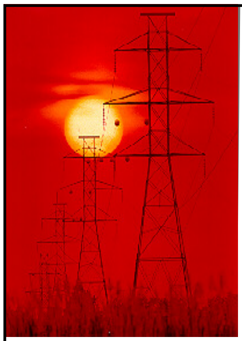


Security Issues for AMI

Frances Cleveland

Xanthus
Consulting International

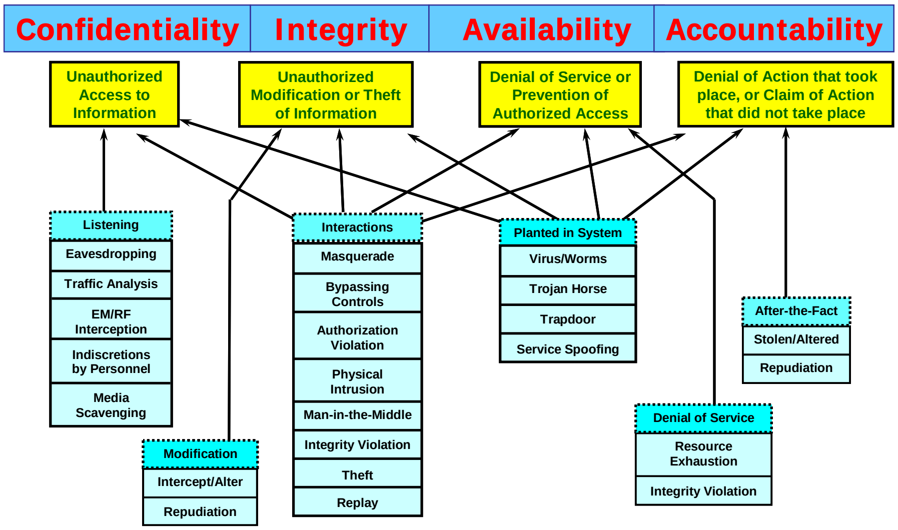
Issue of Cyber Security for AMI Systems

- **Advanced Metering Infrastructure (AMI)** is becoming of increasing interest to many stakeholders
- AMI 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*."
  - But encryption does not ensure security!
  - 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 …?**

Components of Security

- **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 within the time frame that 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.

Security Requirements, and the Intertwined Threats that Undermine Them



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

Listening: Eavesdropping; Traffic Analysis; EM/RF Interception; Indiscretions by Personnel; Media Scavenging

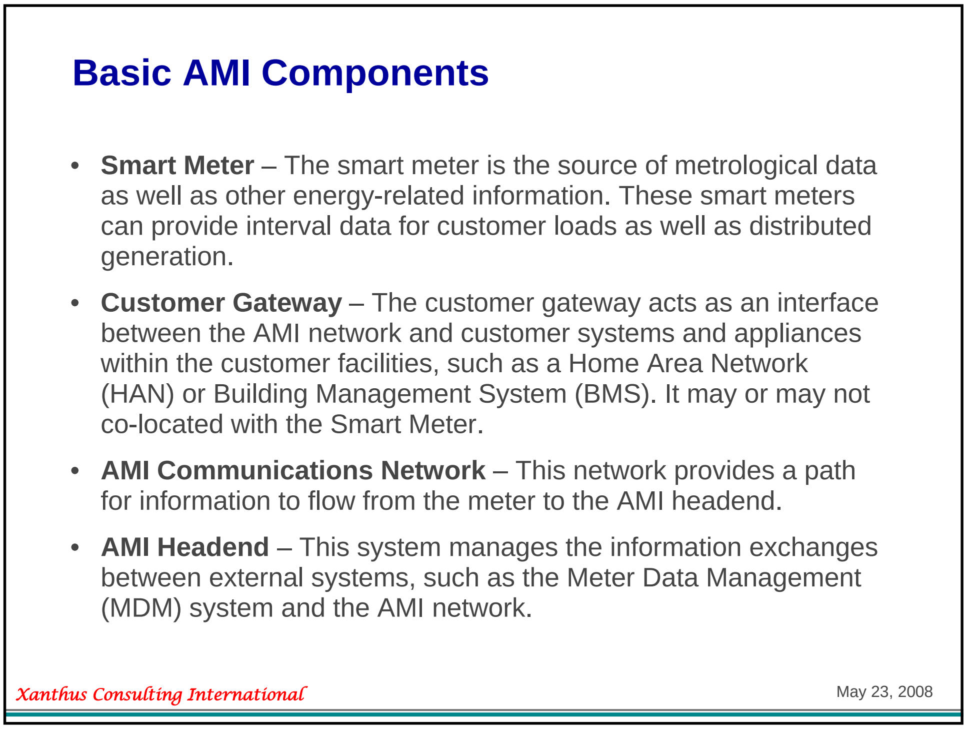
Modification: Intercept/Alter; Repudiation

