EAVESDROPPING ON THE SMART GRID

Craig Valli, Andrew Woodward, Clinton Carpene, Peter Hannay, Murray Brand,
Reino Karvinen and Christopher Holme
School of Computer and Security Science, Edith Cowan University
SRI - Security Research Institute, Edith Cowan University
Perth, Western Australia
c.valli@ecu.edu.au, a.woodward@ecu.edu.au, c.carpene@ecu.edu.au, p.hannay@ecu.edu.au,
m.brand@ecu.edu.au, r.karvinen@ecu.edu.au, c.holme@ecu.edu.au

Abstract
An in-situ deployment of smart grid technology, from meters through to access points and wider grid connectivity, was examined. The aim of the research was to determine what vulnerabilities were inherent in this deployment, and what other consideration issues may have led to further vulnerability in the system. It was determined that there were numerous vulnerabilities embedded in both hardware and software and that configuration issues further compounded these vulnerabilities. The cyber threat against critical infrastructure has been public knowledge for several years, and with increasing awareness, attention and resource being devoted to protecting critical in the structure, it is concerning that a technology with the potential to create additional attack vectors is apparently insecure.

Keywords
Smart Grid, eavesdropping, wireless, Zigbee, 915Mhz

INTRODUCTION

The smart grid initiative is not only an Australian phenomenon, nations around the world are considering and implementing variants of the smart grid technology for their own power networks (NIST, 2010). It is crucial that these technologies are thoroughly tested as they typically have an installed life of 30-50 years. This research aimed to analyse the vulnerabilities that were perceived to exist in the smart grid system which was made available to study. By having the opportunity to perform an in-depth vulnerability assessment against the components used within the advanced metering infrastructure (AMI), and the supporting infrastructure, conclusive evidence can be gathered to discern the effective security of the smart grid.

This research was initially targeted only at smart grid meters however due to some agreed changes as a result of the conduct of the initial research, the assessment was conducted across the meters, the relay devices and the access point to the extent permissible with given resources and funding. We were fortunate in that an energy provider has supplied us with equipment, where no other power owner or vendor in Australia was willing to sell or loan us equipment. It should also be noted that the vendor for the energy provider was extremely protectionist and obstructionist in releasing hardware or materials to us.

The configuration of the solution provided by vendor to the energy provider was as supplied (Figure 1):

- Smart grid meter - 2.4Ghz Zigbee and 915 Mhz Relay Uplink
- Pole Relay Unit - Vendor 915 Mhz Device
- Access Point - 915 Mhz Bridge and Raven-X 3G Router

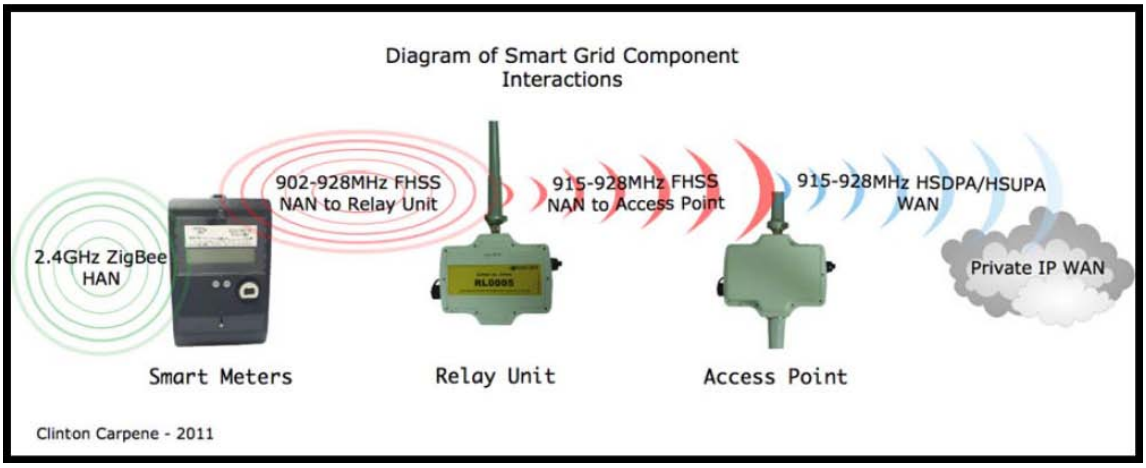

Figure 1: An overview of the smart grid, displaying the interactions between each smart grid component

