Unified Architecture for Large-Scale Attested Metering

Michael LeMay, George Gross, Carl A. Gunter, Sanjam Garg
University of Illinois Urbana-Champaign
{*mdlemay2,gross,cgunter,sanjamg*}*@uiuc.edu*

Abstract

We introduce a secure architecture called an attested meter *for advanced metering that supports large-scale deployments, flexible configurations, and enhanced protection for consumer privacy and metering integrity. Our study starts with a threat analysis for advanced metering networks and formulates protection requirements for those threats. The attested meter satisfies these through a unified set of system interfaces based on virtual machines and attestation for the software agents of various parties that use the meter. We argue that this combination provides a well-adapted architecture for advanced metering and we take a step towards demonstrating its feasibility with a prototype implementation based on the Trusted Platform Module (TPM) and Xen Virtual Machine Monitor (VMM). This is the first effort to use virtual machines and attestation in an advanced meter.*

1. Introduction

Advanced metering systems [1] are a key component in all of the demand reduction and self-healing grid initiatives that have been proposed over the last several decades. They have great potential to improve the stability and reliability of the electric power grid, and will become key tools to empower consumers in the energy market. However, if they are not based upon a secure system architecture, they could in fact become one of the grid's most significant liabilities, due to their expected pervasive deployment.

Data collection and control systems on the grid are expected to have lifetimes stretching into the decades, and thus are designed with extreme reliability and dependability as primary objectives. However, these systems have traditionally existed in isolation, on dedicated networks that are owned and controlled by Electric Service Providers (ESPs). Isolation has made these systems intrinsically less vulnerable to a variety of security threats.

In contrast, advanced metering systems may be connected to the Internet, or even a wireless network that is highly vulnerable to eavesdropping and physical attacks. Thus, it is unacceptable to protect the data and control information flowing to and from meters using the fixed-key cryptography and simple passwords that have traditionally been used to protect IT resources on the power grid.

Additionally, advanced meters could be used for several other purposes besides simple metering, and such sharing appears to be necessary to make advanced metering economically viable [23]. This raises difficult questions about how ESPs will preserve the integrity of the critical billing information gathered by meters, and how we can isolate applications originating from diverse, mutually-distrustful domains while allowing them to execute simultaneously on a single meter.

With these issues in mind, we have developed a comprehensive security architecture for advanced meters. We analyze the unique security requirements of metering systems and use several cutting-edge security technologies in concert to provide a secure computing and communication base that satisfies those requirements. Our work will have implications in the fields of Internet-connected control systems, Trusted Computing (TC) and attestation, virtualization, and access control architectures.

In its most essential form, the attested meter uses Virtual Machines (VMs) to isolate several applications running simultaneously on a single meter. This preserves the integrity and confidentiality of the logic and data within each application, while still permitting controlled cooperation between different applications. This is necessary, since some applications may export functionality to other applications on the same meter.

The attested meter provides a Mandatory Access Control (MAC) enforcement module for network communications that will regulate each application VM on the meter. The network policies are formulated by application providers, since they most clearly understand the data requirements of their own applications. These policies are presented to customers to allow them to verify that their privacy is being preserved.

According to the dictionary, to attest to something is to affirm that it is true or genuine. Attestation allows the at-

1530-1605/07 $20.00 ©2007 IEEE

tested meter to prove to a remote entity that it is using hardware and software that the remote entity trusts. To accomplish this, it uses asymmetric keypairs, hardware-protected storage, and cryptographic coprocessors that are securely embedded in a Trusted Platform Module (TPM) [4]. The exact mechanisms used to establish trust in individual components will be discussed in more detail below.

To motivate the attested meter, we have included a comprehensive threat analysis that predicts the capabilities and intentions likely to be exhibited by a variety of attackers. Our prototype implementation of the attested meter, using COTS hardware and software components, demonstrates how the attested meter defends against these attacks in a practical setting.

The rest of this paper is organized as follows. In Section 2, we describe the functional characteristics of advanced metering. In Section 3 we describe the security requirements and attacker profiles that are relevant to advanced metering. The actual architecture is presented in Section 4, along with background on the underlying technologies that it uses. We are currently developing a prototype implementation of our reference architecture, and we discuss that effort in Section 5. Next, we discuss other research efforts that have had an influence on our work or recommend a different approach to meter security. We conclude our paper with a discussion of the main outcomes of our work thus far, and a brief overview of our future work.

2. Review of Advanced Metering

2.1. Functional Characteristics

An "advanced meter" is is an electronic meter that can at least be read remotely. In the future, advanced meters will provide many capabilities beyond this basic requirement, and afford a number of potential advantages to ESPs, their customers, and many other entities [1]: *1) Customer control*: Customers gain access to information on their current energy usage and real-time electricity prices. *2) Demand response*: Power utilities can more effectively send control signals to advanced metering systems to curtail customer loads, either directly or in cooperation with the customer's building automation system. Current demand response schemes are typically very coarse-grained and provide marginal power savings. *3) Improved reliability*: More agile demand response and Distributed Energy Resource (DER) management can improve the reliability of the distribution grid by preventing line congestion and generation overloads. These improvements will also reduce the strain on the transmission grid. *4) Simplified sub-metering*: Multiple customers can be monitored by a single meter, reducing equipment costs and maintenance burdens. In some settings, it may even be possible for an MDMA to collect readings from multiple meters in a hierarchical fashion.