Interactions: Masquerade; Bypassing Controls; Authorization Violation; Physical Intrusion; Man-in-the-Middle; Integrity Violation; Theft; Replay

Planted in System: Virus/Worms; Trojan Horse; Trapdoor; Service Spoofing

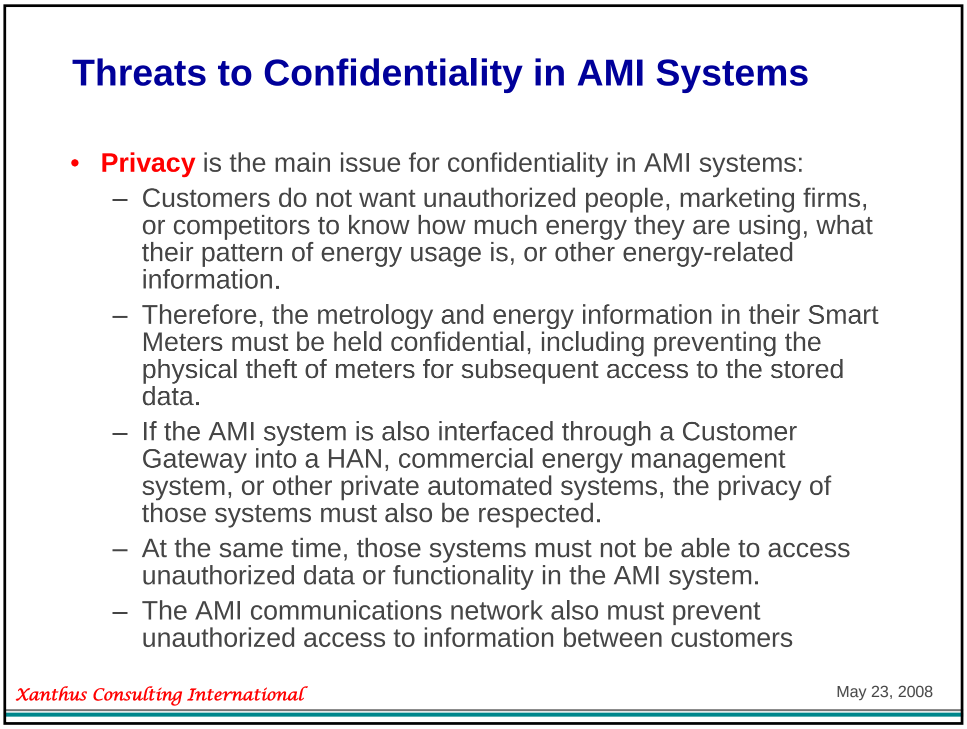
After-the-Fact: Stolen/Altered; Repudiation

