Smart Meter Technology

Proof of concept smart meter attacks on IPL

Daniel Kemp, Joseph Johnson, Kenneth Gouge, Thomas Howey, Jonathan Ervin

Group 2

CIT 460 Feng li

***Abstract*—Smart meter technology, how an attack can occur via its vulnerabilities.**

***Keywords*—Smart Grid, encryption, attack methodology, Silver Springs(*key words*)**

I. What is a Smart Meter/Grid

Smart meters are attached to a house and replace the old analog meters with wireless meters. The meters have been touted as a way to monitor usage in real time, without a meter reader. The meters have been controversial because of the wireless component, which is susceptible to attack like any other wireless device.

The frequency of operation for smart meters is typically in the 902 MHz and 2.4 GHz bands. The power output is typically 1 watt in the 902 MHz band and much less in the 2.4 GHz band. The intended range of a transmitter in a smart meter is typically very localized. The smart meter only communicates when it is commanded to do so, typically several times a day; transmitters operates under FCC rules.

Typically smart meters send bursts of data, averaging about 6ms long, and sent in intervals of minutes or hours. The daily broadcast frequency ranges from 5% to as low as 0.01% and broadcast at long intervals to a local node, some broadcast at short intervals to be picked up by meter reading vehicles. Smart meters can also communicate over WiFi, Blueooth, or ZigBee (IEEEE 802.15.4).

II. Vulnerabilities

Smart grids are susceptible to the same attacks as any other wireless device. Some of the major threats are system level threats which attempt to take down all or part of a smart grid area by denying operators access. The next is a radio subversion attack which attempts to take over one or more radios or the RF communications modules.

The vulnerability of most concern by the utility companies is the theft of service attack, which is meant to deprive the utility company of its revenue. Network barge in by strangers who attempt to join the RF and disrupt the signal. The denial of service attack which attempts to disrupt the utility to most or all customers in a given range. The result would make the entire network unusable. The last vulnerability would be cloning, which is when one person attempts to clone another signal to either deprive them of service or to deprive the utility company of its revenue by reporting a zero usage to the utility company.

III. Maintaining the Integrity of the Specifications

Digital Reconnaissance Based On Smart Meter Power Readings

The steps for an attack include:

A. *First Step - Isolating target for attack*

The first step will involve finding a suitable location for said attack. A location with a relatively visible smart meter with low physical security for ease of access. Must be able to access locations without arousing suspicion

B. *Second Step - Gathering data to develop attack*

The ability to analyze a smart meter used for home would be most beneficial. This process will take the longest in terms of understanding smart meter trends over a length of time and data gathering. The keys to this step are to identify the Smart Meter broadcast signal. The likelihood of multiple smart meters being within close proximity is very great, this means zeroing in on a specific smart meter without cross talk causing inaccurate signal reading and collection. The next step would be to record RF signals to understand data output (ping frequency, incoming VS outgoing, quantitative and qualitative analysis of data outgoing signals). After that the signal would have to be ddemodulated into usable data. After ddetermining physical security of localized reconnaissance device placement (i.e., meter inspections schedules). The goal is to get usable RF data to turn into digital data without arousing suspicion.

C. Third Step - Analyzing data

After the data has been demodulated, deciphering will likely involve encrypted transmissions. If the data is encrypted, the next task would be to determine what encrypting is being used and how it can be broken. High level encryption may be able to be bypassed by redundant use of encryption keys throughout all meters. Proprietary encryption may be weak enough for brute force attack. Once data is decrypted, using data to build a picture of power consumption throughout a 24 hour, weekly, or monthly trend in order to establish trends.

D. Fourth Step - Developing remote recon gear

The gear used must be able to record specific RF signals. Waterproofing will be necessary as the device will most likely be exposed to the elements. The device must be able to be placed inconspicuously and must not interfere with the function of the smart meter. The device must be easily accessed in order to route data. This can be done by allowing device to access local Wi-Fi networks for remote access of RF data packets for demodulation. Finally the device must also have access to a power source for 24/7 readings.

E. Fifth Step - Attack

First the recon device must be placed. Second, start recording the RF signals. The next step would be to ddemodulate the signals into digital data. Finally decrypt the digital data, and use the data to follow power trends (i.e. when inhabitants are home or not). Establishing these trends can be used maliciously for those interested in robbery, stalking, or can be used for staking out potential criminals.

