Energy Theft in the Advanced Metering Infrastructure

Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel

Systems and Internet Infrastructure Security Laboratory (SIIS)
Pennsylvania State University, University Park, PA
{smclaugh,podkuiko,mcdaniel}@cse.psu.edu

Abstract. Global energy generation and delivery systems are transitioning to a new computerized "smart grid". One of the principle components of the smart grid is an advanced metering infrastructure (AMI). AMI replaces the analog meters with computerized systems that report usage over digital communication interfaces, e.g., phone lines. However, with this infrastructure comes new risk. In this paper, we consider adversary means of defrauding the electrical grid by manipulating AMI systems. We document the methods adversaries will use to attempt to manipulate energy usage data, and validate the viability of these attacks by performing penetration testing on commodity devices. Through these activities, we demonstrate that not only is theft still possible in AMI systems, but that current AMI devices introduce a myriad of new vectors for achieving it.

Key words: AMI, Smart meter, Penetration testing, Attack tree

1 Introduction

The smart grid being globally deployed today will forever change the way energy is used. This new infrastructure offers more efficient, lower cost, and more environmentally sound energy management than its antiquated predecessor. The advanced metering infrastructure (AMI) is a crucial piece of this new smart grid infrastructure. AMI provides a computer-based sensor system that extends from the homes and buildings that use power to the utilities that manage it. From a technology standpoint, AMI provides the necessary communication and control functions needed to implement critical energy management services such as fine grained pricing schemes, automatic meter reading, demand response, and power quality management. The smart grid has been widely deployed in Europe and Asia, with other parts of the world seeing more gradual but accelerating adoption.

The smart grid, AMI in particular, introduces new security challenges [12]. By necessity, AMI will consist of billions of low-cost commodity devices being placed in physically insecure locations. The equipment is under the control of the often disinterested, unsophisticated, or sometimes malicious users. Even in simple and/or low value services, such an arrangement would be extraordinarily difficult to secure.

This paper considers one of the most important threats against the new smart grid—energy theft. Referred more generally as *theft of service*, energy theft occurs when a customer manipulates the energy usage statistics provided to the utility. To understand this threat, we develop an attack tree that systematically articulates the ways by which an adversary may attempt to manipulate usage data as it is collected, stored, or transmitted. We further preliminarily show the feasibility of different classes of attacks by penetrating currently deployed smart-meters, and attempt to identify root causes of existing vulnerabilities.

Theft of service for electric meters is nothing new. Annual losses in the United States alone are estimated at $6 billion [9]. Traditional theft in pre-AMI systems required the mechanical manipulation of analog meters. Conversely, in AMI, usage data may be tampered with after recording or in transmission to utilities. Moreover, software based attacks often require less expertise to execute and thus are likely to be more widespread. Precedence has shown and as we argue throughout, that these types of software attacks are quickly monetized by criminal groups that sell the hardware and software needed for theft of service. Examples include the descrambler boxes that lead to over $4 billion in cable theft per year [4] and sites that sell SIM unlock codes for cellular phones [11]. For these reasons, it is imperative for the AMI vendors, energy producers and distributors, governments, and customers to understand the potential scope and source of energy theft. This paper attempts to inform this need.

The rest of this paper is organized as follows. Section 2 explains the capabilities of AMI systems. Section 3 presents a threat model that shows how these capabilities may be leveraged for energy theft. A description of the tested equipment is given in section 4, and in section 5, we show the results of our security evaluation of a smart metering system, and explain their significance to energy theft. Finally, we discuss future directions for our study in section 6 and conclude in section 7.

2 AMI Background

The advanced metering infrastructure (AMI) is the sensor network of the smart grid. It provides the information about energy usage (demand) to utilities, consumers and the grid itself. This enables all parties to make better decisions about reducing costs and strain on the grid during times of peak demand. The necessary information about demand is coupled along with the energy distribution itself. This information is measured and aggregated by *smart meters*, digital electric meters that contain commodity CPUs, storage, and communication interfaces. These two components–smart meters and communication networks–form the infrastructure needed to provide AMI services. Broadly speaking, smart meters perform four basic functions with respect to power management; *a*) the monitoring and recording of demand, *b*) the logging of power relevant *events*, e.g., outages, *c*) the delivery of usage and logging information to the upstream utilities, and *d*) delivering and receiving of control messages, e.g., controlling smart appliances, remote disconnect, etc.