It should be noted that this research was entirely "black box" testing without access to manuals or technical information.

REVIEW OF RELEVANT LITERATURE

Silver Springs Networks' whitepaper "Smart Grid Security; Myths vs. Reality" (2011) attempts to vanquish several myths about the state of the smart grid's security. The document highlights many of the common fears amongst the academics and professionals, and attempts to subjugate them. The myths that are detailed in the document include:

Nobody is paying attention to security: it is claimed that a survey revealed all vendors are incorporating security into the infrastructure (Silver Spring Networks, 2011). Whilst it is mentioned that stakeholders are actively working with standards bodies such as the NIST, Silver Springs Networks never explicitly states that they are incorporating the NIST guidelines into their model.

The smart grid makes it easy for hackers to cause widespread blackouts: the paper mentions that the devices can include authorisation check functions prior to processing a termination command, and that monitoring facilities can be implemented to actively prevent widespread disconnections.

Using IP in the data communications network means the smart grid is as vulnerable as the Internet: like Cisco, Silver Springs Networks maintains that the IP network in usage will remain largely a private network, mostly separated from the Internet (Cisco Systems Inc., 2009; Silver Spring Networks, 2011). Whilst robust security measures can reduce the risk of an attack occurring, it must be noted that any connection to a public network, such as the Internet, provides a potential vantage point for an attack.

Wireless networks lack security and are easy to hack: according to the paper, the concept of authenticating users and encrypting data is fundamental to wireless security. Interestingly, the paper notes that "the level of security implemented is generally driven by the needs of the applications that are accessing the network wirelessly", and that the act of reading a meter wirelessly would require less rigorous security than upgrading a meter (Silver Spring Networks, 2011). The reader can infer from this explanation that whilst encryption and security may exist, varying levels of security may be applicable across the smart grid model, which could expose attack vectors.

Cracking one meter provides access to the entire smart grid because everything is interconnected: the paper describes that devices in the network can be designed to maintain a unique identity, and only communicate with other devices once the identity has been verified. Once again, it is not mentioned whether the devices have been designed with these rouge-detection mechanisms in place, or whether these considerations might be added in future iterations.

Proprietary security schemes are more secure than IP- based security technologies: like Cisco (2009) and Frost & Sullivan (2006), Silver Springs Networks commends the usage of Open protocols and standards in the network model, as opposed to proprietary protocols. The paper discusses that proprietary protocols often do not have the development support and resources of an open or peer-reviewed standard (Silver Spring Networks, 2011).

Whilst compelling, the whitepaper fails to provide any technical specifications as evidence to support the claim that each concern is a myth; rather each topic is overviewed in a relatively superficial fashion.

Cisco Systems Inc. (Cisco) provide their perspective on the possible challenges of securing a large-scale smart grid network. The whitepaper "Securing the Smart Grid" (Cisco Systems Inc., 2009) identifies 5 areas that Cisco describes as potential challenges to the smart grid project:

1 Scale: Any smart grid network needs to be built with scalability as a requisite. A nationwide electrical network will have an extremely large number of devices operating simultaneously, and therefore needs to be designed with this as a consideration. Cisco recommends the usage of network segmentation to allow for the network to scale, whilst maintaining controllability over small areas.