IV. Attack 2 & 3: Intercepting and Augmenting Incoming/Outgoing Data Packets (MITM)

The principle behind this attack is to create a barrier between the smart meter and the local node so we can control the flow of data between them. This is a twofold attack because we can focus on either manipulating incoming messages or outgoing messages for malicious means. The steps will be very similar, with the main differences being at the end of the attack steps.

A. First Step - Isolating target for attack

The first step will involve finding a suitable location for the attack. A location with a relatively visible smart meter with low physical security for ease of access. The unit must be able to access locations without arousing suspicion.

B. Second Step - Gathering data to develop attack

The ability to analyze a smart meter used for home would be most beneficial. This process will take the longest in terms of understanding smart meter trends over a length of time and data gathering. The keys to this step are to first identify the smart meter broadcast signal. Due to the likelihood of multiple smart meters within close proximity, this means zeroing in on a specific smart meter with cross talk causing inaccurate signal reading and collection. The same process will need to be repeated for identifying incoming transmissions from local nodes. The next step would be to record the RF signals to understand data output (ping frequency, incoming VS outgoing, quantitative and qualitative analysis of data outgoing signals) as well as data input. After recording, the next step is to demodulate the RF signals into usable data. Finally the determining the physical security of localized reconnaissance device placement (i.e., meter inspections schedules). The goal is to get usable RF data to turn into digital data without arousing suspicion. Incoming and outgoing transmissions need to be parsed and separated.

C. Third Step - Analyzing data

After data has been demodulated, deciphering likely encrypted involve transmissions. If the data is encrypted, the next task would be to determine and how it can be broken. High level encryption may be able to be bypassed by redundant use of encryption keys throughout all meters. Proprietary encryption may be weak enough for brute force attack. Once data is decrypted, using data to build a picture of power consumption throughout a 24 hour, weekly, or monthly trend in order to establish trends.

D. Fourth Step - Creating Transmission Barrier

A Faraday cage-like apparatus will need to be constructed, for the purpose of blocking incoming and outgoing transmissions. The cage will need to be inconspicuous to the common eye, and be able to keep RF signals broadcast inside the cage separated from signals broadcast outside the cage. The Smart Meter (SM) is enclosed in a Faraday Cage a device inside is able to broadcast and receive RF signals at a specific signal that the Smart Meter broadcasts and listens to. The device is connected to an outer device, connecting two similar devices between the cages via a wired connection. The outer device receives incoming messages from the local node and can broadcast messages from the smart meter to the local node. By doing this, we now control the flow of data between the local node and the smart meter

E. Fifth Step - Developing Capture/Relay Device

The localized deployment will involve three main parts, first the Faraday Cage, which is a small enclosure with copper screening that will be used to block incoming and outgoing RF signals. The enclosure should be large enough to full surround the smart meter and have room for a relay device inside. The cage will need to be tested to ensure that it does act as a impassible barrier for RF signals while simultaneously remaining inconspicuous. Next the external relay must be able to capture and record incoming RF signals from the local node. Upon capture, the signal will be demodulated and encrypted. The signal can also be passed along to internal relay in order to preserve communication between the smart meter and the local node. The external relay must also be able to broadcast an RF signal to the local node with enough dB. The device will need to be weather resistant and can be constructed using Arduino or Raspberry Pi chipsets. The external relay must also be remotely accessible to the attacker in order to analyze data. Finally, the internal relay will be very similar to the external, except that it will only be able to listen or broadcast to the smart meter within the Faraday cage and must backhaul all collected data through a wired connection to the external relay. The internal relay will also need to broadcast data, it can broadcast at much lower dB due to the proximity to the smart meter.

F. Sixth Step – Attack

The attack involves controlling the flow of data between the local node and smart meter. Pings sent from the local node requesting usage statistics can be captured before reaching the smart meter and can be responded with augmented replies reporting lower usage statistics in order to artificially lower electrical bills. Another use would be to capture incoming software update information for the smart meter to understand the internal architecture of the smart meters software for the purpose of discovering further exploits. These software updates can later be used to pass on faulty updates that allow for more exploits.

V. Data Encryption

The energy industry often uses “home-grown” encryption algorithms instead of proven industry standards [6]. This inconsistency in security increases the risk of wireless smart meters becoming vulnerable to hacking. In many large scale deployments, it is not uncommon for all wireless smart meters to have the same set of encryption keys [9].

Weak security standards increase the risk that a malicious attacker could perform traffic analysis on the overheard cipher text. So although many may find the encryption sufficient enough if a hacker or nation-state was able break the encryption they would then have the encryption keys to every smart meter on that particular network.