Denial of Service: Resource Exhaustion; Integrity Violation



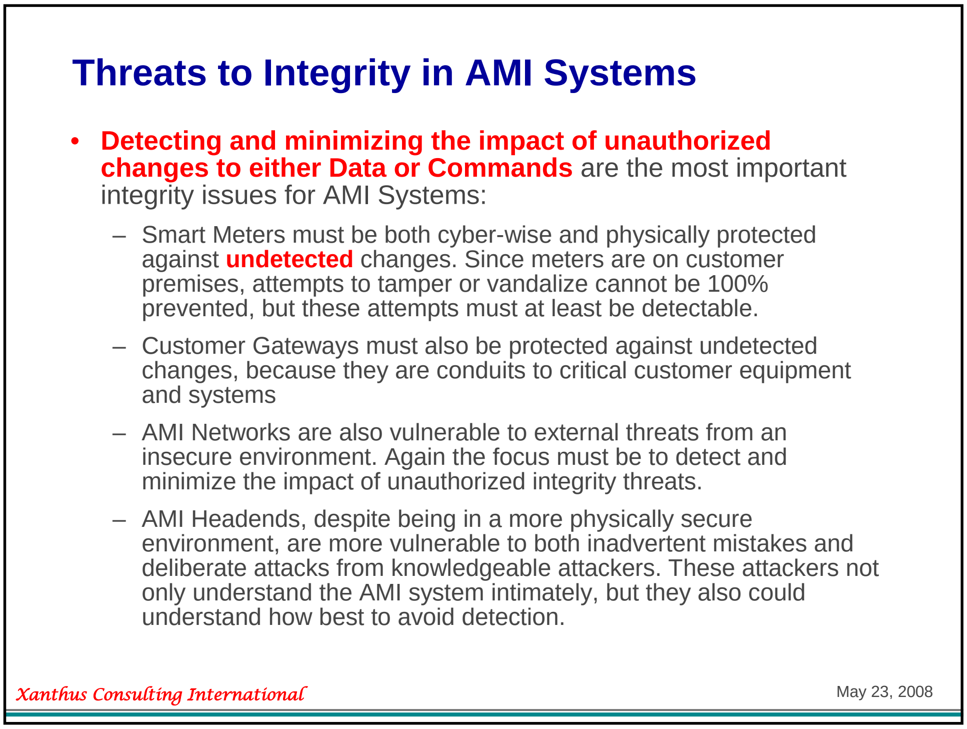
Basic AMI Components

- **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.



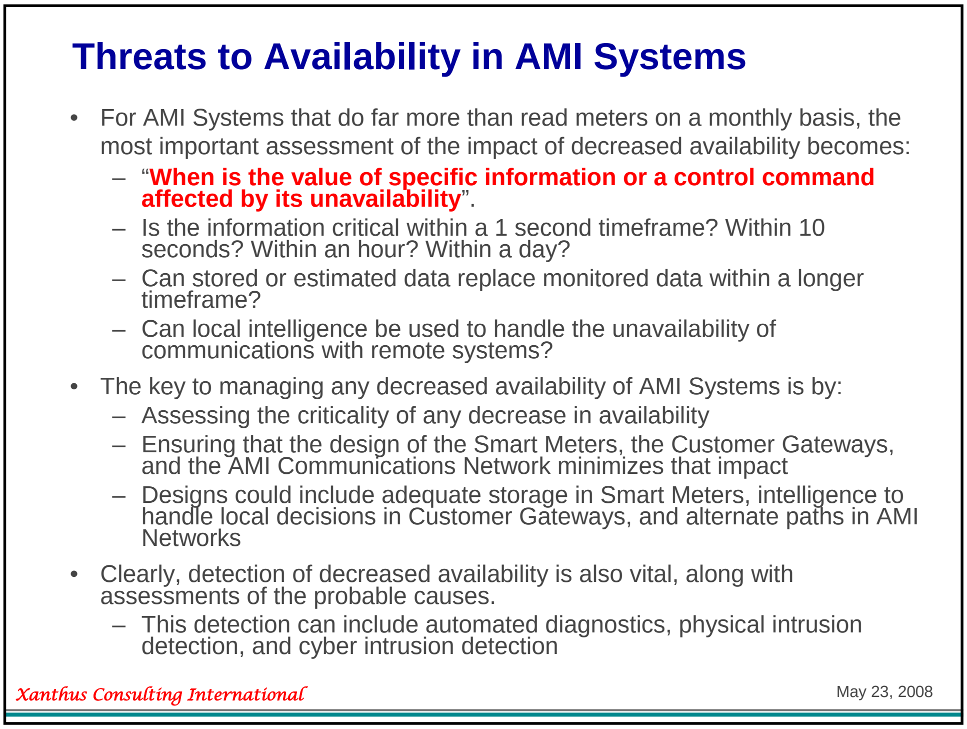
Threats to Confidentiality in AMI Systems