There are several distinct categories of advanced metering systems that support the functionality discussed above with varying degrees of success. The least capable systems use short-range radio networks, requiring readers to drive by in vans to read the meters. More capable systems support unidirectional fixed network communication, and the most capable systems have fully bidirectional network connections. The less capable systems are typically less expensive to deploy initially, but fully networked systems provide more economic benefits in the long run [9]. Thus, we concentrate on meters with bidirectional connections throughout this paper.

Meter reading systems with fixed networks usually allow service providers to distribute real-time pricing schedules to meters, which can influence customer behavior and induce manual or automatic demand response actions. Many systems also support direct control signals. These may be desirable for managing a distributed energy resource, or for controlling a primary breaker on a premise without dispatching a maintenance worker.

In Figure 1, we show how a bidirectional metering network that is based on the attested meter could be organized. The network is divided into two main domains that are connected via a WAN link. The first domain houses the MDMA and its associated applications, such as those for analyzing metering data. The second domain comprises the metered premises, which may have mesh network connections between themselves to extend the overall reach of the metering network. Each of these premises may also be equipped with a facilities LAN containing a consumer portal, which interacts with a consumer portal application on the meter. The LAN also provides connectivity for a management console from which the customer interacts with the consumer portal, most likely using a web browser as the interface.

2.2. Unique Characteristics

Just as cellphones have become ubiquitous, mobile computing platforms, advanced meters may become the first ubiquitous, fixed (non-mobile) computing platforms. This could have a number of positive outcomes, such as the expansion of network access into currently unreachable areas. However, it also raises serious privacy concerns. The introduction of cellphones compromised the location privacy of customers, since the radio signals of cellphones can be tracked to determine the approximate locations of cellphone users [29]. Similarly, advanced meters can be used to determine not only whether a metered premise is occupied, but also how the occupants of the premise are currently behaving [13]. This information could be correlated with location information to develop detailed profiles of those individu-

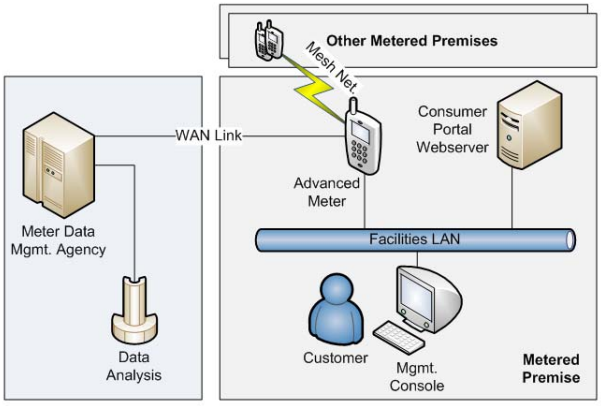

Figure 1. Proposed bidirectional metering network interactions.

als, unless we control the dissemination of such information.

Another significant characteristic of advanced meters follows directly from the previous one. Massive meter deployments may lead to significant availability issues. If many meters attempt to transmit large quantities of data simultaneously, they may overload their communications infrastructure. This could interrupt service providers' income, if they are unable to collect billing data for significant periods of time. It could also lead to blackouts if load reduction signals are blocked or delayed. Thus, the attested meter minimizes bandwidth requirements wherever possible.

3. Security Requirements

The attested meter attempts to provide the three major security assurances referred to by the acronym CIA: confidentiality, integrity, and availability. It also strives to preserve customer privacy. In the following section we attempt to predict some specific ways in which various adversaries may attempt to undermine these assurances.

Different attackers are likely to have different objectives. There are several categories of attackers that have appeared in the past, and are likely to be particularly significant to advanced metering networks.

3.1. Curious Eavesdroppers

Possibly the least dangerous type of attacker is the curious eavesdropper. In a residential setting, neighbors are often interested in the behavior of occupants in surrounding homes. Currently, they satisfy their curiosity by observing the lights and sounds of a household, which serve as coarse indicators of occupant activity. When advanced metering systems are deployed, these curious individuals may attempt to determine more detailed information about their neighbors by eavesdropping on the communications of advanced meters.

It seems unlikely that an ordinary individual will be sufficiently motivated to spend more than a few hours acquiring such information. However, if meter communications are not properly secured, it may be possible for skilled developers to distribute scripted utilities for capturing and analyzing those communications. This could lead to something like the "script kiddy" phenomenon that has occurred in the realm of computer cracking. This sort of scenario would be particularly feasible if meters communicate to form mesh networks, in which the communications from each meter may flow through several others on the route to the MDMA.