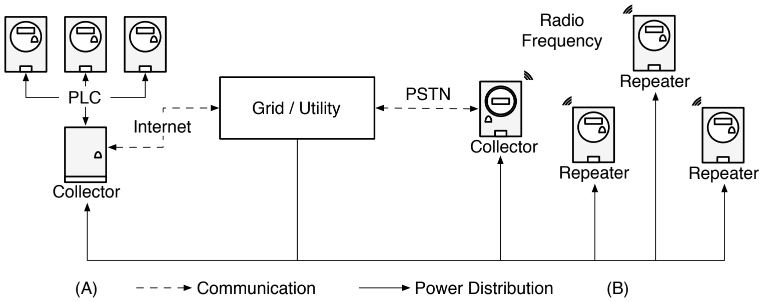

Fig. 1. Two example AMI network configurations. In (A) a power line communication (PLC) local network connects meters and a dedicated collector node. The collector communicates with the utility over the Internet. In (B) meters act as radio frequency repeaters to a collector node which itself functions as a meter. A backhaul link to the public switched telephone network connects the collector and utility.

AMI enables a number of services related to demand measurement and billing. Meters supporting automatic meter reading (AMR) can report demand to utilities automatically via communication networks. The two predominate network configurations are shown in Figure 1.[1] A local network of *repeater* meters is established between meters for the purpose of aggregating usage information to a *collector* meter. A backhaul network is then used to to transport the aggregate data from the collector to the utility. Local networks typically rely on either wireless mesh topology or power line communications (PLC). The backhaul link often uses a public network such as the Internet or the public switched telephone network (PSTN). Along with AMR for meter reading, AMI provides additional capabilities for dynamic pricing schemes such as time-of-use.

Time-of-use (TOU) [7] pricing refers to a pricing scheme in which power costs more during hours of peak demand. TOU schemes divide a day into several partitions called tariffs, typically peak and off-peak. Ideally, customers will be motivated to reduce costs by moving some energy-intensive tasks to off-peak hours, reducing the peak strain on the grid.

Beyond new interactions with customers and the grid, smart meters promise new anti-tamper measures. Previous meter tamper detection mechanisms were limited to locks and tamper-evident seals. While these measures are often sufficient for keeping honest people honest, they offer little to deter malicious tampering, and are often circumventable. Beyond physical tamper detection mechanisms, smart meters may be configured to log events concerning command history and conditions in the meters environment. This includes the detection of events indicative of physical tampering. One such mechanism, outage notifi-

[1] Other configurations are available but less widely deployed, such as those which use cellular networks. Apart from the access media, the operation is identical to that described in this paper. Thus the majority of attacks described herein apply to AMI systems built on these other access networks as well.

cation, records periods during which voltage has dropped or been removed from the meter's sensors. Reverse energy flow, which is indicative that the meter has been inverted in its socket, may also be detected through meter firmware. If customers participate in distributed generation, reverse energy flow is no longer indicative of meter inversion. In this case, additional tamper detections are necessary to differentiate between meter tampering and power actually received by the grid. Having covered the relevant AMI functionality, we go on to describe the threat model for energy theft.

3 Energy Theft

In this section, we use the security modeling technique of attack trees [14] to understand strategies for energy theft in AMI. Attack trees recursively break down an adversary goal into subgoals until a number of possible attack strategies are reached. The root node specifies the single goal of all attacks in the tree, in our case, this goal is demand forgery. Below the root node is a set of sub goal nodes that describe different approaches towards the root goal. The leaf nodes, which have no descendants, represent the specific attacks that must take place for the goal to be achieved. Paths to the root goal are augmented with the logical operators AND and OR which determine whether one or all of the children in a given internal node need be completed in order to achieve the goal.