- **Privacy** is the main issue for confidentiality in AMI systems:
  - Customers do not want unauthorized people, marketing firms, or competitors 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 through 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.
  - The AMI communications network also must prevent unauthorized access to information between customers



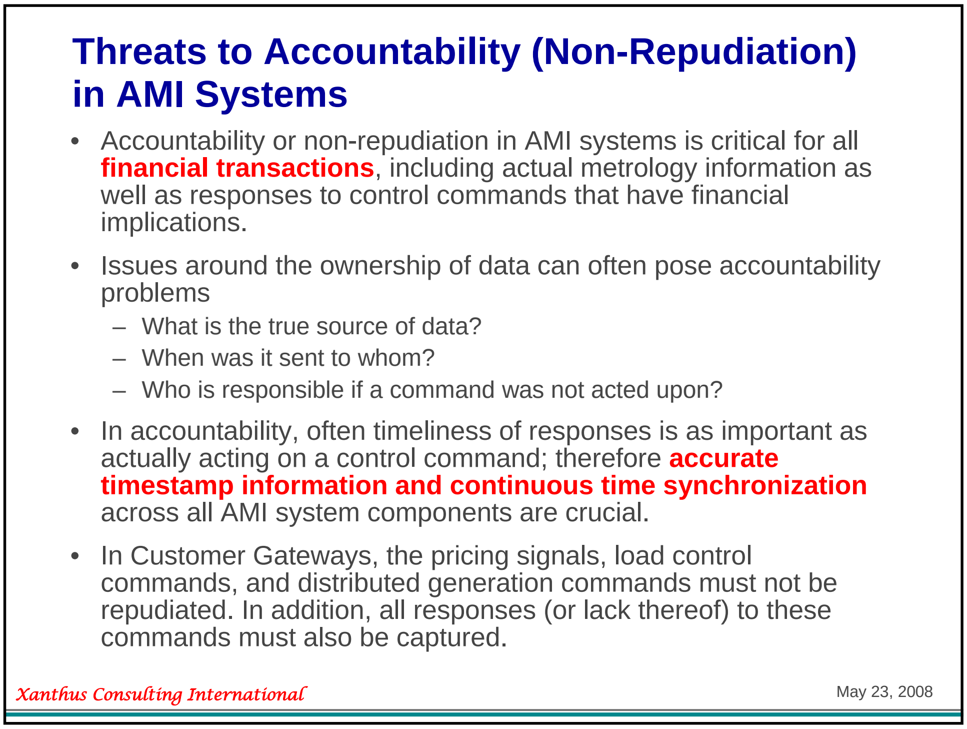
Threats to Integrity in AMI Systems

- **Detecting and minimizing the impact of unauthorized changes to either Data or Commands** are the most important integrity issues for AMI Systems:
  – Smart Meters must be both cyber-wise and physically protected against **undetected** changes. Since meters are on customer premises, attempts to tamper or vandalize cannot be 100% prevented, but these attempts must at least be detectable.
  – Customer Gateways must also be protected against undetected changes, because they are conduits to critical customer equipment and systems
  – AMI Networks are also vulnerable to external threats from an insecure environment. Again the focus must be to detect and minimize the impact of unauthorized integrity threats.
  – AMI Headends, despite being in a more physically secure environment, are more vulnerable to both inadvertent mistakes and deliberate attacks from knowledgeable attackers. These attackers not only understand the AMI system intimately, but they also could understand how best to avoid detection.