2 Legacy devices: Devices in the smart grid network are expected to have a much longer lifecycle than the typical three to five years for standard networking equipment (Cisco Systems Inc., 2009). As a consequence, the smart grid needs to be designed to support legacy devices and accommodate older technology in the future as well as embrace new directions or technologies.

3 Field locations: field locations are the devices in the smart grid network such as smart meters, access points, cabling, substations, etc. These locations have to be designed and constructed with physical security as a consideration, as well as information security.

4 A culture of "security through obscurity": Cisco proposes that current electrical grid security makes the assumption that if a vulnerability isn't well known, it will not be exploited, and believes that vulnerabilities will not remain hidden indefinitely (Cisco Systems Inc., 2009). Cisco compels vendors to choose peer reviewed standards and protocols as opposed to developing proprietary standards and protocols, as historically these have proven to offer greater security. This is a sentiment that is echoed in "Open Standards, Open Possibilities; Addressing Reliability Through Next Generation Utility Information and Control Systems" (Frost & Sullivan, 2006).

5 Evolving standards and regulations: Cisco expresses concerns that no ratified standards exist that address AMI, however recognises the efforts of NIST in developing guidelines and standards to address the requirements of the smart grid, and urges vendors to consult such guidelines. Early adopters are claimed to be the most vulnerable aspects of the smart grid, with insufficient independent and field-testing of equipment likely to impact on the security of the technology (Cisco Systems Inc., 2009).

PROOF OF CONCEPT ATTACKS

The Not-So-Smart Meters, by Steve Gold, exposes theoretical attack avenues by referencing attacks that have occurred on other network-enabled devices. Citing outstanding insecurities with similar network enabled devices, Gold infers that the smart grid will inherit these vulnerabilities. The article provides examples of vulnerabilities present in wireless communications, HTTPS, and smart card technology, however often fails to provide relevant substantiation for these claims. As an example, Gold, whilst attempting to convey the inherent risks of the 802.11 wireless network (Wi-Fi) protocols, provides a case study pertaining to an attack on the original Apple iPhone as evidence. The attack, however, failed to highlight any security vulnerabilities in the wireless protocols themselves. The attack described required the user to browse to a compromised web page in order to complete the exploit. Upon doing so, their phone could be remotely controlled via a Wi-Fi connection. This attack, however, was not androgynous, and could just have easily taken place over a wired communications medium, as it required human intervention similar to a phishing scam.

Goodspeed (2008) has published documentation on proven attacks against the microcontrollers being used in some iteration of smart meters. While the attacks require the executer to have some background in electronics, they can be performed by anybody with physical access to the devices.

In 2009, Mike Davis showcased a presentation titled SmartGrid Device Security: Adventures in a New Medium, which discussed a number of vulnerabilities to which current smart meters were susceptible. Davis (2009) concluded the presentation by providing a proof of concept attack that used a single, physically compromised smart meter, to infect, via radio, neighbouring smart meters (Davis, 2009). Davis and fellow IOActive researchers created a simulation that predicted their self-replicating smart meter worm could spread to over 20,000 smart meters in less than 24 hours (Davis, 2009). Davis (2009) also discusses the remote disconnection feature of the smart grid. He expresses concerns that, whilst it may be economically in the best interests of utility providers, the feature will need extra attention to ensure it does not become exploitable. Davis believes that the possibility of disconnecting multiple electrical services remotely will surely become a target for attackers (Davis, 2009).

Unfortunately, Davis (2009) does not identify which devices would be susceptible to attack, or the means by which the devices were compromised. In order to protect the technology and stakeholders involved, Davis

(2009) refuses to divulge which vendors or models are vulnerable to the executed attack, making it merely anecdotal from the perspective of this research. Furthermore, as a penetration test, the attack does not adequately quantify the insecurities of the smart grid.

