Cyber Security Issues for Advanced Metering Infrastructure (AMI)

F. M. Cleveland Senior Member IEEE

Abstract *– Advanced Metering Infrastructure (AMI) is becoming of increasing interest to many stakeholders, including utilities, regulators, energy markets, and a society concerned about conserving energy and responding to global warming. AMI technologies, rapidly overtaking the earlier Automated Meter Reading (AMR) technologies, are being developed by many vendors, with portions being developed by metering manufacturers, communications providers, and back-office Meter Data Management (MDM) IT vendors.*

In this flurry of excitement, very little effort has yet been focused on the cyber security of AMI systems. The comment usually is "Oh yes, we will encrypt everything – that will make everything secure." That comment indicates unawareness of possible security threats of AMI – a technology that will reach into a large majority of residences and virtually all commercial and industrial customers. What if, for instance, remote connect/disconnect were included as one AMI capability – a function of great interest to many utilities as it avoids truck rolls. What if a smart kid hacker in his basement cracked the security of his AMI system, and sent out 5 million disconnect commands to all customer meters on the AMI system …?

Index Terms *– Security, Advanced Metering Infrastructure, smart meters, customer gateways, AMI network, AMI headend, Meter Data Management*

I. Generic Security Requirements and Threats

Generically, security requirements for managing data can be classified as follows:

- **Confidentiality** - Requirement that data is accessible only to authorized entities, and that intentional or unintentional disclosures of the data do not occur.
- **Integrity** - Requirement that data is authentic, correctly reflecting the source data, and complete, without unauthorized modifications, deletions, or additions. (This does not imply the data is valid, only that it is the same as the source.)
- **Availability** - Requirement that data is accessible by authorized entities whenever they need it.
- **Non-Repudiation** – Requirement that the entities receiving the data do not subsequently deny receiving it. The reverse is also true: that if the entities did not receive the data, then they cannot subsequently state that they did receive it.

Many different types of security threats can undermine these requirements, with some able to threaten many different vulnerable areas. For instance, a hacker who masquerades as a legitimate meter data management system can access confidential information, change control commands, deny access to legitimate systems, and repudiate having received critical data. Figure 1 illustrates the relationships between threats and the security requirements.

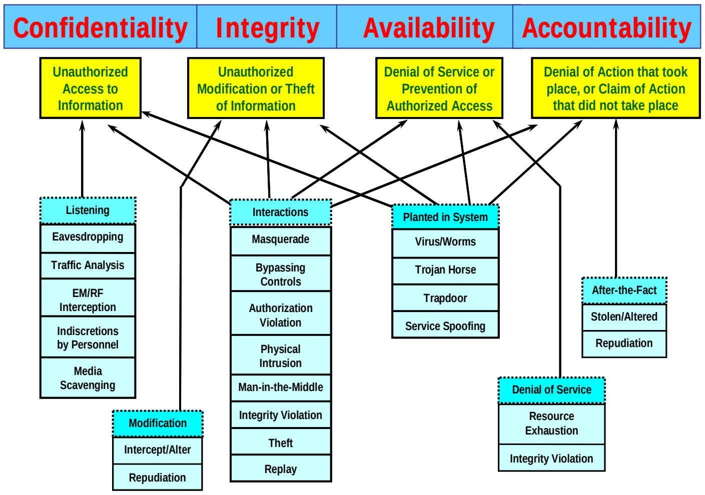

Figure 1: Security Requirements Undermined by Security Threats

All of the security requirements require some form of authentication of the entities, to determine if they are authorized to interact with the data.

II. AMI Security Requirements and Threats

For many aspects of AMI systems, the same types of requirements apply as for typical IT systems. However, AMI systems have some unique security requirements. Some of the key AMI requirements are discussed in the next sections. For the sake of these discussions, AMI systems are viewed as consisting of the following components:

- **Smart Meter** – The smart meter is the source of metrological data as well as other energy-related information. These smart meters can provide interval data for customer loads as well as distributed generation.
- **Customer Gateway** – The customer gateway acts as an interface between the AMI network and customer systems and appliances within the customer facilities, such as a Home Area Network (HAN) or Building Management System (BMS). It may or may not co-located with the smart meter.

- **AMI Communications Network** – This network provides a path for information to flow from the meter to the AMI headend.
- **AMI Headend** – This system manages the information exchanges between external systems, such as the Meter Data Management (MDM) system and the AMI network.

A. Confidentiality in AMI Systems

Privacy is the main issue for confidentiality in AMI systems at the customer site. Customers do not want unauthorized people or marketing firms to know how much energy they are using, what their pattern of energy usage is, or other energy-related information. Therefore, the metrology and energy information in their Smart Meters must be held confidential, including preventing the physical theft of meters for subsequent access to the stored data.