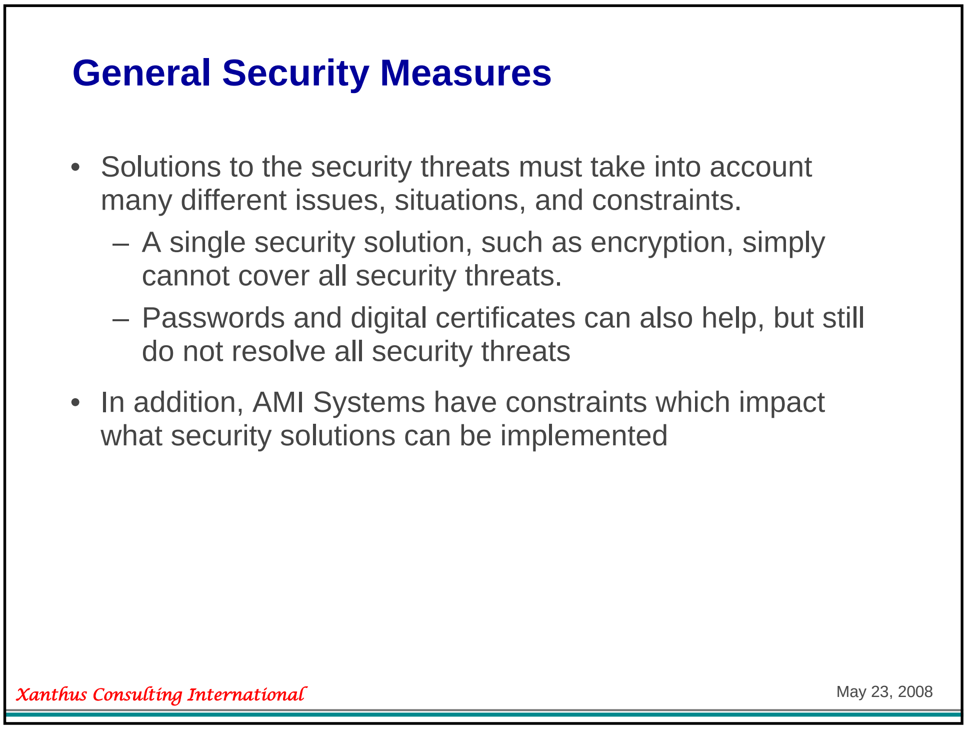
Threats to Availability in AMI Systems

- For AMI Systems that do far more than read meters on a monthly basis, the most important assessment of the impact of decreased availability becomes:
  – "**When is the value of specific information or a control command 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?
- The key to managing any decreased availability of AMI Systems is by:
  – Assessing the criticality of any decrease in availability
  – Ensuring that the design of the Smart Meters, the Customer Gateways, and the AMI Communications Network minimizes that impact
  – Designs could include adequate storage in Smart Meters, intelligence to handle local decisions in Customer Gateways, and alternate paths in AMI Networks
- Clearly, detection of decreased availability is also vital, along with assessments of the probable causes.
  – This detection can include automated diagnostics, physical intrusion detection, and cyber intrusion detection



Threats to Accountability (Non-Repudiation) in AMI Systems

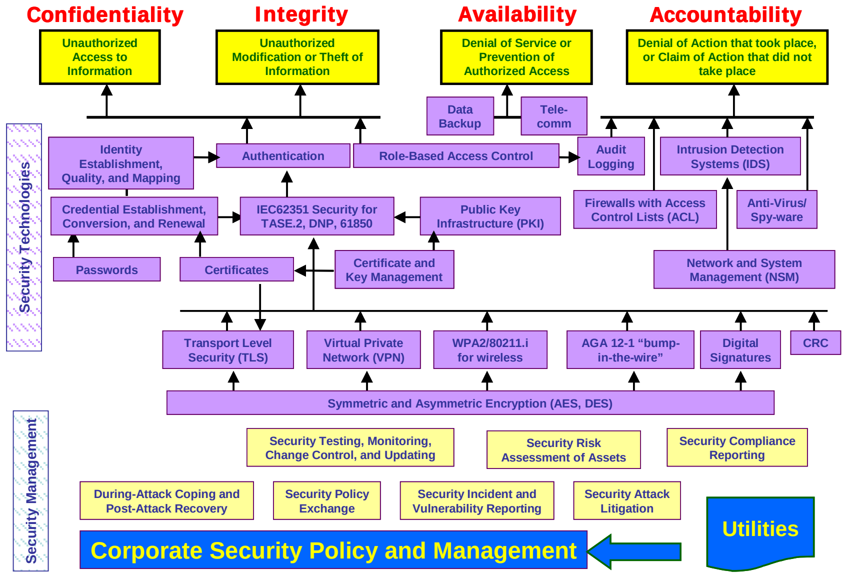
- Accountability or non-repudiation in AMI systems is critical for all **financial transactions**, including actual metrology information as well as responses to control commands that have financial implications.
- Issues around the ownership of data can often pose accountability problems
  - What is the true source of data?
  - When was it sent to whom?
  - Who is responsible if a command was not acted upon?
- 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.
- In Customer Gateways, the pricing signals, load control commands, and distributed generation commands must not be repudiated. In addition, all responses (or lack thereof) to these commands must also be captured.



