Edith Cowan University
Research Online

Australian Digital Forensics Conference | Security Research Institute Conferences

2009

The not so smart, smart grid: Potential security risks associated with the deployment of smart grid technologies

Craig Valli
Edith Cowan University

Originally published in the Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2009.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/adf/63

The not so smart, smart grid – potential security risks associated with the deployment of smart grid technologies

Craig Valli
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University

Abstract

The electricity grid has been up until now a relatively stable artifice of modern industrialized nations. The power grids are the most widespread wired networks in the world. They are heavily regulated and standardized to protect the integrity, stability and reliability of supply. The grids have been essentially closed systems, this is now rapidly changing with the introduction of the network enabled smart meter. These meters are "web" accessible, connect and interact directly with electrical appliances in domiciles and businesses. This move now brings a range of extreme risks and complexities into these stable networks. This paper explores the security issues and potential problems associated with current moves to provide these smart meters to existing grid connections.

Keywords

SCADA, smart grid, critical infrastructure, electricity grid, security, smart meter

INTRODUCTION

The electricity is grid is the most widespread wired network in most industrialized nations. Currently there are moves in some western countries to place "smart" meters into these networks so that companies who managed these networks and customers can have greater control over their power supply.

These smart meters atypically will allow for each appliance in the home to be monitored and controlled via a network connection. Some will allow connection via web interface to control these devices. Electricity networks are highly regulated and standardized due to the nature of the material that is transmitted across these systems. Simple errors or omissions could result in catastrophic failure of equipment or loss of life. Devices and appliances that are attached to these networks are built to specified standards, tolerances, limits, overrides and fail-safe's. This level of control and engineering is not only in an effort to protect end users of the facility from electrocution but largely to protect the integrity of the network, the supply of the service and the support infrastructure. The modern electricity network to ensure stability is essentially a closed system as a result of engineering controls and legislation.

Previously an esoteric error detected in a controller on these closed networks unless it presented an immediate operational threat did not require amelioration i.e. it was not a threat. This lack of necessitated amelioration is because the control system was not entropic, did not have uncontrolled connections and was performing within acceptable limits and consequently there was no likelihood of the operating conditions changing. In an Internet connected reality this is no longer true.

SCADA networks already have had sustained cyber attacks with devastating consequences. However, these documented attacks would atypically have had to have crossed certain security barriers presented by the infrastructure provider in the form of firewalls, IDS and other network countermeasures. In a smart metered reality the meters are the infrastructure and these provide routes to and from the operational cores of the infrastructure provider. The number of network egress and ingress points almost expands exponentially with the provision of smart meters in the household that also connect via network to network enabled appliances. This increased complexity and diversity of devices represents significant challenges for the provision of basic security let advanced security such IDS and IPS capability on these particular smart enabled networks.

Many of these smart meter systems now add several layers of complexity beyond the simple addition of these network enabled devices. The smart meters potentially add an series of compounding extreme risks into networks that up until now have largely been unaffected by network effects such as DDoS and flash worms. We have an Internet that largely is now a hostile and entropic place in which to operate. Viruses, worms and malicious codes are part of the landscape and are often spread via network means to infect more victims. Power infrastructure owners are now saying would it not be a great idea to connect these relatively closed stable systems which contain all your electrical powered devices to the Internet via a network of smart meters. The premise for this is so we can monitor your electricity and deliver you better

service, the road to many disasters are often paved with good intentions, this current logic of deploying current smart meters is potentially no exception.

Many of these products are accessible over the Internet and use the "web" to allow access to your power and appliances. Or to put it another way lets use one of the most insecure technologies to allow anyone to access your power supply mechanism and appliances. Hyper Text Transfer Protocol (http) or the "web" protocol is inherently insecure, there is ample evidence of this. Its main purpose is the transmittal of data streams generated on web servers that interpret HTML for display on system consoles. These transmissions are typically performed in plain text which allows for the interception of any passwords, PINs or other protections that are used in the interactions with the power meter. The protocol being plaintext also allows for the passive detection of other elements of control via capture of network data streams. This interception will allow simply replay attacks where a sequence of packets are captured and then simply replayed across the network to get the same effect on the appliances.

The provision of open network connections enables a range of technological attacks that are simply not possible unless you have network access to the device. The following sections will examine what problems or issues the provision of connection to these electricity grids could present.

TECHNICAL ATTACKS AGAINST SMART METER TECHNOLOGY

A DDoS (Distributed Denial of Service) literally denies service to a wide range of victims using many compromised hosts to achieve this. The worst that normally happened in these situations was that you could not access a website or a service until ameliorations were put in place. Now with the potential for these distributed smart meters to be accessed it means that there is a whole new meaning to the words denial of service. To overload a circuit or an electrical device such as a motor a quick way to achieve this is simply power cycle the device within an interval quick enough so that any residual power has not dissipated, the result is circuitry overload or worse fusion of the moving parts of the device. So a denial of service here could mean a malcode or exploit of the smart meters firmware that makes the power cycle say once every 5 seconds. Now distribute this across all meters of the same type in suburb and you can see the potential for catastrophic failure of a power supply network.