The attack tree model is well suited here for a number of reasons. Individual attack trees can be composed to achieve specific goals. For example, an adversary that attempts to cause rolling blackouts [8, 10] may have a sub-goal of forging energy demand at distribution substation meters. Attack trees also provide a way to reason about a system's vulnerable points in a top-down manner. This is useful for identifying both the root causes of attacks as well as the "low-hanging fruit" that is likely to be exploited.

3.1 Attacker Model

Before describing the attack tree for energy theft, we define the types of attackers that are motivated to commit energy theft.

- **Customers:** Traditionally, customers have been the primary adversaries aiming to steal power. The means and motivation to tamper with analog meters is very much individual in nature. That is, customers are limited in their resources and technical abilities, but in the case of AMI, can distribute some of the labor in discovering vulnerabilities and designing attacks to members of organized crime.
- **Organized Crime:** The motivation in the case of organized crime is the monetization of energy theft. Because of the extended computing and network capabilities of AMI, the task of creating software and hardware tools to compromise smart meters can be offloaded from customers to professional hackers. Members of this group will leverage certain design aspects of AMI systems, such as the widespread use of the same password set over many meters, to greatly amplify the profit from cracking a single meter.

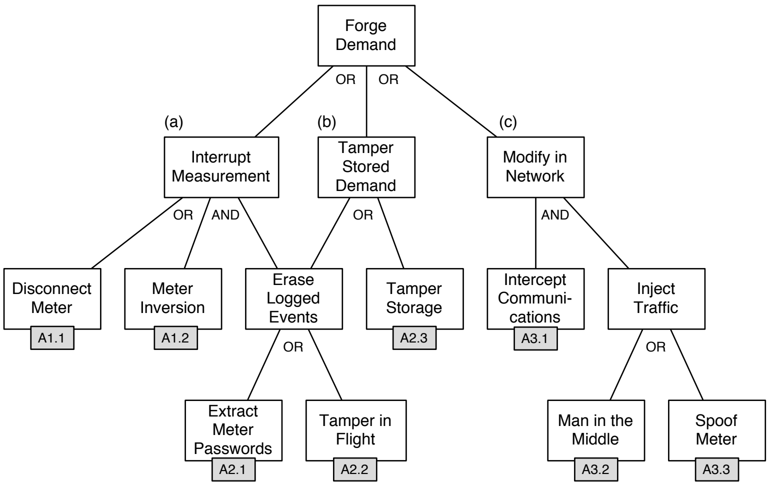

Fig. 2. An attack tree with leaves detailing the necessary attacks to commit energy theft. Theft can take place (*a*) before the meter makes a demand measurement, (*b*) before/while demand values are stored in the meter or (*c*) after measurements and logs have left the meter in transmission to the utility. The attacks leading to each of the three are labelled Ai.j for the jth attack that occurs at place (i).

- **Utility Insiders:** Utility insiders are implicitly trusted to be honest in the case of analog meters and the same model applies for AMI. It is preferable however that utility side systems enforce proper user and group management to provide properties such as separation of duties [5].
- **Nation States:** Adversaries with this level of expertise and resources have little motivation to commit theft as evaluated in this paper. They may however use discovered smart meter vulnerabilities for the denial of service or invasions of privacy.

3.2 Energy Theft Attack Tree

We present an attack tree for energy theft in Figure 2. As shown, the single requirement for energy theft is the manipulation of the demand data. There are three ways to tamper with demand data; *a*) while it is recorded (via electromechanical tampering), *b*) while it is at rest in the meter, and *c*) as it is in flight across the network. We discuss each of these ways in detail.

The first class of attacks, which aim to prevent the meter from accurately measuring demand, are the only class that previously existed for analog meters. The other two classes are exclusive to AMR and AMI. AMI does increase the difficulty of executing this class of attacks by logging sensor data that determines when power is cut to the meter, or if reverse energy flow occurs. Thus, to execute attacks A1.1 or A1.2 undetected, it is necessary to also erase the logged events that indicate outage or reverse energy flow before they are retrieved by the utility.

As these events are stored in the meter along with demand measurements, their removal falls under the second class of attacks on data stored in meters.