To prevent eavesdropping, we use strong cryptographic techniques to preserve confidentiality, making it extremely difficult or impossible to develop tools capable of compromising a large class of systems automatically. Additionally, we attempt to ensure that the information meters transmit is not useful or interesting to eavesdroppers. For example, we transmit a monthly bill from the meter rather than sending interval measurements, so that eavesdroppers will be unable to determine much information about customers' behavior, unless they are able to access the meter itself.

3.2. Motivated Eavesdroppers

Thieves and other criminals are likely to have capabilities only marginally superior to those of curious eavesdroppers, but may be much more motivated. They could benefit greatly from having enhanced information about the behavior of building occupants, to help them plan crimes. As we mentioned above, one of the primary sources of information about building occupants comes from their lighting. This is why vacationers often put their lights on timers, to obscure their true occupancy status [11].

If thieves were able to access detailed power measurements from homes, their intelligence capabilities would be greatly improved, increasing their probability of performing robberies without being captured. If they were able to remotely compromise meters and perform surveillance over the network, their productivity and elusiveness would be enhanced even further.

Given the enormous potential rewards for their labor, this class of attacker may be willing to perform physical modifications to meters or other infrastructure elements, to enhance their capabilities.

To prevent these attackers from achieving success, the attested meter relies on tamper detection components to deal with hardware modifications. It also uses confidentiality-preserving techniques on network communications that can withstand targeted attacks, which will almost certainly be more potent than the scripted attacks discussed above. We

assume that the communications medium the meter uses can be directly accessed by adversaries that have installed taps or compromised other nodes that route a particular meter's communications.

3.3. Unethical Customers

Unethical customers may attempt to steal electricity by tampering with metering hardware or software, or its communications. These insiders may have capabilities and motivation levels similar to external thieves, but they will have more opportunities to physically tamper with their metering equipment, since they are the legitimate occupants of the metered premises.

The objectives of internal thieves are quite different from those of external thieves. External adversaries are primarily concerned with compromising the confidentiality of meter data, whereas dishonest customers wish to compromise the integrity of meter data, to reduce their bills. To accomplish this, they may either reduce the usage reported by the meter, or they may shift usage indications from higher-priced time intervals to lower-priced intervals.

It is generally impossible to entirely prevent the hardware or software tampering that could be used to carry out these attacks, since the customer has physical control over both the meter and the wiring in the house, but we attempt to make it at least as difficult to tamper with attested meters as it currently is to tamper with mechanical meters. Remote attestation is used by the MDMA to detect software tampering that could be a sign of customer theft, and tamper detection modules report hardware modifications.

3.4. Overly Intrusive Meter Data Management Agency

One of the most important adversaries the attested meter protects against is an overly intrusive MDMA. The MDMA is an external entity that is responsible for interacting directly with the meter to gather billing data and other statistics. The MDMA processes the data that it collects, and then transfers it to other clients that require the data, such as the ESP's billing department. Thus, by protecting against an overly intrusive MDMA, we also protect meter users from all of the MDMA's clients.

If MDMAs were granted access to high-resolution data collected on customers' meters, they would be able to construct detailed profiles of the behavior of those customers. This is demonstrated by [13], which discusses how electrical appliances can be distinguished by how much active and reactive power they require. Given a set of appliance power signatures, it is actually possible to take a series of active and reactive power measurements and determine which appliances were running at each point in time by studying the transitions in those measurements. In fact, measurements from a single point on the main line feeding a residence often provide sufficient information to distinguish between loads within the residence that are as similar as the small and large burners on electric stoves.

Thus, we must provide mechanisms for making MDMAs accountable to their customers whenever they collect data from meters. The attested meter includes a trusted third party that regulates the network communications of all other applications on the meter. The network policy for each application is actually formulated by that application's author and accompanies the application itself. The privacy-preserving properties of the policy are lucidly presented to the customer through the consumer portal, and any attempted policy violations are also reported using the consumer portal. Thus, both the customer and the service provider are assured that their interests are being protected.

3.5. Active Attackers

The attested meter addresses the serious threats posed by terrorists and other active attackers. It has been noted that Al Qaeda has a high level of interest in Supervisory Control And Data Acquisition (SCADA) systems [14]. If metering systems with control capabilities are deployed, it is likely that terrorists will also attempt to exploit those systems. Thus, the introduction of advanced metering systems could actually serve to broaden the power grid's attack surface.

Active attackers that wish to disrupt the powergrid using the metering infrastructure could adopt a number of tactics. The most obvious tactic would be to access the meters themselves and instruct them to cut off power to the metered premises, using the hard disconnect function included on some meters.

To prevent these attacks, we must ensure that remote entities authorized to perform control functions are properly authenticated. We must also ensure that meters are constructed using appropriate security engineering techniques to prevent software exploits from granting unauthorized access to control functions. The attested meter includes a number of applications that satisfy these properties, and also ensures that non-compliant applications are unable to compromise other applications on the same meter.

In recent times, attacks against the network infrastructure supporting various applications have become more common. Typically, these take the form of Denial of Service (DoS) attacks. Grid instability or even a blackout may occur if such an attack against a metering network could be sustained for a sufficient length of time, since load reduction signals could be blocked. DoS attacks can be carried out at a variety of logical and physical layers of the network, and are difficult to eliminate entirely. However, certain net-

work technologies are more vulnerable to DoS attacks than others, and must be carefully configured to minimize these risks [6].