The common weaknesses of smart meter encryption include the use of RC4, which has similar weaknesses as when used in WEP. It is also generally used with weak authentication which only increases the overall risk. Smart meter encryption also has a weak digest function, which is often linear and vulnerable to man in the middle attacks [5]. The broadcast security is also usually undefined, has very little security, and uses the same mechanism that are used to push out firmware updates [4].

Lastly key usage is one of the most glaring weaknesses as the same master key is often used. Should authentication become compromised all session key become known to the attacker [7].

The industry continues to try to come up with its own standards, which differ from proven, tested standards. The Common Smart Grid Protocol (OSGP) is used in Europe and North America and comprises mainly of these custom algorithms for authenticated encryption [6]. Most are based on an EN 14908 algorithm that has a 48-bit key, extremely weak digest, and is very susceptible to forgery attacks. Below is a diagram of the OSGP protocol scheme.

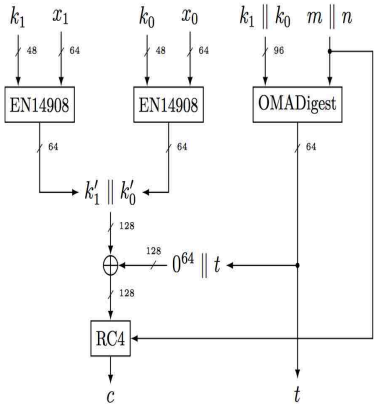

Fig. 1. The OSGP AE scheme. Notation: $x_0 = \{81,3F,52,9A,7B,E3,89,BA\}$, $x_1 = \{72,B0,91,8D,44,05,AA,57\}$, $k = k_1 \| k_0$: Open Media Access Key (OMAK), m : message, n : sequence number, t : authentication tag, $k' = k'_1 \| k'_0$: Base Encryption Key (BEK), c : ciphertext.

VI. Silver Springs Smart Meter Security

There are more than forty-six million smart meters in the United States alone. Worldwide shipments of smart meters are expected to top one hundred million per year in the next few years. Utility companies will ping these meters often throughout the day which generates huge amounts of data. It’s analyzing all this data that is slow and Silver Spring Networks is actually developing cloud-based software to help with this issue.

Silver Spring Networks knows that security plays a huge role in the stability of the smart grid. This being the case they implement stringent authentication and authorization measures into their products and networks. In doing this, they help to ensure end-to-end protection of communications and devices themselves. If a hacker gains access to a single endpoint, it does not open up access to the entire network. Each device actually operates with separate credentials in their networks. They also implement tamper detection and resistant technologies so that a hacker shouldn’t be able to physically access a device either. The firmware that they load on the endpoints requires the digital signature to be verified before any upgrades take place. Lastly, transmissions between the endpoints and applications are encrypted and they ensure data integrity by applying hash functions.

The Silver Spring Networks interpreter endpoint is the plug-n-play replacement for the older analog-style meters. It lacks any external wires or antennas and is permanently sealed within the impact resistant glass enclosure. The interpreter operates within the 902MHz to 928MHz unlicensed bandwidth. The default data interval is six hours and each transmission within this time frame includes more than just the current state. It actually transmits the last twenty-four hours of fifteen-minute interval data. Meaning that there will be redundancy with the data transmissions considering it transmits every six hours. The actual network interface card that lies within. Silver Spring Networks actual call it the NIC 5. They claim that it delivers self-forming and self-healing network capabilities to devices requiring high throughput. It can transmit up to 2.4Mbps with just a ten millisecond latency. It uses public-key based authentication methods and also implements AES encryption techniques. This typically operates on the 902-928MHz spectrum but with the latest technologies having frequency hopping spread spectrum, this allows the device to jump to the 2.4GHz band. The devices are actually set to use internet protocol version six instead of the typical version four that we find mostly being used today.

Lastly, intercepting these wireless transmission signals is clearly possible. There are even devices out there today that developers can form into just having that purpose. Software defined radios like the HackRF One can actually have an antenna plugged into it which can then be used to not only transmit, but also receive transmissions on a wide spectrum. By wide I mean as drastic as 1MHz all the way to 6GHz. This clearly encompasses the broadcast spectrum of the smart meters. When this device receives signals, it digitizes them much like analog waves are digitized so the computer can interpret them.

VII. DEFENSE OF SMART GRIDS

As noted by [3], smart grid systems are being deployed in many countries. As a major component of these smart grids, the smart meter has been installed at consumer locations and power substations. As of 2013, there are over an estimated 300 million smart meters around the world. Because smart grids are widespread and use computers and networks to communicate, they are susceptible a variety of attacks including DDoS and false data injections as noted by [1].