Smart meters store a large range of data. This includes tariffs for TOU pricing, logs of both physical events and executed commands, recorded net demand and their own programs among others. Because effectively all aspects of a smart meter's behavior are controlled by the contents of its storage, the ability to tamper with that storage (A2.3) gives a customer complete control over its operation. An attack involving overwriting the meter's firmware, while powerful, is a significant reverse engineering task. Thus, this type of attack is limited to members of organized crime aimed at selling meter hack kits.

For the purposes of energy theft, only a few select items in the meter's storage are of interest, namely, audit logs and the recorded total demand. Both of these values can be accessed through established administrative interfaces which require passwords. Their modification is usually limited to reset, clear in the case of an audit log and zero in the case of demand record. Consider the case in which a malicious customer has somehow obtained a meter password. The customer's electric bill may be reduced by X% by executing a demand reset operation after the first X% of the billing cycle. Because the administrative interface to the meter requires login credentials, a prerequisite to these attacks is extracting the necessary passwords from the meter (A2.1). In section 5 we explain one method that can be used for extracting the meter passwords and explain the far reaching consequences once they are no longer secret.

The third class of attacks involves injecting forged values into communication between meters and utilities. These attacks contribute to the above described monetization of energy theft in that they may be executed by any node between the meter and utility, which is not necessarily at the site where the meter is located. Furthermore, because of the two tier architecture of AMI, (local networks and backhaul links), executing a network based attack at a collector node makes possible the modification of all demand recorded for the set of repeaters. In some commercially available AMI systems, this can be in upwards of 1,000 nodes depending on the particular metering system.

The goal for subtree (3) requires two distinct types of actions, interposition of the attacker on the backhaul network (A3.1) and injection or modification of traffic between the meter and utility (A3.2,A3.3). Interposition is needed for any passive attack, including capturing the protocol between meters and utilities for reverse engineering. Network interposition can most easily be achieved close to one of the endpoints. For customers, tapping a line between the meter and the first backhaul link is the easiest. Utility insiders would have ready access to the links and routers leading up to the computers performing remote meter reads. The second task, traffic injection, requires the attacker to replace demand information from meters with forged data. In the event that an AMI system correctly uses cryptography for message integrity and authentication, this attack will require that the keys used for encryption first be extracted from meter storage (A2.3).

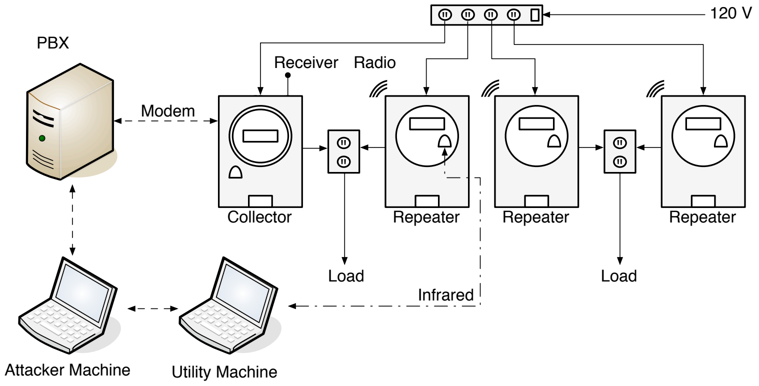

Fig. 3. Experimental testbed.

If there is a flaw in the authentication or integrity protocols between the meter and utility, then a meter spoofing attack (A3.3) is sufficient for sending forged demand data and event logs. In this attack, a common device, such as a laptop computer, is used to receive calls from the utility in place of the meter and provides crafted values for specific fields. If the authentication mechanism is flawed but an encrypted channel is established between the meter and utility, a "man in the middle attack" (MIM) will be required [6]. This involves a node on the backhaul link from the meter to the utility to impersonate one to the other while the secure session is established to obtain the key used for cryptographic message integrity.