3.6. Publicity Seekers

A significant portion of the cracker community is fueled by a desire for notoriety [17]. Currently, crackers release worms and viruses that attack large numbers of computers connected to the Internet, and they also perform targeted attacks against smaller numbers of computers. These attacks often generate significant publicity, from which the cracker derives some degree of satisfaction. However, much more publicity could be generated by an attack against a metering network that causes blackouts or other physical effects.

Future advanced meters may share many architectural features with smartphones, since both are embedded architectures with communications capabilities. Crackers have already developed viruses to attack smartphones [18], which raises concerns about viruses attacking metering networks. In fact, meters may be intrinsically more vulnerable than phones, since they will have constant network connectivity and will most likely run network servers that could potentially be exploited without requiring the meter owner to perform any operation to infect the meter.

The attested meter prevents these attacks from completely disrupting the meter by isolating applications from one another, so that a successful attack on one application does not damage other applications on the meter. In the future, these techniques could potentially be applied to protect smartphones as well.

4. Attested Metering Architecture

This section provides a detailed design for the attested meter. First, we provide a solid basic platform for supporting arbitrary embedded applications. This platform provides fundamental assurances such as application isolation, integrity measurement and protection, and mandatory access controls. Next, we include an architectural specifications for the most unique application in our architecture.

4.1. Virtualization

The first specific objective of our system is to permit controlled sharing of metering hardware. We wish to allow many service providers, plus the customer, to run their own applications on a single meter without interfering with each other. Some interaction between applications will be necessary, since some applications may provide system services that other applications use, such as building automation interfaces.

However, we must ensure that both applications permit those interactions, and that the interactions are minimized and strictly controlled by a mandatory access control policy. For example, the MDMA agent on each meter requires access to the demand response application, so that it can coordinate demand response actions. However, we must ensure that the demand response application is unable to compromise the integrity of the metering data in the MDMA agent. Typical operating systems are unable to provide strong isolation between applications, so we rely on virtualization technologies.

A Virtual Machine Monitor (VMM), also known as a Hypervisor, can partition a single physical machine into several logical system images, known as Virtual Machines (VMs). Each of these VMs supports an independent OS instance, with its own set of isolated virtual resources. The degree of isolation provided by the Virtual Machine Monitor (VMM) can be adjusted based on application requirements, and it is easier to determine the ways in which that isolation can be violated on a VMM than on a standard Operating System (OS) because VMMs are usually implemented using much smaller codebases than most conventional OS kernels.

Xen is a popular para-virtualization environment on PCs [7]. It satisfies most of our requirements, including support for mandatory access control over both physical and virtual resources with the sHype framework [24]. Other capable security architectures have already been built atop Xen, demonstrating its utility [22].

4.2. Mandatory Access Control for Networking

Just as controlled inter-application communications are a necessary precondition for strong application isolation, extra-application communications must be controlled to protect the privacy of customer data. As we discussed in our threat analysis section, we are concerned about an overly invasive MDMA gathering too much detailed information on customer consumption habits. We are also concerned about rogue VMs establishing connections to arbitrary endpoints and releasing sensitive information. The obvious countermeasure to this possibility is a MAC framework for network communications.

In the Xen VMM that was discussed in the previous section, the physical network devices in the meter are managed by a specific virtual machine that presents a high-level driver interface to all other VMs on the meter. Thus, by controlling the network connections passing through the network device VM, we can control all networking on the entire meter.

To impose meaningful restrictions on communications, the proposed system must consider state information from

past and current connections, and should also dissect any standard protocols in use to monitor the semantic values being transmitted by VMs. For standard protocols, this permits the Mandatory Access Control (MAC) framework to not only restrict how much data each VM is permitted to send to specific parties, but also what types of measurements can be transmitted with specific frequencies. Both permitted and denied transmissions will be audited and made available to the consumer portal VM.

The networking policy to be applied to each VM will be provided by the party that supplies the VM, since they are most familiar with the data requirements of that VM. However, the privacy implications of the policy will be described to the customer through the consumer portal, preferably using a graphical diagram or other comprehensible presentation format, and the VM's actual transmissions will also be presented to the customer using a similarly lucid format.

Incidentally, these network policies should help to reduce the bandwidth usage of metering applications. If applications are developed to operate within the framework of strict bandwidth limitations to preserve privacy, then they will use the communications infrastructure more efficiently. However, when large numbers of meters are deployed, temporary network outages become inevitable. Thus, the applications that run on meters must also be capable of tolerating short outages. In the case of ESPs, this sort of tolerance is already built into the billing system, but other applications may need to be adapted.

4.3. Trusted Computing and Attestation

One of the primary goals of the attested meter is to reduce the amount of information that must be transmitted between meters and remote entities such as the MDMA. Thus, we would like to perform data processing as close as possible to the origin of that data. For example, we specify that the meter must compute the customer's monthly bill locally. However, for this arrangement to be acceptable to those who have a financial stake in the outcome of the computation, we must provide techniques for remotely verifying the integrity of the hardware and software components performing the computation.