If the AMI system is also interfaced to a Customer Gateway into a HAN, commercial energy management system, or other private automated systems, the privacy of those systems must also be respected. At the same time, those systems must not be able to access unauthorized data or functionality in the AMI system.

Since AMI systems not only connect customer site gateways and meters to the utilities, but also provide potential communication channels between customers over the AMI network, privacy must also be addressed on this network as information is transmitted across it. In addition, the network channels must not allow unauthorized access for, say, one customer to view the energy information of another customer. Therefore, the AMI network will have to contain mechanisms to prevent customer-to-customer interactions, whether by the network's architecture or through security measures.

At the AMI headend, the customer information must again be kept confidential, with only authorized systems allowed to access specific sets of data. However, in this location, standard IT security measures can usually be used.

B. Integrity in AMI Systems

Integrity in AMI systems means not only preventing changes to data as it is retrieved from the meter, but also to the integrity of control commands, such as preventing unauthorized control commands from being transmitted through the AMI system to the smart meter or customer gateway. In fact, one of the scariest scenarios is a hacker issuing disconnect commands to millions of meters, by pretending to be a valid meter management system.

Requirements for security integrity start at the Smart Meter, where the meter itself must be both cyber-wise and physically protected against undetected changes. The key here is "undetected". There is absolutely no way for a meter stuck to a wall outside a customer's premises to be safe from a physical attack (i.e. ripped off the wall or smashed). In addition, the meter's "smart" computer chips can be breached, the contents exchanged, or new data added. However, if this attack is detected, then remedial actions can be taken, such as discounting any data from the meter or ignoring any control commands emanating from it, as well as "rolling the truck" to determine what happened.

Integrity of the Customer Gateways is also important since they may interface to critical equipment inside the customer premises, including grocery store freezers, industrial production equipment, or health-related monitors. Again, it is critical to recognize that these Customer Gateways can never be completely secure either physically or cyber-wise, so the most important aspect is the ability to detect even the most subtle unauthorized changes.

The AMI network is also open to external, unsecured environments, whether these are radio airwaves, cellular phone channels, power line carrier signals, or fiber optic cables. The focus therefore must again be on detecting potential integrity breaches as much as on trying to prevent them.

The AMI headend is typically in an apparently secure environment in a utility site or other meter data management site. However, because the data and control commands are more accessible (the AMI headend must interface to a variety of other systems) and because more knowledgeable personnel potentially have access to it, this area has additional integrity concerns. First there are just the inadvertent or careless mistakes that are bound to occur in any system and with any human participants. But in addition, there are the "disgruntled employee" threats, which are often far more dangerous because these employees know exactly what to do to cause maximum damage and how to avoid being detected – or at least how to do significant damage before they are detected and stopped. At the AMI headend, the metering data could be modified, dropped in a bit bucket, or replaced with seemingly valid data. From the AMI headend, commands could be sent to change pricing signals, request (or negate) load control actions, to reset meters, or to connect/disconnect loads and distributed generation. More insidiously, security certificates could be compromised such that some of these nefarious activities could also be initiated from a customer site or within the AMI network.

C. Availability in AMI Systems

In the past, availability of meter readings has not posed a big problem, since utilities would routinely estimate meter readings whenever they could not access them. However, with so much more than meter readings being exchanged between customer premises and utilities in AMI systems, availability of this information and control commands has become crucial.

The most important assessment of the impact of decreased availability becomes: "When is the value of specific information affected by its unavailability". Is the information critical within a 1 second timeframe? Within 10 seconds? Within an hour? Within a day? Can stored or estimated data replace monitored data within a longer timeframe? Can local intelligence be used to handle the unavailability of communications with remote systems?

Within the smart meter, the most common causes of decreased availability include the failure of some component, including physical damage, software glitches, and internal communications, as well as human tampering with the meter, possibly in attempts to change the readings by disconnecting the meter or "making the meter run backwards". Although most of these problems cannot be completely prevented (although steps can be taken to minimize their occurrence), the key to managing any decreased availability of smart meters is detection, along with assessments of the probable causes. This detection can include automated diagnostics, physical intrusion detection, and cyber intrusion detection.

At the customer gateway, availability is also a crucial issue, since pricing signals and other load control or distributed generation commands can have significant financial impacts on the customer. In addition loss of access to customer gateways could possibly cause serious electrical problems on the power system if large numbers of customer gateways or key customer gateways are unavailable at critical times. For key customer gateways, redundancy could be necessary to achieve the desired availability, while for other customer gateways, detection of decreased availability could be the most important.