Since multiple methods can be used against smart grids, there have to be multiple forms of defense as well. Defense techniques can range from cloud computing to embedded firewalls mentioned by [1], [2]. These techniques have their own rules and methods in protecting smart grids

A. Cloud Computing

Historically, energy companies have used one sources of energy, such as fossil fuels, to provide electricity. In today's market, electricity comes from multiple resources, including renewables. The complexity of managing large amounts of data from multiple sources is not part of the typical power company's business model. Compare this with cloud computing that was originally designed to obtain, store, and deliver data to and from multiple sources. It can be a viable solution power companies to manage large amounts of data from these multiple sources.

Cloud computing can be used to protect the smart grid against DDoS attacks. When paired with common DDoS defense techniques, such as honeypots, cloud computing can reduce the damage done by DDoS attacks smart grids. However, cloud computing was not designed with the intention of protecting critical infrastructure. Originally, it was designed for the storage and retrieval of data from multiple sources. That said, it can provide energy companies with a cheaper method of storing and retrieving the large amounts of data that smart grids produce, as noted by [1].

Cloud computing was not originally designed for industries, such as energy, where data consistency and availability is a major concern. Because power companies have to reduce the risks of outages, the risks and benefits of cloud computing need to be considered. As noted in Table 1, cloud computing has multiple attributes for power companies to consider. Each attribute has its own risks and benefits.

TABLE 1: Potential Risks and Benefits of Cloud Computing with Smart Grids[1]

CC Attribute	Potential Risk	Potential Benefit
Agility & redundancy	Lack of efficiency in ability to scale up and down to match demand. Costs associated with latency.	Ability to adapt to fluctuations and resource intensive tasks. Low storage costs due to economies of scale.
Device & location independence	Consistency of data: connectivity, latency and performance issues	Resilience. Low operation costs. Location & geographic independence.
Real-time response & elastic performance	Consistency of data; latency, performance, and data auditing issues; billing errors	Quick response to fluctuations in energy demand ensuring proper electricity distribution/delivery
Self-healing	Causes of errors / malfunctions may remain unknown. Self-repair may lead to system in-efficiencies or data inaccuracy	Would greatly enhance the robustness and endurance of SG systems.
Virtualization & automation services	Data security; Hypervisor and VM vulnerabilities and potential misconfigurations	Faster response time, disaster recovery, and deployment of security implementations

The size and complexity of the smart grid places it at greater risk for DDoS attacks. It contains a large amount of components, such as smart meters, data servers, control systems, and more, that can be viewed as a potential target for attackers. [1] found that a DDoS attack on even a small portion of the smart grid can place the entire network at risk

The use of various defense techniques can decrease the risk to smart grids. One technique is attack prevention though a system of honeypots with different configurations can be used to detect multiple methods of attack. Another technique is real-time attack detection to discover anomalies in traffic patterns and determine if these anomalies are legitimate or malicious in nature. A third technique, attack source identification, is used to discover the geographical location of the DDoS attack. A fourth technique, attack reaction, is used to diminish the effects of the DDoS attack, as noted by [1]. These techniques are described below in Table 2.

TABLE 2: Defense Techniques and Beneficial Cloud Computing Attributes [1]

Type of Defense	Type of Attack	Defense Technique
Attack Prevention	SYN Flood (TCP), Smurf Attack, PDF GET, HTTP GET, HTTP POST	Honeypots
Attack Detection	SYN Flood, Smurf Attack	DoS-Attack-Specific Detection
	PDF GET, HTTP GET, HTTP POST	Anomaly-Based Detection
Attack Source Identification	SYN Flood, Smurf Attack, PDF GET, HTTP GET, HTTP POST	Hash-Based IP Traceback
Attack Reaction	SYN Flood, Smurf Attack, PDF GET, HTTP GET, HTTP POST	HIP Filtering
		Load Balancing
		Selective Pushback
		Source-End Reaction
		Analysis of Traffic Data
		Fault Tolerance
		Resource Pricing

B. Embedded Firewall

Many of the smart grid's devices, such as smart meters, are located in the field without protection from the energy company's firewall. [2] found that these devices provide a critical component of the smart grid but also act as easy targets for attackers.

One way to reduce the chances of attacks is to limit the number devices that can successfully communicate with the smart grid network. This can be accomplished by using an embedded firewall on the smart meters themselves. The firewall can enforce policies that define allowable communication by limiting the IP addresses that can connect to the device. The best way is to configure a whitelist of trusted hosts and block all other connections. Because each packet must pass through this firewall, many attacks can be stopped before even connecting to the device [2].