RELATED GUIDELINES AND ATTACK METHODOLOGIES

Although no ratified standard exists currently, the National Institute of Standards and Technology (NIST), provides a draft guideline for the construction and specifications of a potential smart grid. In a 4 volume document series Guidelines for Smart Grid Cyber Security (GSGCS), NIST details the requirements of a secure, functional iteration of the smart grid. The documents provide a list of device specifications, including appropriate device protocols and standards that will provide a reference point for vulnerability testing in this project.

Given the speculation surrounding the possible insecurities associated with the smart grid, it is not surprising that documents exist that seek to expose these insecurities. ASAP has created a report titled AMI Attack Methodology (2009) that introduces a comprehensive attack framework against the smart grid. This attack methodology seeks to highlight the dangers of implementing the smart grid by formulating attacks against the devices that facilitate the technology; smart meters. Whilst exploiting vulnerabilities discovered in the smart grid is external to the scope of this research, some of the possible attack vectors listed in the AMI Attack Methodology, along with elements of the attack framework itself, have been adopted to assist with this investigation. Similarly A Classification Framework for Smart Grid Meters Vulnerability Assessment (Valli, et al., n.d.) provides an unofficial list of various potential vulnerabilities, which assisted in this research's generation of flaws.

The unpublished, confidential, document Smart Grid Security Assessment (Smart Grid Security Assessment, n.d.) provides an overview of the initial investigation that this project will continue. The document indicates that, along with this investigation, concurrent vulnerability assessments of other aspects of the smart grid will take place, as well as exploitative attacks against various aspects of the technology. Elements of this research, therefore, may assist in developing and extending the parent investigation, or its sibling projects, and may provide the foundation for future research on the topic.

EAVESDROPPING ATTACKS AGAINST THE SMART METER SPECIFIC TESTING AT 915 MH LABORATORY

The NAN packets were captured by placing the smart meter, and access point within a faraday cage. This placement inside the cage was performed in an attempt to isolate interference from various other ~900MHz radio networks that are present. Initially, we used a Rohde & Schwarz "Spectrum analyser" to determine what the frequency of the broadcast was it was emanating from smart meter. We then tested with everything off, open cage, testing to establish baseline (902mhz) -43.7 dbm (closest background signal). Next we turned everything off, sealed cage, testing to establish baseline -70 dbm which is background noise. We then tested with cage closed, AP & meter on via UPS, signal of -15.99dbm (920mhz).

We then proceeded to gather packet dumps using the SmartRF04 ICE using TI SmartRF Packet Sniffer. This was passive capture with no injection or other interference with the wireless stream or the communications. We conducted 2 packet capture sessions with a gross data capture exceeding 500MB of traffic (these are supplied with results).

We performed some basic packet analysis on the captured traffic. The analysis revealed that many of the packets were in fact encrypted. We used the ZenaSniffer utility to attempt to recover the keys and were unsuccessful. We have not at this stage performed any extended cryptanalysis due to time and resource constraints. We are however in the next few months undertaking attacks on this captured data using GPU-based technology and potentially rainbow table attacks.

EAVESDROPPING ATTACKS AGAINST THE SMART METER SPECIFIC TESTING AT 2.4GHZ – LABORATORY

The smart meter's Home Area Network (HAN) side network interface uses the 2.4GHz ZigBee wireless communications protocol to communicate with smart grid enabled devices (such as IHDs) and provide additional functionality (i.e. automatic usage polling, remote powering-off of devices such as air conditioners, lights, etc.). Using the KillerBee framework (with the accompanying USB dongle) and the Zena Sniffer, HAN bound ZigBee packets were captured from the smart meter.

We used a Rohde & Schwarz "Spectrum analyser" again to determine what the frequency of the broadcast was. We then tested the sealed cage for attenuation in 2.4Ghz and it peaked at -60dBm likely caused by leakages. The

closed cage with AP & Meter on peaked at -46.5 dBm. We then started sniffing Zigbee with SmartRF04 ICE using TI SmartRF Packet Sniffer.