4 System Under Study

In this section, we describe the environment and tools used for our preliminary smart meter security analysis. This analysis included reverse engineering and attacking meter communication protocols and details about the capabilities of the meters themselves. We describe the functionality and aspects of the implementation that are relevant to the results of the security analysis without respect to any specific vendor or equipment.[2]

The full experimental testbed is shown in Figure 3. It provides the full range of functionality needed to evaluate the security of the meters and communications within a typical AMI configuration. The local network, a wireless mesh operating in the 900 MHz band, is the only interface not yet evaluated in our study. The PSTN is used for the backhaul network to the utility. An Asterisk [13]

[2] We are currently working with the appropriate agencies to notify the vendors of our preliminary findings. Due to the potential impact on public safety, it has been suggested that we do not identify the specific vendor with the current text. It is our expectation that we will be able to release this information in the final proceedings version with more detail on the tested equipment and attacks presented below.

based private branch exchange (PBX) is used to simulate the telephone network for communication between the meter and utility. A “utility machine” runs the back-end software used by utilities for reading, programming and resetting meters. Both the utility machine and collector meter communicate over telephone using voice-band modems.

The testbed meters are form 2S single phase residential meters. Each meter is equipped with an infrared optical port that can be used for the same functions as the modem port, albeit without the same security measures. Both the modem and optical ports require passwords to read measurements and modify meter programs. The configuration has three repeater nodes in the local network and one collector connecting to the utility machine.

Auditing is used for outage notification and reverse energy flow detection as well as other more benign events. The audit logs may be retrieved via the optical port or telephone modem. Note that as some customers have contracts to sell generated power back to the grid, the reverse energy flow detection can be disabled. The intrusion detection feature in the collector node ensures that the meter is the only device off the hook when communicating with the utility. The meter automatically interrupts communication and hangs up when another phone is picked up.

Additional monitoring software was run on the utility machine to capture both the telephone modem and optical port protocols. The meter reading software running on the utility machine was disassembled in order to understand the use of cryptography in communications as well as the structures used to parse protocol messages. A separate “adversarial machine” is used for attacks on communication between the meters and utility machine.

5 AMI Security Analysis

The results of our security analysis show that the studied system contains design flaws that allow for energy theft using both pre- and post-AMI techniques. For each type of vulnerability, we describe the existing protections, how they may be circumvented and either describe a proof of concept attack as validation or explain how how validation could be achieved in future work.

Physical Tampering – A number of the identified attacks (A1.1, A1.2, A2.1, and A2.3) require some type of physical tampering of meters. Two types of tamper detections are provided by the studied meters, physical and firmware based. The physical tamper protections are the same as those for analog meters. Tamper evident seals are essentially the only means of detecting that the meter enclosure has been opened. Typically, two types of seals are used, one on the meter socket enclosure provided by the utility, and one on the meter’s outer cover. The utility seal is a non-standard serialized tag and is outside the scope of this study. The seal placed on the meter’s cover is a standard aluminum meter seal with a flag containing a stamped string between one and five characters. We were able to pick any stamp of our choice (including those used by vendors and utilities) from the tamper seal vendor without any special credentials. The

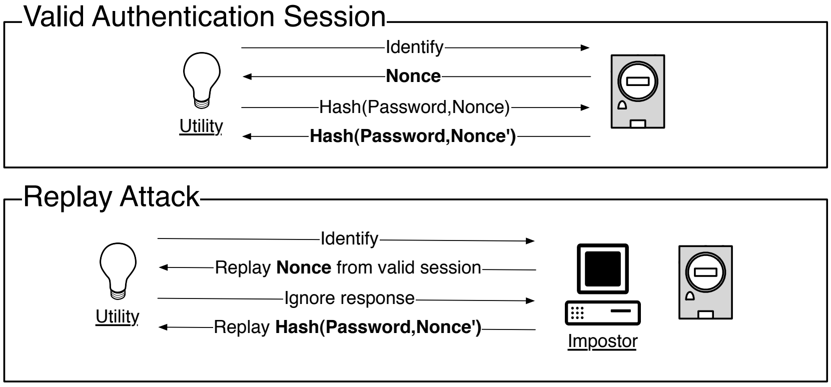

Fig. 4. The replay attack discovered in the studied system. Because the two messages in the mutual authentication round are dictated by the nonce, replaying a previously recorded nonce will allow the impostor to authenticate without knowing the password used to key the hash.

ability to replace the seal on the meter cover eliminates any evidence that the cover was removed.