Defective network stacks embedded in devices and operating systems have been a long known and utilized avenue for exploit and vulnerability. Many of these exploits have in the past enabled RPC or complete administration level exploitation of the vulnerable systems as well as DoS. In some cases the attacks have been enabled by the sending of a specifically crafted network packet that enables the particular exploit or vulnerability a good example of this was MS03-26.

Many of these smart meters are designed as low power devices and as such do not have significant computational power. This low compute power is a manifest problem for the provision of strong encryption for the exchange of sensitive or operational data. Strong compute is typically needed to enable the factoring of large prime numbers or the performance of complex algorithmic machinations to create sufficiently robust cryptography. By the use of rainbow tables and advanced fuzzing techniques it maybe possible to break the cryptography provided by these systems and thereby access passwords and other critical information. If the cryptography is however, generated on a key basis due to the large size of the networks and devices it is highly unlikely that a power grid provider would be frequently updating keys for the devices. It is well known that conventional networks have these distribution problems already and with the provisioning of devices onto the proportionately larger electricity grid and associated multitudes of smart appliances the problem would only become more acute.

Firmwares of many of these devices do not have the capacity to perform CRC or standard integrity checks on the firmware upgrade being sent to the actual device. This type of weakness is again another avenue for malfeasance and possible destruction of these devices within a networked context. A malcode or exploit within the existing firmware could allow for the bypassing of necessary authentications and protections for the upload of a firmware. The malfeasant firmware could have an embedded command and control malcode that allows remote procedure calls or execution of arbitrary code on the device. A more sinister possibility is the download of a null or corrupted firmware that which when a forced reboot of the device is undertaken will cause the unit to malfunction or worse become inoperable or "bricked". This exploit has been proven in concept on one of the processor platforms used in smart meters (Goodspeed 2007).

Some more subtle malfeasant firmware could be the installation of firmware that falsely reports a lower rate of energy supply from the company or the converse of this for someone supplying power back into the grid. If there are limited mechanisms for checking a firmware likewise monitoring of changes in these firmware's could also be significantly impaired. It is interesting to note that many of the successful prosecutions against hackers in the 1980s were not able to be prosecuted for compromise of the actual computer but the theft of electricity as a result of the actual hacking activity.

The above mentioned attacks are only targeted at the meter. The appliances connected to these meters in some instances will be connected via a valid IP number. Many of the larger white good appliances in homes already have the ability to receive firmware updates across the wire. This ability brings all of the issues presented in the previous power meter appliances with it. What is different is that these appliances often transform electricity into some other energy such as heat, cooling, mechanical motion or mechanism control. This enables a wider range of possible attack vectors down to the appliance level. Imagine the consequences of setting a freezer or refrigeration to an elevated temperature for an extended period of time. The attack on a dishwasher or washing machine to constantly dump water. These all seem at a minor or singular level inconsequential but with the aggregated or multiplied effect through a DDoS approach significant problems could easily manifest across a range of utilities and services. The technology to enable this is almost standardised code by attackers through the creation and exploitation of botnets to drive this style of attack.

Side channel exploits for the particular chipset that many of these smart meters use is now known. While still hard to effect it has been at least proven to occur (Goodspeed 2008). In this paper the author presents a methods for a side-channel timing attack against the MSP430 serial bootstrap loader (BSL). As the author states the BSL attack works even after a protective JTAG fuse has blown as there is a need to write updates to the BSL which can be done without exposing the internal memory to an attacker. Each firmware image contains a password which if it can be overwritten will allow control of the device and also will prevent the BSL from erasing all of the memory. The converse is also true if the password is changed from the known good to a bad then after X number of retries the BSL will erase the memory. In addition in this paper Goodspeed presents some early indication that voltage glitching attacks may work which are further cause for concern.

Many of the current range of smart enabled meters and devices rely on Zigbee of 802.15.4 wireless based protocol. Designers seem to constantly forget that any wireless signal can be brute forced into a denial of service by the use of a stronger signal base in the same frequency band it is basic physics. Putting the obvious aside, there are already tools available for purchase that can scan for Zigbee devices, and further to that people are already customizing the software that supports these devices(Wright 2009). The Zigbee security specification is explained in slides by (Reddy) with one of the following caveats "Keys can be factory-installed or setup over the air or using out-of-band mechanisms (eavesdropping should be prevented when this is setup)". Furthermore in an article by (Ocenasek 2009) the author identifies security issues with Zigbee and breaks them into three topical areas management problems, insufficient integrity protection and key management problems. Many of these problems are inherent or similar to ones in WiFi or 802.11b it will not take many experienced attackers to rapidly assimilate knowledge and produce tools capable of breaking many of these identified issues.