The AMI network poses additional availability challenges since even redundant or meshed communications channels inherently have many points of failure, and often experience decreased availability in local areas due to radio interference, cut cables, path degeneration, loss of bandwidth, etc.

In addition to outright telecommunications failures, AMI network availability can be seriously affected by traffic overloads. In particular, if a power system outage affects millions of customers, "last gasp" outage alarms could flood the AMI network. If this AMI network is also being used to manage distributed generation or distribution automation or other critical functions, that information might not be able to get through in a timely manner. Therefore, managing the availability of the AMI network resources during emergency or critical times is more important than just detecting decreased availability.

Availability problems at the AMI headend may often reflect the initial system design, since AMI systems are still new concepts marrying new technologies with less than complete understanding of the scope of the functions that will use the AMI information or the eventual magnitude of the information flows.

D. Accountability (Non-Repudiation) in AMI Systems

Accountability or non-repudiation in AMI systems is critical for all financial transactions, including actual metrology information as well as responses to control commands. This accountability requirement is particularly problematic because often the different components of an AMI system are purchased from many different vendors and owned by many completely different entities, from customers, to AMI service providers, to Meter Data Management services, to utility billing systems. Even the data can be "owned" by different entities from the time it is created (say a meter reading), to when it is used by the customer for usage information, transported to the MDM for billing, and analyzed for load and generation patterns by utility planners.

In accountability, often timeliness of responses is as important as actually acting on a control command; therefore accurate timestamp information and continuous time synchronization across all AMI system components are crucial. Audit logs of key interactions are the most common way to ensure accountability (remembering that these audit logs can also be vulnerable to security integrity and availability threats).

In the smart meters, it is obvious that metered values should not be repudiated, since they are the basis for all billing. In addition, any changes to the meter's time and date, any time of use parameters, and other tariff-related parameters must be accountable.

Similarly in customer gateways, pricing signals, load control commands, and distributed generation commands should not be repudiated. In addition, all responses (or lack thereof) to these commands must also be captured.

The AMI network needs to be accountable for what information it did – and did not – transport to its final destination. This accountability of the AMI network is particularly critical since a customer gateway could "claim" that it sent critical data, thus fulfilling its accountability requirement, while blaming that the AMI network failed to transport the information.

The AMI headend will need to be responsible for collecting the information from many of the audit logs to provide a time-synchronized record of all critical transactions – which function itself must be accountable.

III. AMI CONSTRAINTS AFFECTING SECURITY SOLUTIONS

As can be seen from the above discussions of security requirements for AMI systems, solutions to the security threats must take into account many different issues, situations, and constraints. One security solution, such as encryption, simply cannot cover all security threats. Figure 2 illustrates some of the many security technologies and policies that can be used to provide the various security requirements.

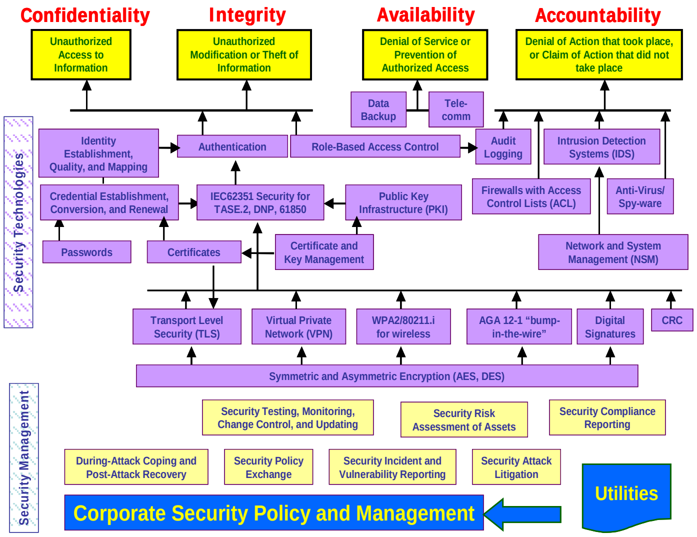
Confidentiality
Integrity
Availability
Accountability
Unauthorized Access to Information
Unauthorized Modification or Theft of Information
Denial of Service or Prevention of Authorized Access
Denial of Action that took place, or Claim of Action that did not take place
Data Backup
Tele-comm
Security Technologies
Identity Establishment, Quality, and Mapping
Authentication
Role-Based Access Control
Audit Logging
Intrusion Detection Systems (IDS)
Credential Establishment, Conversion, and Renewal
IEC62351 Security for TASE.2, DNP, 61850
Public Key Infrastructure (PKI)
Firewalls with Access Control Lists (ACL)
Anti-Virus/ Spy-ware
Passwords
Certificates
Certificate and Key Management
Network and System Management (NSM)
Transport Level Security (TLS)
Virtual Private Network (VPN)
WPA2/80211.i for wireless
AGA 12-1 “bump-in-the-wire”
Digital Signatures
CRC
Symmetric and Asymmetric Encryption (AES, DES)
Security Management
Security Testing, Monitoring, Change Control, and Updating
Security Risk Assessment of Assets
Security Compliance Reporting
During-Attack Coping and Post-Attack Recovery
Security Policy Exchange
Security Incident and Vulnerability Reporting
Security Attack Litigation
Utilities
Corporate Security Policy and Management