General Security Measures

- Solutions to the security threats must take into account many different issues, situations, and constraints.
  - A single security solution, such as encryption, simply cannot cover all security threats.
  - Passwords and digital certificates can also help, but still do not resolve all security threats
- In addition, AMI Systems have constraints which impact what security solutions can be implemented

Solutions for Security Threats and Vulnerabilities



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

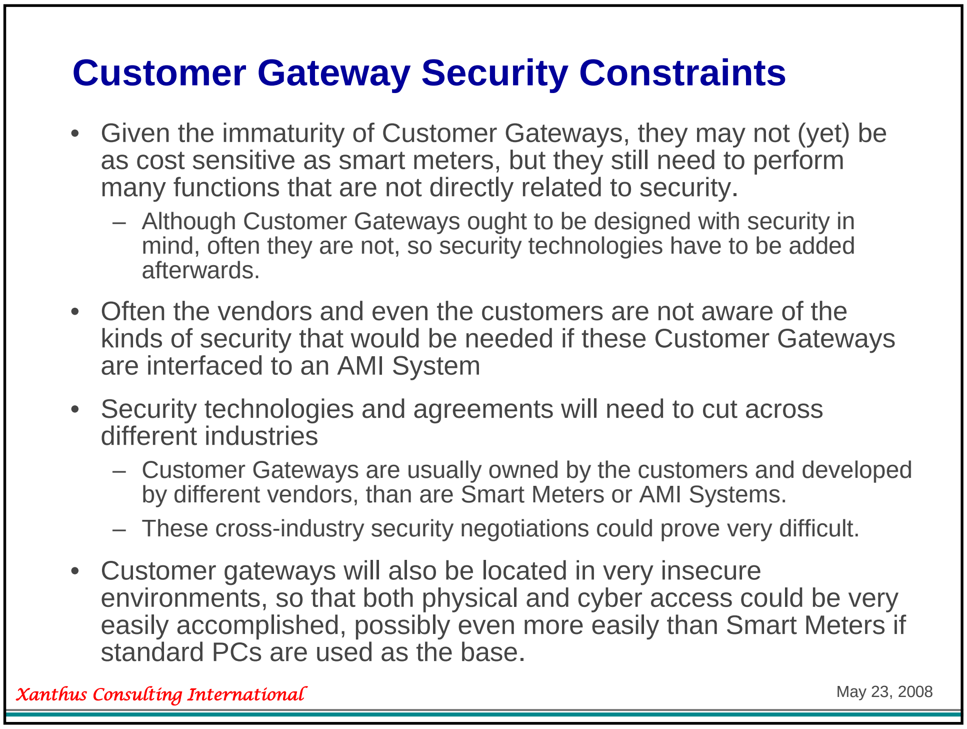
Security Attack Litigation

Utilities

Corporate Security Policy and Management

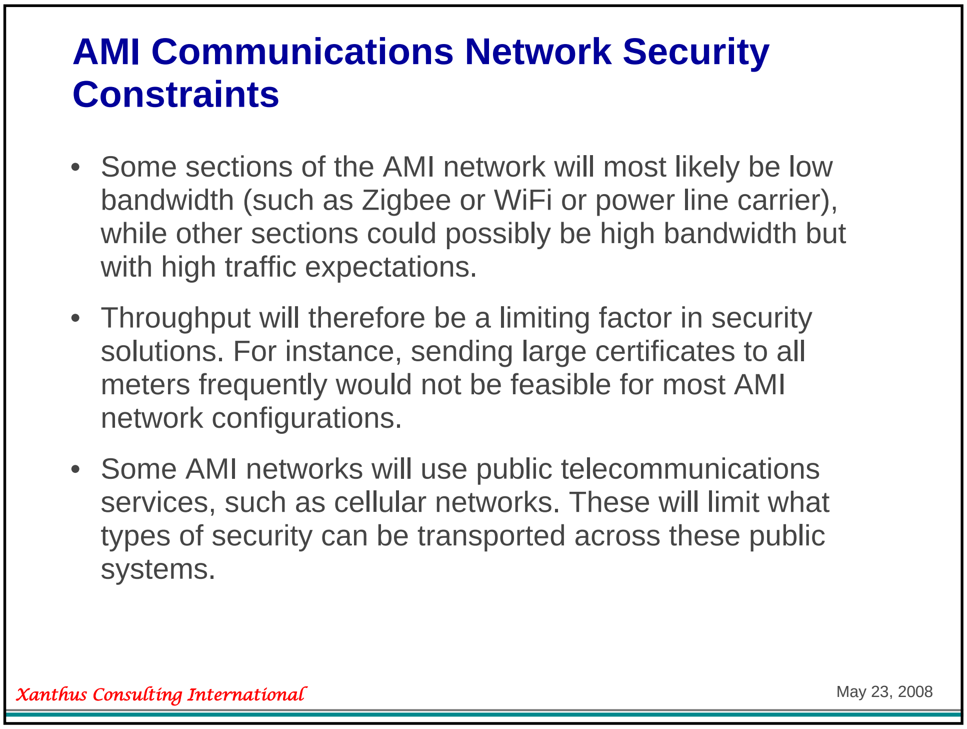
Smart Meter Security Constraints

- 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 on-going 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.