It is worth noting that even with injection attacks, no keys were recoverable using ZigBee cracking tools. A significant limitation on the experiment, however, was the caveat that no devices were actually associated to the 2.4GHz ZigBee module of the smart meter. This is due to the fact that the authors were unable to obtain a test device (such as an IHD) for use within the experiment.

EAVESDROPPING ATTACKS AGAINST THE SMART METER SPECIFIC TESTING AT 915MHZ – LIVE IN THE FIELD AT A ENERGY PROVIDER DEPLOYED UNIT IN THE POWER GRID

This step involved the researchers in attending on site where these devices are currently physically deployed. Having performed the testing in the laboratory we were cognisant of frequency usage and equipment needed to execute.

We successfully gathered packet dumps from live systems on the 915 MHz networks. We accomplished this with the SmartRF04 ICE using TI SmartRF Packet Sniffer that was used within the laboratory experiments. The researchers captured over 4 hours of packet data from the field. This represents some 200MB of packet captures.

EAVESDROPPING ATTACKS AGAINST THE SMART METER TESTING AT 2.4GHZ – FIELD

The objectives of this particular test were to determine if encryption was used in the system, and if there was encryption present is it possible to determine master key, network key, and link key that the Smart Meter uses to provide this encryption. The data transmitted over a ZigBee network can be easily collected via the air interface, and presents an significant opportunity for interception, modification and fabrication of packets transmitted. Encryption can be employed by the ZigBee protocol and used in networks to mitigate threats from sniffing but only against interception of the plaintext. The plaintext should be able to be derived from the crypted packets once encryption schemes have been identified.

The killerbee framework provides a variety of utilities for ZigBee network discovery, collection of Zigbee traffic via sniffing, conducting of replay attacks and encryption attacks. The Smart Meter uses ZigBee on the Industrial, Scientific and Medical (ISM) band to communicate with home automation and display devices such as the In Home Display (IHD) device. Encryption is used by the system, and the network key was not revealed by the use of the tools at a superficial level i.e performing sniffing of the connections. It would appear at this stage that the implementation does not provide or initiate connection in plain text, this is good. However, this is not to say that further analysis, using other tools or manual methods may reveal the key for this setup nor that other configurations may use plaintext connections. When the key is determined, further attacks related to modification and fabrication will be performed to assist a vulnerability analysis.

TOOLS UTILISED FOR TESTING

- Dell Latitude 2110 Laptop
- Linux Backtrack 4r2 Live USB
- KillerBee 1.0 Framework as downloaded from the Internet
- 2 x Atmel RZUSB Sticks with KillerBee Firmware installed on them
- Python Modules python-gtk2, python-cairo, python-usb, python-crypto

ATTACK METHODOLOGY USING KILLERBEE FRAMEWORK

As mentioned the attacks used the KillerBee Framework, for technical details of what each particular command does please consult the KillerBee documentation.

1. Configure laptop with software tools.
2. Insert 2 x Atmel RZUSB Sticks
3. List the device Ids of RZUSB Sticks zbid
4. Record device Id's (DEVID1 and DEVID2)

5. Discover and enumerate ZigBee networks zbstumbler -i DEVID1
6. Record CHANNEL and PANID
7. 7. Run zbdump on one of the RZUSB zbdump -i DEVID1 -f CHANNEL -w FILENAME.CAP
8. Run zbassocflood on the other RZUSB zbassocflood -i DEVID2 -p PANID -c CHANNEL
9. Allow to run for 1 or 2 minutes
10. Stop the zbdump program and see if the network key is in the packet capture zbdsniff FILENAME.CAP

The methodology was first applied in the lab with only the smart meter. All steps were applied, however the network key was not retrieved. It was considered that a device may have to have been previously associated with the smart meter for the association flood to work. The test was repeated at a residential location, where a IHD was associated and clearly working with the smart meter. However, in this case, retrieval of the network key failed as well. The IHD was brand new, and had only just arrived at the residential location. The entire association process was captured, but the network key was not extracted from the packet capture. Further analysis may reveal the key(s), and it is considered that this initial association may be a good instance to retrieve the key(s).