A small embedded firewall can be used to protect smart grid devices, such as smart meters, from a wide variety of cyber-attacks, as stated by [2].

B. Smart Meter Resiliency

[3] performed experiments on two commonly found smart meters, the Power Quality Meter SHARK 200 Meter and the Power Nexus 1500 Meter, to study their response to DoS attacks. They wanted to measure their response time and their abilities to communicate with the smart grid server while under attack.

Their experiment found that, when meters were subjected to DOS attacks, responses from Ping requests by the meter were extremely slow and, in some cases, had no response at all. They found that the meters would disconnect from the smart grid network when the ping traffic increased. The two meters tested by [3] were found to have no security countermeasures against common DoS attacks.

They went on to use ARP cache poisoning to conduct the DoS attacks. They conducted two different test attacks on the smart meter. The first test involved sending fake ARP requests to inject fake IP/MAC addresses into the ARP cache. Their results shows that the ARP caches were corrupted and prevented from communicating with the server. Their second experiment also involved ARP cache poisoning with the intent to reroute traffic from the smart meter to the attacker before forwarding to its intended destination, creating a MITM attack. Their results that the tested smart meters were vulnerable to these types of attacks.

Based on the results of [3]'s experiment, they concluded that smart meters are easy targets for malicious users. Their design is based on a cost effective model with ease-of-use for end-users. They found that smart meters lack basic security functions, including packet filtering and IDPS systems. They came up with four suggestions for increasing the security of smart meters: "…(1) smart meters should allow for packet filtering to filter network packets… (2) ARP cache of smart meter should be made static…(3) network traffic with high-speed rate…should be denied from reaching the kernel…smart meters with IDS should be able to use basic common attack signatures and download new attack signatures. (4) Smart meters should be equipped with encryption capabilities…"

Fig. 1. The OSGP AE Model

References

[1] A. Calfino, E. Dincelli, S. Goel, "Using Features of Cloud Computing to Defend Smart Grids against DDoS Attacks" in *10th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA '15),* Albany, NY, 2015, pp. 44-50 [Online].Available: http://www.albany.edu/iasymposium/proceedings/2015/ASIA15_proceedings.pdf#page=54.

[2] A. Grau, "Smart Grid Security: Blocking Cyber-attacks with an Embedded Firewall," in *Embedded Systems Engineering*, 2012. Accessed: Mar. 5, 2016. [Online]. Available:http://eecatalog.com/smart-energy/2012/10/11/smart-grid-security-blocking-cyber-attacks-with-an-embedded-firewall/

[3] K. Shuaib, Z. Trabelsi, M. Abed-Hafez, A. Gaouda and M. Alahmad, "Resiliency of Smart Power Meters to Common Security Attacks", in *The 6th International Conference on Ambient Systems, Networks and Technologies*, London, 2016, pp. 145-152.

[4] Buchanan, B. (2015, 5 15). Lifehacker Australia. Retrieved from When Smart Grids Meet Dumb Crypto: http://www.lifehacker.com.au/2015/05/when-smart-grids-meet-dumb-crypto/

[5] Burton, G. (2015, 5 11). 'Dumb crypto in smart grids': Smart meter encryption standard fundamentally flawed, claim researchers. Retrieved from Computing: http://www.computing.co.uk/ctg/news/2407891/dumb-crypto-in-smart-grids-smart-meter-encryption-standard-fundamentally-flawed-claim-researchers

[6] Donovan, F. (2015, 5 12). 'Home-brewed' encryption scheme opens millions of smart meters to hacking, warn researchers. Retrieved from Fierce IT Security: http://www.fierceitsecurity.com/story/home-brewed-encryption-scheme-opens-millions-smart-meters-hacking-warn-rese/2015-05-12

[7] Gridco.de. (2015, 5 15). Insecure Open Smart Grid Protocol. Retrieved from Gridco.de: http://www.gridco.de/en/2015/05/15/Insecure-Open-Smart-Grid-Protocol/

[8] Jackson Higgins, K. (2014, 10 1). Smart Meter Hack Shuts Off the Lights. Retrieved from Information Week: http://www.darkreading.com/perimeter/smart-meter-hack-shuts-off-the-lights/d/d-id/1316242

[9] Smart Grid Awareness. (2014, 12 30). Cyber Hackers Can Now "Harm Human Life" Through Smart Meters. Retrieved from Smart Grid Awareness : https://smartgridawareness.org/2014/12/30/hackers-can-now-harm-human-life/