Remote attestation is one of the most promising applications supported by Trusted Platform Modules (TPMs) [4]. It is a technique for remote entities to determine what hardware and software another system is using. The measurements are recorded by a tamper-resistant hardware device (the TPM) containing an embedded private key that is used to sign the measurements. The private key has a corresponding public key that is certified by the manufacturer of the TPM and can be used to verify signatures generated by the TPM. TPMs also contain a set of registers called Platform Configuration Registers (PCRs) that can only be modified by the TPM.

Applications interact with the TPM through a restricted interface that allows them to provide raw data for the TPM to digest and add to a particular PCR. When it comes time to attest to the state of the system, the remote system requesting the attestation must provide a 160-bit nonce to prevent replay attacks. This nonce is then signed, along with a PCR containing the desired measurement, and returned to the remote system. This signature is accompanied by a list of hash values representing the important software and hardware components installed in the system. The remote party can then search for these hashes in a database of components that have been certified in some fashion, perhaps by a vendor or consumer protection group.

By themselves, these hash values have very little semantic value, since they simply prove that the system was in some configuration at the time the attestation was generated [25]. Typically, the remote party requesting the attestation is most interested in the future behavior of the system providing the attestation. Thus, advanced schemes must be developed to analyze the information flows that are present within a system and use the result of an attestation at one point in time to provide a basis for showing that the system will never enter an invalid state [12, 16, 26].

4.4. Consumer Portal

The most unique application in the attested meter is what we refer to as a "consumer portal VM," for reasons that will quickly become apparent. This application serves as an agent for the customer that physically owns the meter in question. It exports information to an external "consumer portal" application and also accepts control commands and configuration information from that portal. The portal itself will probably take the form of a dynamic website that provides an intuitive interface for customers. We did not invent the concept of a consumer portal, and its general requirements have been discussed elsewhere [28]. However, the attested meter is the first to specify a concrete instantiation of the general concepts underlying the consumer portal, including a unique customer authentication mechanism.

Customer Authentication Customers must be authenticated to their advanced meters before they are granted access to any metering data. Due to space restrictions, we reserve a detailed discussion of authentication protocols for a future publication, but we do suggest a few basic guidelines here.

By default, customers will possess a certificate or other authentication token that they can use to authenticate themselves to their meter. This token shall be associated with the meter by authenticated maintenance personnel whose actions are irrevocably audited and reported to the customer.

Alternatively, customers who have physical access to their metering hardware can exploit its interface to perform authentication without relying on third parties. Most advanced meters already include small displays that can be used to convey short strings of text to the user. This interface could easily be extended to include a small selection of buttons that accept input from customers for use in interactive authentication protocols.

Customer Authorization After authenticating customers using the scheme discussed above, we must control how customers access the meter's functions and data stores. In a typical installation, all of the information the meter collects should be reported to the customer, so that they can make fully informed decisions about their energy consumption.

In some installations it may be necessary to provide meter access to additional parties, particularly in industrial or academic campuses that are staffed by dedicated facilities personnel. The meters in these installations will be equipped with more advanced consumer portal VMs that contain sophisticated access control systems.

Other individuals such as maintenance personnel also have access to the meter, and their actions can be limited using a similar access control policy. For practical reasons, customers may not be permitted to modify this policy themselves, but its security implications will be presented using similar techniques as those applied to network access control policies. Furthermore, all significant operations performed by maintenance personnel are irrevocably audited and reported to the customer.

5. Prototype Implementation

We are currently in the early stages of constructing a prototype attested meter to demonstrate its feasibility and utility. In this section, we describe the results of our initial implementation experiences, and discuss our ongoing efforts.

5.1. Metering Platform

Computing Platform The focal point of our prototype is the computing platform that actually implements our basic architecture. Initially, we are developing prototypes based on commodity desktops using the IA32 architecture, since they are readily accessible and support all of the software components that the attested meter requires. However, in the future we will develop prototypes based on embedded processors such as the ARM, to demonstrate how the attested meter can be scaled down to the processors that are the best candidates for future metering hardware.

The most basic software component installed on our platform is the Xen VMM. Our final prototype will run at least four distinct VMs on this platform. The management VMs will provide support for device drivers, and implement the network access control module we discussed earlier. The second VM in the diagram will implement the interface to the MDMA. It will establish network connections to the MDMA, and also provide information to the consumer portal VM. The consumer portal VM will reside within the third VM on the system, and will interact with the network enforcement module and provide information to the external consumer portal application. Finally, the demand response VM provides services to both the MDMA and consumer portal VMs.