Personal communications with the energy provider revealed that the IHD must indeed be associated with a Smart meter before it will communicate with it. Future research will attempt to capture and analyse the association sequence to determine whether it can be repeated or used to associate an unauthorised device.

DISCUSSION AND OBSERVATIONS

The wireless sniffer was used to collect the association traffic of the smart meter and the In Home Display (IHD) unit. The Expert Info screen showed that the network (NWK) traffic is encrypted. The IHD displayed the following sequence during this association: Scanning , Authenticating, Wireless base up, Completed, Searching for services and Synchronising.

The KillerBee utility zbdsniff did not reveal the network key during this transaction, nor did it locate the key resulting from using the killerbee utility zbassocflood. It is clear from the initial evidence gathered that the payload of the ZigBee implementation as presented at the moment is encrypted.

The high level use of the KillerBee framework has not revealed the network key deployed in this instance. However, further static analysis of the resulting packet captures may reveal the key. Further analysis of data collected for this test needs to be performed. If the key is determined, further attacks employing modification and fabrication may be performed to further identify potential vulnerabilities with system as deployed.

CONCLUSION

The research conducted for this project demonstrated conclusively that the technology as it currently stands has not been implemented according to network security best practices. This conclusion is based on the numerous vulnerabilities in both hardware and software and configurations that were discovered through the process of examining the equipment using a verifiable methodology. Whilst this technology potentially has many benefits from both sustainability and environmental vectors, the numerous security vulnerabilities inherent in smart grid question whether the technology is currently mature enough to be deployed in production environments.

Future research in this area would be both technical and non-technical. Technical research would look at other implementations and products, although given the difficulties in undertaking this current project, feasibility of such research is questionable. Non-technical research would attempt to determine reasons as to why the technology is being developed and implemented with security as an add-on and not fundamental to the product itself.

Given the increasing global awareness of the cyber threats against critical infrastructure, it is concerning that a technology which potentially provides a large attack surface for every owner of a smart meter to exploit is being developed and sold in such an insecure fashion. Whilst regulation in these areas has not been shown to be particularly effective in the past, that should not preclude action. If there is no significant improvement in the level of security offered by vendors of these products, the government may need to make policy decisions related to roll out of these systems need to ensure that appropriate security standards are part of the implementation for smart grid systems.

REFERENCES

ASAP. (2009) Advanced Metering Infrastructure Attack Methodology: ASAP,.

Cisco Systems Inc. (2009) Securing the Smart Grid. San Jose.

Davis, M. (2009) SmartGrid Device Security: Adventures in a new medium. Black Hat USA 2009. Web Conference. IOActive.

Frost & Sullivan (2006) Open Standards, Open Possibilities; Addressing Reliability Through Next Generation Utility Information and Control Systems. Palo Alto.

Gold, S. (2009) Not-so-smart meters? *Network Security, 2009*(6), 9.

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

NIST. (2010) Guidelines for Smart Grid Cyber Security *Vol. 2, Privacy and the Smart Grid*: The Smart Grid Interoperability Panel – Cyber Security Working Group.

Silver Spring Networks (2011) Smart Grid Security; Myths vs. Reality. Redwood City.

Valli, C. (2009) The not so smart, smart grid: Potential security risks associated with the deployment of smart grid technologies. *Proceedings of The 7th Australian Digital Forensics Conference*, 19-23, Perth, Western Australia.

Valli, C., Woodward, A., & Hannay, P. (n.d.). A Classification Framework For Smart Grid Meters Vulnerability Assessment. Perth: Edith Cowan University.

Wright, J. (2009) KillerBee: Practical ZigBee Exploitation Framework or "Wireless Hacking and the Kinetic World" [Presentation]: Willhackforsushi.com.