The ability to covertly hide information of internet enabled crime quite literally in the fridge is a possibility even now. Some refrigerators come with their own storage capacity to store recipes and other items of interest on them, it is not much of an extension to use these storages for malfeasant purposes. With the use of distributed network RAID technology literally no memory space is too small to harness in this way. To anthropmorphise for a moment the sales pitch could be "..and would you like a hacker in the freezer compartment to go with that as well." Now given the range of appliances that could be connected into the house and the dormant storage in these devices again the problem could become extremely complex to mitigate against and also investigate forensically.

CRIMINAL ATTACKS USING TECHNOLOGY

A malfeasant staff member at an infrastructure supplier could see that after a 3-4 day period that a particular household has a had a significant drop in consumption. This would indicate that the property maybe vacant and hence able to robbed with little risk of detection. Also with some control of the properties power supply the ability to flatten any backup batteries that maybe in an alarm system is also a distinct possibility.

As outlined in Valli 2002 an attack could also be perpetrated at the individual by simply powering off appliances. This attack could be timed once again with the knowledge that an individual is going on holiday. The ability to putrefy the contents of the freezer and refrigerator, flood the house by overflowing the washing machine and ruining floor coverings, these would not be financially insignificant events to overcome.

DDoS has been used successfully by organized crime to extort money from online businesses such as casinos. The use of DDoS to now deny resources to an enterprise elevates this criminal activity to whole new level of economic based extortion.

REMEDY?

Remedy is not simple but it is also not impossible to achieve a reasonable level of assurance and safety within the network even by adding these particular devices. It is without question that many of these devices will have undergone significant engineering testing for compliance with the electrical standards and requirements for attachment of the device to a power network. This practice of course is a perfectly acceptable paradigm within which to operate when the only people who would be interacting with these devices are licensed or certified professionals however, with smart meters this is not the case.

By placing these devices on a network the operational testing requirements should expand. This expansion now requires extensive testing for deployment of the device in a situation where it may come under sustained network attack due to its connectedness.

Full functional testing of firmware should be undertaken and again run through rigorous testing for malcode or exploit potential. This testing would include tests such an examination of authorization, authentications etc used to protect the system. It is apparent that at least some of the chipsets currently in use in devices now are themselves vulnerable to exploit or attack. So this has major impacts on how these chips should be used and the circuits and boards into which they are designed. Many of the manufacturers of these meters may have to significantly retool or redesign these meters to overcome inherent problems with the chosen chip architectures.

CONCLUSION

The move to this type of smart enabled scenario is not one that should be taken lightly. Currently there is some hyperbole in some of the discourse on both sides of the argument around the deployment of these devices. One of the problems is that unlike many of the issues faced by the current Internet at present it does not largely touch or control large parts of the infrastructures or facilities we need to sustain our modern society. What parts we have that are currently touching have been proven to be significant cause for concern in particular SCADA networks where there have been numerous attacks.

The blind introduction of smart enabled technologies into the largest network in the world with known problems is simply dilettante in the extreme. If I analogise for a moment if smart meters were drugs and these drugs had a known potential flaw that killed people effectively in large numbers when they took the drug and came into direct contact with salt water, would we allow its production let alone sale? Yet currently smart meters/grid (drugs) have known potential flaw that can kill large numbers of them when they become connected to a network (water) that contains malware (salt).

Finally, we have measurable and significant impacts on organisations now when they become infected with malcodes from an IT perspective. Some of these impacts have run to hundreds of millions of dollars in global terms. The process for recovery of this at worst is reformat the drive and reconstruct the infected computers from backups. So what will the total cost be when the power goes off and how easy is it going to be to restore the entire affected electricity grid.

REFERENCES

Goodspeed, T. (2007). "Memory-Constrained Code Injection." 2009, from http://travisgoodspeed.blogspot.com/2007/09/memory-constrained-code-injection.html.

Goodspeed, T. (2008). Practical Attacks against the MSP430 BSL. Twenty-Fifth Chaos Communications Congress. Berlin, Germany.

Ocenasek, P. (2009). Towards Security Issues in ZigBee Architecture Human Interface and the Management of Information. Designing Information Environments, Springer Berlin / Heidelberg: 587-593.

Reddy, J. S. (2009) "ZigBee Security." Retrieved 19th August, 2009, from http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=9436.

Valli, C. (2002). The New Homeland Defence. The European Conference On Information Warfare & Security. B. Hutchinson. Brunel University, Uxbridge, MCIL,Reading**:** 143-148.

Wright, J. (2009). "Locating ZigBee Devices." 2009, from http://www.willhackforsushi.com/?p=227.

COPYRIGHT

Craig Valli ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.