Password Extraction – Attack (A2.3) requires that meter passwords be extracted. If the meter is physically tampered with, this may be achieved through optical port snooping. We used monitoring software on the utility machine to capture the optical port protocol used to communicate with the meter and found that passwords are transmitted in the clear. Once the meter is opened, placing a reader device on the optical port pins or near the optical lens is sufficient for capturing the password amidst the rest of the protocol. Furthermore, the password is always identifiable can be located according to the ANSI C12.18 standard [3].

Eavesdropping – The studied meters offer some protection against the interception of traffic (A3.1) over the telephone backhaul link. Whenever a meter detects that another device on the same line has gone off the hook, it will hang up. This works correctly in the case when a device such as a telephone or modem (technically any FXO [1]) picks up on the line. This feature does not work in the case of devices placed on the path between the meter and first link to the phone company. The PBX in our experimental testbed is one example of such a device (technically an FXS [1]). Using the open source software running on the PBX, we were able to monitor modem communication. In a full attack scenario, the monitored communication would later be demodulated from a waveform to the actual protocol.

Meter Spoofing – One risk of placing a physically insecure device on a network is the potential for a spoofing attack (A3.3), in which another adversarial device impersonates the legitimate one. The studied system uses the standard ANSI C12.21 protocol for mutual authentication of meters and utilities. In this pro-

Table 1. A summary of the vulnerabilities in the studied AMI system and the attacks they enable. The specific vulnerability in the studied system that enables each attack identified in section 3 is shown along with the design assumption behind that vulnerability. Assumptions are numbered for reference in this section.

Attack Number & Description	**Vulnerability**	**Design Assumption**
(A1.1, A1.2) Measurement interruption	Inadequate physical tamper protections	1. Physical limitations
(A2.1) Password extraction	Insecure optical communication	2. Near field security
(A2.3) Meter storage tampering	No Firmware Integrity Protections	3. Physical integrity of meter
(A3.1) Communication interception	Insufficient intrusion detection	4. Trusted backhaul nodes
(A2.2, A3.2, A3.3) Communication tampering	Failure to check for replay	5. Trusted endpoint node

tocol, the meter creates a cryptographic nonce which is sent to the utility. The utility software then computes a message authentication code (MAC) by hashing the password and nonce. The calculation is done using the ANSI X3.92-1981 data encryption algorithm [2]. The MAC is then sent to the meter which calculates its own MAC which is sent to the utility software. At this point, mutual authentication is complete. The flaw in the studied system is that the utility software does not verify the freshness of the nonce from the meter. Thus, an adversary that is able to eavesdrop on an authentication session can replay the nonce and authenticate itself as the meter. See figure 4

For a proof of concept meter spoofing attack, we used a laptop computer to impersonate a meter to the utility. Using the communication logs from eavesdropping on the backhaul link, we wrote a computer program to answer the utility's call and perform a demand and diagnostic read function. Using this program, we were able to insert chosen values for any field ready by the utility, including demand. Note that in the event that meters are modified to use encryption and mutual authentication, meter spoofing may still be achieved by extracting the cryptographic keys from the meter's storage (A2.3)

6 Understanding Vulnerabilities

Up to this point, we have modeled attacks leading to energy theft and shown vulnerabilities and proof of concept attacks in an AMI system. The goal now is to understand the design assumptions behind the vulnerabilities. The grouping of attacks by these assumptions is shown in Table 1. We explain the impact of each of these assumptions on attacks on AMI and show that they create three properties that increase the ease and monetization of energy theft. These are, amplification of efforts, division of labor, and an extended attack surface.

As is the case with analog metering, assumption 1. states that there are economical and practical limitations to how well a meter can be physically secured. This limitation ideally would be addressed by the advanced security features provided by AMI. This however is not the case as the existing firmware protections are not tied to the meter's physical enclosure. While possible electromechanical tampering is detected, the assumption is made that the meter internals, and thus the tamper detection mechanisms, are not accessed.

Assumption 2., which states that optical port communication with an untrusted device is secure, is incorrect. Given this, both the optical signal could have been sensed by special equipment or recorded inside a compromised meter. While special equipment may be needed to obtain a password from the optical port, the payoff is multiplied by the number of meters using that password.