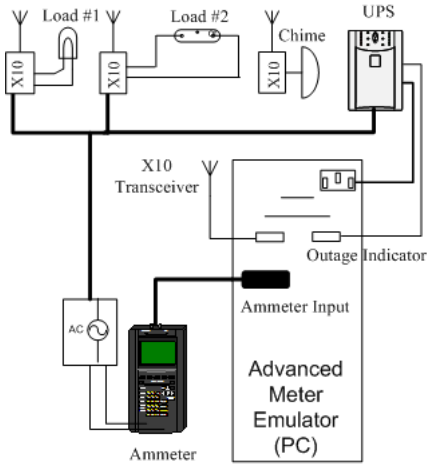

Figure 2. Physical interactions of prototype

Physical Interfaces Our emulated meter maintains connections to several sensors and actuators that realistically simulate various features of future metering systems, as demonstrated in Figure 2.

Most importantly, our meter reads data from a RadioShack digital multi-meter, via an RS-232 serial connection. Our current meter only provides active power measurements, but our final prototype will use reactive power measurements as well, to explore the ways in which that information can enhance the usage statistics provided via the consumer portal.

Our meter also interfaces with a USB-connected uninterruptible power supply, which notifies the meter of outages and reports the line frequency. One important feature of advanced meters is their ability to automatically report outages to the MDMA, which is explored by our prototype.

Additionally, our meter can send direct control signals to X10 home automation devices, to simulate demand response actions. These simple devices have a subset of the capabilities of industrial building automation systems, although they are designed for much less demanding applications. We use them to physically simulate the effects of

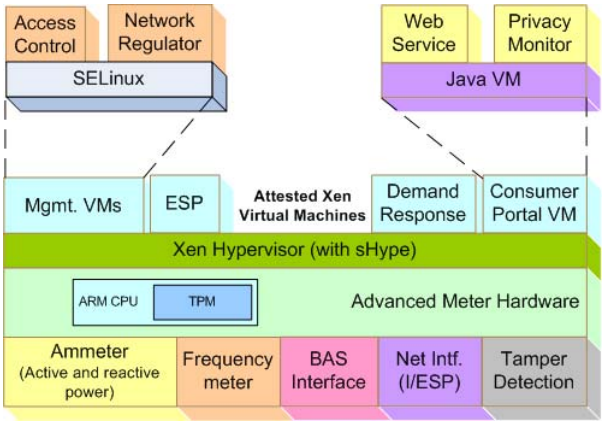

Figure 3. Layered system architecture

various demand response strategies.

Of course, our metering platform requires network connectivity. In reality, meters would most likely be connected to at least two networks, one for communicating with the MDMA and one for communicating with the customer, but our prototype currently uses a single Ethernet connection for all of its communications.

5.2. Virtual Machines

We are developing four applications that will run in separate virtual machines on our platform. We have selected these particular applications for our discussion because they are relevant to electrical metering and provide the most commonly required functionality. The attested meter is completely extensible, so these are by no means the only applications that can be installed on a meter, nor is it necessary for all of these applications to be installed on all meters.

The resulting layered system is depicted in Figure 3. In the lowest layers of the figure, we have shown the hardware components that may be used to construct a typical meter. The Xen hypervisor occupies the next layer, since it is the only software component that interacts directly with hardware. Each of the components shown above the hypervisor is a separate virtual machine, and is described in more detail below. Our architecture is capable of supporting arbitrary VMs, but we have only shown those that are directly relevant to electrical metering.

Supervisor VM The privileged VM supervises the other VMs. Specifically, it provides support for network policy enforcement, and mandatory access control over the other VMs that are run on the meter. It uses the security features provided by SELinux [19] for operating system controls, and sHype for VMM controls. It has recently become possible to decompose the functionality of the privileged VM into several less-privileged VMs, to provide better fault isolation.

Meter Data Management VM The second VM emulates the MDMA's software agent. It reads physical measurements from our electrical meter and records those measurements in a lightweight database. It communicates with the MDMA itself using the ANSI C12.22 protocol [2], and the ANSI C12.19 data table definitions [3].

The MDMA agent has support for real-time pricing and demand response commands. When it receives a command that should trigger a demand response event, it delegates the command to the demand response VM for further processing.

Demand Response VM This VM controls the interface to the building automation system and also contains logic to process indirect demand response requests. Ultimately, this VM is under the control of the customer, so it is also capable of receiving commands from the consumer portal VM. These commands can be used to alter the way in which the demand response VM handles signals from the MDMA VM, and can also be used to directly invoke voluntary demand response events.

Consumer Portal VM The final VM interfaces with the external consumer portal application, and also has internal interfaces to both the MDMA and demand response VMs. Additionally, this VM interacts with the network policy enforcement module installed in the privileged VM to process the alerts provided by that module, reporting them to the external consumer portal application as necessary.

The interface between the consumer portal application and the consumer portal VM conforms to an OASIS draft standard known as oBIX, for Open Building Information eXchange [10]. This document specifies a standard set of data types for information exchanged between various building information systems, and also specifies a number of special documents for retrieving metadata describing accessible objects. We use this metadata to automatically adapt our consumer portal application to whatever consumer portal VM is currently in use.

5.3. Attestation.

Currently, we are using the Linux Integrity Measurement Architecture (Linux-IMA) to provide attestations from all of these applications. Linux-IMA measures all of the binary applications that are loaded by the Linux kernel and records those measurements in the PCRs of the TPM. Xen provides a unique virtual TPM (vTPM) to each VM [8], so we can install Linux-IMA in each of the VMs without causing conflicts. Of course, we must also guarantee the integrity of

Linux-IMA itself, and the integrity of the component that performs that measurement, until the chain eventually terminates at the TPM itself [5].