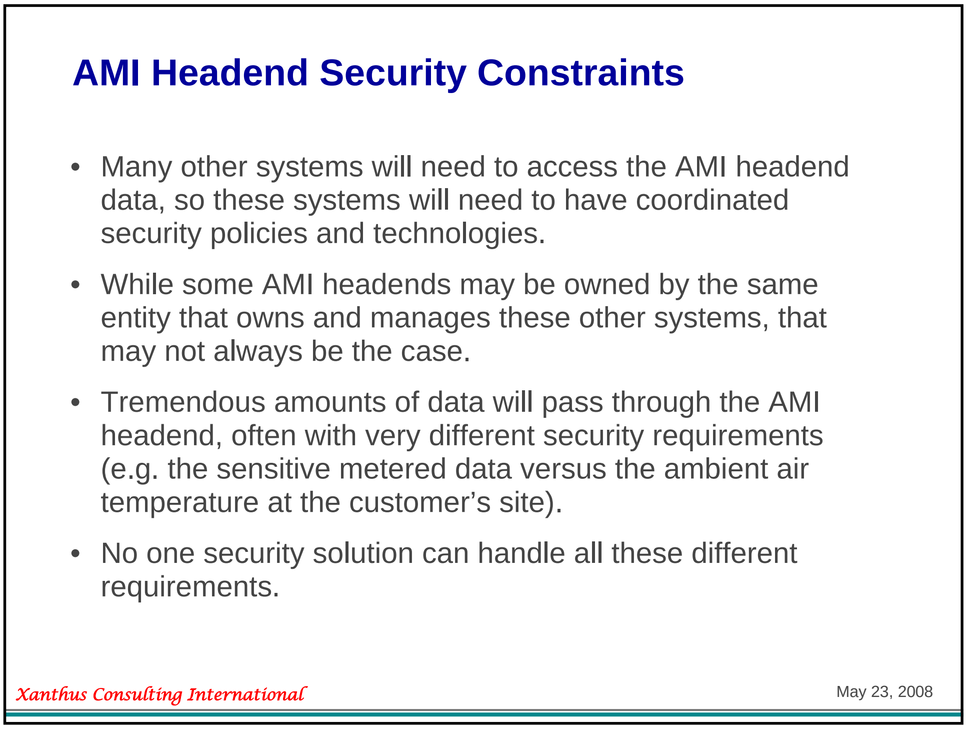
Customer Gateway Security Constraints

- 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 Customer Gateways ought to be designed with security in mind, often they are not, so security technologies have to be added afterwards.
- Often the vendors and even the customers are not aware of the kinds of security that would be needed if these Customer Gateways are interfaced to an AMI System
- Security technologies and agreements will need to cut across different industries
  - Customer Gateways are usually owned by the customers and developed by different vendors, than are Smart Meters or AMI Systems.
  - These cross-industry security negotiations could prove very difficult.