Assumption 3. is another example of amplification of adversary effort. The potential for tampering with the meter's stored firmware has several consequences beyond the mere ability to steal power. First, modifications at the firmware level are hard to detect without off-line inspection of the firmware contents. Second, the customer using the tampered firmware for theft does only the small amount of work needed to upload the malicious image. The majority of effort is put forth once by a group with the goal of selling malicious meter firmware. This is indicative of both the ability of AMI to multiply the effort put into attacks and a distribution of labor between organized crime and customers. Finally, as tampered firmware may be a sign of remote exploitation, the customer has plausible deniability if tampering is detected.

Assumption 4. leads to the poor use of authentication and encryption for integrity as well as a circumventable intrusion detection mechanism in the studied system. This assumption is likely due to misunderstanding the security requirements of extending the attack surface into public networks.

Finally, the failure of mutual authentication of utilities and meters, by assumption 5., creates a vulnerability that is both widespread and easily exploitable. The ability to simply substitute another device for a meter encourages the creation and distribution of meter spoofing software which leaves no evidence of tampering at the meter itself. This is another example of AMI's extended attack surface.

7 Conclusion

We posit that the basic requirements of AMI are in conflict with security. While some poor engineering choices are sure to exacerbate some of these issues, there are fundamental reasons why a fully digitized metering system is inherently more dangerous that its analog predecessor. Several of these reasons include:

1. **Amplification of effort:** In many cases, compromising a single meter is sufficient for stealing power with many more. Attacks that capture a password once and use it many times or the penetration of a head end meter to modify all usage in an area are exemplary.

2. **Division of labor:** Customers may avoid a large degree of risk and effort by using pre-made meter programs to overwrite meter firmware and spoof communications with utilities and the grid. It is a near certainty that 'script-kiddie' style attacks on meters will be easily attainable off the Internet.
3. **Extended attack surface:** AMI extends the attack surface for metering to entire public networks. Tampering at the endpoints of these networks is particularly useful for energy theft as the demand information for many meters passes through collector meters and links to utility servers.

Note that this list is in no way comprehensive.

In this paper, we studied the ways in which energy theft is likely to occur in AMI systems. Our findings show that those interested in mounting theft will have the capacity to do so, at least in the foreseeable future. What is left is to begin working now in further identifying the vulnerabilities and finding ways to mitigate them. Such efforts should not only be targeted to combating theft, but also to all of the other personal and national safety issues vulnerabilities in AMI systems represent. It is our hope that this paper has provided a usable roadmap to begin these efforts.

References

1. 3CX. FXS, FXO Explained. `http://www.3cx.com/PBX/FXS-FXO.html`, 2009.
2. American National Standards Institute. ANSIX3.92-198 Data Encryption Algorithm, 1981.
3. American National Standards Institute. C12.18 Protocol Specification for ANSI Type 2 Optical Port, 2006.
4. National Cable Television Association. Ncta 2005 signal theft survey. `http://www.ncta.com`, 2005.
5. D. D. Clark and D. R. Wilson. A comparison of commercial and military computer security policies. In *IEEE Symposium on Security and Privacy*, pages 184–195, 1987.
6. Yvo Desmedt. Man in the middle attack. In Henk C. A. van Tilborg, editor, *Encylopedia of Cryptography and Security*, page 368. Springer, 2005.
7. Chris S. King. The economics of real-time and time-of-use pricing for residential consumers. Technical report, American Energy Institute, 2001.
8. R. Kinney, P. Crucitti, R. Albert, and V. Latora. Modeling cascading failures in the north american power grid. *The European Physical Journal B - Condensed Matter and Complex Systems*, 46(1):101–107, July 2005.
9. Electric Light and Power Magazine. Reducing revenue leakage. `http://uaelp.pennnet.com/`, 2009.
10. Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, November 2009.
11. Netwondo LLC. Unlock your google phone. `http://www.unlock-tmobileg1.com/`, 2009.
12. Patrick McDaniel and Stephen McLaughlin. Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy Magazine*, May/June 2009.
13. The Asterisk Project. Asterisk open source pbx. `http://www.asterisk.org`.
14. Bruce Schneier. Attack trees. *Dr Dobb's Journal*, 24(12), December 1999.