6. Related Work

Many other security analyses of various aspects of the power grid have been performed, such as the one within the IntelliGrid Project [15]. However, these analyses usually produce a laundry list of security technologies that can be applied to various parts of the electrical infrastructure, without specifying how those security technologies can be integrated to achieve meaningful security goals. In contrast, the architecture proposed in this paper makes specific recommendations for using security technologies in concert to provide confidentiality, integrity, availability, and privacy assurances to all meter users. Additionally, other architectures tend to lag behind the current state-of-the-art in computer security techniques, whereas the attested meter uses virtualization and Trusted Computing (TC) techniques that have only recently become feasible.

The security and privacy requirements of advanced metering systems are specifically addressed in [27]. This document provides a valuable overview of the legal requirements for security and privacy in metering networks, and reinforces our assertion that access to detailed usage statistics should be carefully compartmented even within the energy service provider. However, their security architecture recommends reliance on controls internal to the MDMA to preserve customers' privacy, at least until meters become capable of calculating monthly bills locally. Furthermore, they focus on closed platforms that are unable to simultaneously support applications from multiple providers.

Their apparent motivation for this narrow focus is that computationally powerful meters are too expensive to be deployed in residential settings. However, it is our belief that value-added services can be used to offset the costs of powerful meters. Additionally, these meters will provide much better protection for customer data, and reduce the strain on the network infrastructure supporting the meters. Finally, the authors focus on a particular type of advanced metering system, one characterized by numerous sensors scattered throughout homes and businesses, and equipped with Software Defined Radios (SDRs). The attested meter is more general, and not tied to any specific network topology.

One of the primary objectives of the attested meter is to efficiently support large-scale meter deployments. This issue has long been a concern, and is the primary focus of [21]. A metering network with one million nodes is informally analyzed, and the scalability issues of such a network are presented. It is assumed that the meters will be read once a month, and that it takes two seconds to perform the entire read operation on each meter. Assuming that the meter reading operations occur serially, it will take 23 days of continuous operation to read all meters once, assuming 100% reliability. A number of communications technologies that were available as of 1995 are reviewed, and the paper focuses specifically on low-power RF and power-line-carrier (PLC) mediums. Since that time, much higher-bandwidth mediums have been developed, such as WiMAX and Broadband over PowerLines (BPL). However, the basic analysis remains sound. Unsurprisingly, the final conclusion of the paper's analysis is that the bottleneck of the system is the MDMA. We foresee similar problems in future networks that can only be alleviated by processing data as close to its origins as possible, as the attested meter requires.

The consumer portal is one of the key components of the attested meter. Its basic features were defined in a document produced by the IntelliGrid Project [28], which in turn borrowed heavily from [20]. In its most essential form, it is a service that provides real-time information about energy usage to customers. The IntelliGrid definition includes a large list of protocols that can be used to construct a consumer portal, including a list of standard security protocols such as SSL. However, they have not considered more advanced TC technologies, and don't discuss specific capabilities of consumer portals. The consumer portal featured in the attested meter supports all of the features recommended by IntelliGrid, and has similar objectives to their abstract portal. In addition, we integrate advanced TC technologies and our prototype provides concrete privacy controls to energy customers that were not mentioned in the IntelliGrid specification.

7. Conclusion and Future Work

Our architecture for secure metering is the first to integrate advanced trusted computing and virtualization technologies in a coherent architecture that preserves confidentiality, integrity, availability, and privacy throughout the IT infrastructure supporting metering systems.

We have reviewed the functional requirements for advanced metering systems, and discussed how our flexible architecture can be extended to support each of those requirements. Additionally, we have presented a detailed threat analysis of future metering networks, based on our current predictions of how those networks will be constructed. The attested meter provides strong defenses against each of the projected threats so that potential adversaries will find it more advantageous to attack other, weaker aspects of the power grid to achieve their overall objectives.

Finally, we have discussed our prototyping efforts, demonstrating that the attested meter has a practical realization. Our prototype should serve as a useful reference implementation for future efforts in this area. We have in-

vestigated the issues that are relevant to the operation of a shared meter after it has been initialized with a fixed set of software virtual machines. Due to space restrictions, we have not addressed the many issues surrounding software distribution, updates, and removal. These are important issues that will be addressed in our future publications.

Acknowledgements

We would like to thank Carl Hauser, Sean Smith and the rest of the TCIP Center team for their feedback on this work. We also thank the authors of [27] for sending us their report and Frank Mueller for suggestions on equipment for our prototype. This work was supported in part by NSF CNS05-24695, NSF CCR02-08996, and ONR N00014-02-1-0715. Michael LeMay was supported on an NDSEG fellowship from the AFOSR.

References

[1] Automatic meter reading (AMR) and related customer service functions. *EPRI IntelliGrid Consortium, http://www.intelligrid.info*, 2004.