Figure 2: Security Solutions: Technologies and Policies

AMI systems have unique constraints that impact which security solutions (technologies and policies) can be used. These constraints are discussed below.

A. Smart Meter Security Constraints

Smart meters are considered to be so “intelligent” that any type of computer software and automation could be included “under the glass”. However, they do have a number of constraints, including:

- Smart meters still need to be very cost effective because millions will be purchased. They have many requirements essentially unrelated to security, such as storing meter readings for extended times even on loss of power, interfacing to many different AMI network technologies, possibly interfacing to customer gateways (within or external to the smart meter itself), providing self diagnostics, etc. Adding additional storage for audit logs, or adding compute power for encryption/decryption, can increase the cost of the meter.
- Smart meters must be certified as “revenue grade” accurate. Therefore any changes and upgrades, say to enhance security or plug security holes, cannot be easily undertaken.
- Smart meters will be located in very insecure locations since they can easily be reached by the public. Therefore physical security or “walls” around the meter are impractical.

B. Customer Gateway Security Constraints

Customer gateways can also be considered to be so “intelligent” that any type of computer software and automation could be included. However, some of the same constraints apply as for the smart meters, as well as some additional constraints:

- Given the immaturity of customer gateways, they may not (yet) be as cost sensitive as smart meters, but they still need to perform many functions that are not directly related to security. Although they ought to be designed with security in mind, often they are not, so security technologies have to be added afterwards.
- Customer gateways are usually owned by the customers and developed by different types of vendors, rather than specified and owned by the utility as smart meters usually are. Therefore, security technologies that cut across the AMI system will be harder to agree to or interface with, since negotiations across industries could be needed.
- Customer gateways will also be located in very insecure environments, so that both physical and cyber access could be very easily accomplished.

C. AMI Network Security Constraints

AMI networks will inherently have security constraints, including:

- Some sections of the AMI network will most likely be low bandwidth (such as Zigbee or WiFi or power line carrier), while other sections could possibly be high bandwidth but with high traffic expectations. Throughput will therefore be a limiting factor in security solutions. For instance, sending large certificates to all meters frequently would not be feasible for many AMI network configurations.
- Some AMI networks will use public telecommunications services, such as cellular networks. These will limit what types of security can be transported across these public systems.

D. AMI Headend Security Constraints

The AMI headend will most likely reside in a relatively secure area, so physical damage may be less of a concern. However, it still has many other security constraints, including:

- Many other systems will need to access the AMI headend data, so these systems will need to have coordinated security policies and technologies. While some AMI headends may be owned by the same entity that owns and manages these other systems, that may not always be the case.
- Tremendous amounts of data will pass through the AMI headend, often with very different security requirements (e.g. the sensitive metered data versus the ambient air temperature at the customer’s site). No one security solution can handle all these different requirements.

IV. Conclusion

AMI Systems are still very new, with their functionality still being worked out and with many different functional requirements and technological solutions being tested. Security must be built in from the beginning to be truly effective, but often it is the lowest consideration as all of the other competing demands are being pursued.

The UCA Users Group, AMI-SEC, is attempting to address many of these security issues for AMI systems. This effort is being undertaken in a very intensive manner, but the challenges are still enormous given the diversity and novelty of the entire AMI system concept.

V. Biography

Frances Cleveland is an IEEE Senior Member, the Chairperson of the IEEE PES Power System Communications Committee (PSCC), the Chairperson of the IEEE PSCC Wireless WG, and the Chairperson of the IEEE PSCC Security Subcommittee. Ms. Cleveland is President & Principal Consultant for Xanthus Consulting International, and has managed and consulted on information and control system projects for electric power utilities for over 30 years, covering SCADA systems, distribution automation, substation automation, distributed energy resources, automated metering infrastructure, and energy market operations. She was a major contributor to EPRI's IntelliGrid Architecture, is the Convenor of IEC TC57 WG15 on cyber security standards, the Editor of the IEC 61850-7-420 data modeling standards for DER.