University in 2003. He received his M.Sc. in Information Security Policy and Management in 2008 from Carnegie Mellon University.

From 2003 to 2007 he worked as a computer technician for various not-for-profit organizations.

Sam joined the Secure Cyber Systems group in 2008 at Pacific Northwest National Laboratory where he has focused on security for critical infrastructure protection including the smart grid, standards development, and wireless technologies for industrial control systems.

Harold Kirkham received the BSc degree in 1966, and the MSc degree in 1967, both from the University of Aston, Birmingham, U.K. He received the PhD degree from Drexel University, Philadelphia, PA, in 1973.

From 1963 to 1968 he was a trainee with Midlands Electricity Board, a distribution utility. From 1968 until the end of 1969 he was at the HVdc research laboratory of the Edison Electric Institute, in Philadelphia, PA, studying ac/dc system operations.

After his PhD he joined American Electric Power, first in New York and then at their UHV station in Indiana. He was at the Jet Propulsion Laboratory (JPL), Pasadena, CA, from1979 to 2009, in a variety of positions, ending as a Principal in the Office of Mission Assurance. For several years he managed a DOE-funded project on communications and control in the electric power system, concerned largely with the integration of distributed generation, and distribution automation. Later he was manager of the NEPTUNE power project, aimed at delivering power via MV cable to science locations on the Juan de Fuca tectonic plate.

In 2009 he moved to the Pacific Northwest National Laboratory, in Richland WA, to work on smart grid related research.

His research interests include both power and measurements. Dr. Kirkham is a Fellow of the IEEE and Past-Chair of the IEEE Power and Energy Society's Instrumentation and Measurements Committee.