[2] Protocol specification for interfacing to data communication networks. *National Electrical Manufacturers Association*, (ANSI C12.22), 2005.

[3] Utility industry end device data tables. *National Electrical Manufacturers Association*, (ANSI C12.19), 2005.

[4] TPM main: Part 1: Design principles. *Trusted Computing Group, https://www.trustedcomputinggroup.org/specs/TPM*, Mar. 29, 2006.

[5] W. Arbaugh, D. Farber, and J. Smith. A secure and reliable bootstrap architecture. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 65–71, May 1997.

[6] M. Barbeau. WiMax/802.16 threat analysis. In *Q2SWinet '05: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pages 8–15, New York, NY, USA, 2005. ACM Press.

[7] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. Xen and the art of virtualization. In *SOSP '03: Proceedings of the nineteenth ACM symposium on Operating systems principles*, pages 164–177, New York, NY, USA, 2003. ACM Press.

[8] S. Berger, R. Caceres, K. Goldman, R. Perez, R. Sailer, and L. van Doorn. vTPM: Virtualizing the trusted platform module. Technical Report RC23879, IBM, NY, Feb. 2006.

[9] S. Borenstein, M. Jaske, and A. Rosenfeld. Dynamic pricing, advanced metering and demand response in electricity markets. *Center for the Study of Energy Markets*, Oct. 31, 2002.

[10] B. Frank. oBIX specification, working draft. May 2006.

[11] S. Hakim, G. F. Rengert, and Y. Shachamurove. Knowing your odds: Home burglary and the odds ratio. *IEEE Technology and Society Magazine*, Sept. 2000.

[12] V. Haldar, D. Chandra, and M. Franz. Semantic remote attestation–A virtual machine directed approach to trusted computing. In *USENIX '04: Proceedings of the Third Virtual Machine Research and Technology Symposium*, pages 29–41. USENIX Association, May 2004.

[13] G. Hart. Residential energy monitoring and computerized surveillance via utility power flows. *IEEE Technology and Society Magazine*, pages 12–16, June 1989.

[14] A. Hildick-Smith. Security for critical infrastructure scada systems. *SANS GSEC Certification, Practical Assignment*, Feb. 23, 2005.

[15] J. Hughes. The integrated energy and communication systems architecture; volume IV, technical analysis, appendix A. *Electric Power Research Institute*, 2004.

[16] T. Jaeger, R. Sailer, and U. Shankar. PRIMA: Policy-reduced integrity measurement architecture. Technical Report RC23898, IBM, NY, Mar. 2006.

[17] Y. Lafrance. Psychology: A precious security tool. *SANS GSEC Certification, Practical Assignment*, Feb. 2, 2004.

[18] N. Leavitt. Mobile phones: The next frontier for hackers? *Computer*, 38(4):20–23, 2005.

[19] P. A. Loscocco and S. D. Smalley. Meeting critical security objectives with security-enhanced linux. In *Proceedings of the 2001 Ottawa Linux Symposium*, July 25–28 2001.

[20] M. Magaletti, M. Rawson, L. ten Hope, T. Surles, and R. Therkelson. A strawman reference design for demand response information exchange. *EnerNex Corporation*, Oct. 31, 2004.

[21] S. Mak and D. Radford. Design considerations for implementation of large scale automatic meter reading systems. *IEEE Transactions on Power Delivery*, 10, Jan. 1995.

[22] J. McCune, S. Berger, R. Caceres, T. Jaeger, and R. Sailer. DeuTeRiuM - a system for distributed mandatory access control. Technical Report RC23865, IBM, NY, Feb. 2006.

[23] A. Patrick, J. Newbury, and S. Gargan. Two-way communications systems in the electricity supply industry. *IEEE Transactions on Power Delivery*, 13:53–58, Jan. 1998.

[24] R. Sailer, T. Jaeger, E. Valdez, R. Caceres, R. Perez, S. Berger, J. L. Griffin, and L. van Doorn. Building a MAC-based security architecture for the xen open-source hypervisor. *acsac*, 0:276–285, 2005.

[25] R. Sailer, X. Zhang, T. Jaeger, and L. van Doorn. Design and implementation of a TCG-based integrity measurement architecture. In *USENIX '04: Proceedings of the Thirteenth USENIX Security Symposium*, pages 233–238. USENIX Association, Aug. 2004.

[26] E. Shi, A. Perrig, and L. van Doorn. BIND: a fine-grained attestation service for secure distributed systems. In *2005 IEEE Symposium on Security and Privacy*, pages 154–168, May8–11 2005.

[27] P. Subrahmanyan, D. Wagner, U. Shankar, D. Mulligan, E. Jones, and J. Lerner. Network security architecture for demand response/sensor networks (draft). Oct. 2005.

[28] D. Von Dollen. IntelliGrid consumer portal telecommunications assessment and specification. *http://www.epriweb.com/public/000000000001012826.pdf*, Dec. 2005.

[29] J. Warrior, E. McHenry, and K. McGee. They know where you are. *IEEE Spectrum*, 40:20–25, July 2003.