- Customer gateways will also be located in very insecure environments, so that both physical and cyber access could be very easily accomplished, possibly even more easily than Smart Meters if standard PCs are used as the base.



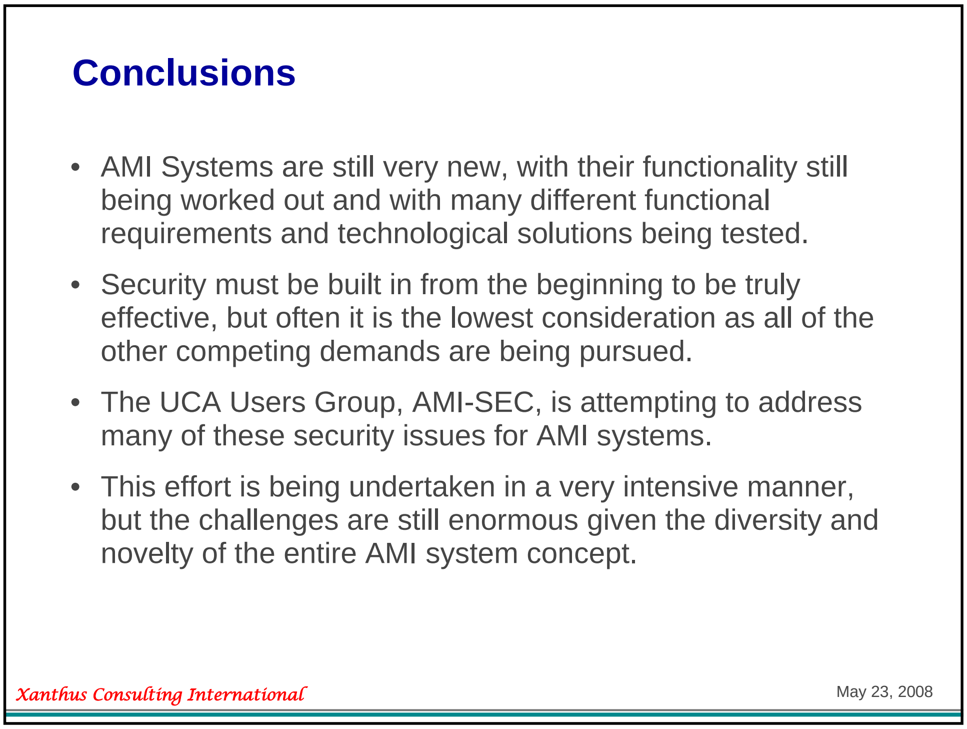
AMI Communications Network Security Constraints

- 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 most 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.



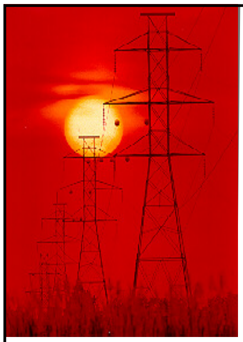
AMI Headend Security Constraints

- 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.



Conclusions

- 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.



So … How can we develop Smart AMI Systems as part of Smart Grid, which will allow us to realize the full potential of these AMI Systems without compromising our security requirements?

Ideas? Comments? Wait until Next Year?

Xanthus
Consulting International