AMI Security Profile

Version 0.02

4/16/2009

This document describes overall AMI security principles, a description of generic components used to provide AMI security mechanisms and AMI requirements mapping to AMI use cases.

Contents

Acknowledgements

UtiliSec Working Group (WG) and AMI-SEC Task Force (TF) would like to acknowledge the work of the primary authors, contributing authors, editors, reviewers, and supporting organizations. Specifically, we would like to thank:

- ASAP-SG (Advanced Security Acceleration Project – Smart Grid)
    - The Security Team including resources from Consumers Energy, EnerNex Corporation, InGuardians, Software Engineering Institute at Carnegie Mellon University, and Southern California Edison
    - Supporting organizations including The United States Department of Energy
    - Participating utilities, including…
- The utilities, vendors, consultants, national laboratories, higher education institutions, governmental entities, and other organizations that have actively contributed to and participated in the activities of the UtiliSEC WG and AMI-SEC Task Force

The UtiliSec WG and AMI-SEC TF would also like to thank the Department of Homeland Security (DHS) Cyber Security Division, National Institute of Standards and Technology (NIST) Computer Security Division, North American Reliability Corporation (NERC) and The Common Criteria for the works that they have produced that served as reference material for the AMI Systems Security Requirements document.

Authors

Bobby Brown

AMI Security Principles

The following are security principles to be applied to developing security policies and requirements for AMI deployments.

Build and Maintain a Defense-in-Depth Network

A layered approach to defending the AMI network must be taken. Defense-in-depth is a mindset that while building and maintaining the AMI network security will be woven throughout several layers from the physical hardware to the software applications that run on them.

- Network tamper must be detectable and reportable; and response capability to network tamper must exist, for example:
    - Intrusion detection/prevention systems at each ingress/egress point between zones of trust (security domain)

    - Removal of casing of meters, routers, access points, etc.
    - Injection of data
    - Replay of data
- The ingress/egress point between each zone of trust (security domain) must be firewalled, for example:
    - Customer Premise
    - Aggregation Point
    - Communications backhaul
    - Utility entry point
    - Corporate Network
- Access to AMI components must be monitored and reported, for example:
    - Log entries include date, time, user id and commands executed
    -

Protect Customer Data

The AMI network has the capability of sending and receiving information that is unique to each customer.

- Customer data must be kept private on the AMI network.

Guarantee Integrity of Information, Control and Management Data

Systems Control and Data Acquisition (SCADA) systems are converging with information networks as they leave the premise of the utility. Control information, metrology information, network management and customer information are destined to share the same physical pathways. The ability to manipulate any of these data sets provides an attack vector against the AMI system.

- Integrity of control data must be maintained
- Integrity of metrology data must be maintained
- Integrity of network management data must be maintained
- Integrity of customer data must be maintained

Validation and constraints of input data must be inspected at the individual level, in addition to the group (batch) level. In a distributed system, data may be handled in aggregate. Where these conditions exist validation and constraint of information must also be present. For instance, it may be perfectly

allowable to conduct a service disconnect remotely for ten (10) homes, but validation and constraints should restrict that capability, for example, for 10,000 homes.

Protect AMI against All Hazards

An *all hazards* approach to securing AMI must be taken in order to establish a resilient AMI system. All hazards include range from cyber terrorism to man-made hazards to natural disasters. This definition does not include remotely probable events, such as a meteor striking a pole top AMI device, but includes those things that we find common and understood. For example, for field components:

- Must meet environmental standards for their given environment
    - Humidity
    - Temperature
    - UV exposure
- Must have appropriate deterrence mechanisms
    - Maximum proximity from potential vandals, animals, etc.
    - Signs and placards (including sign-on warnings of unauthorized users)
    - Alarms
        - Flashing lights
        - Alarms/Buzzers
        - Electronic message to administrator
- Must have appropriate prevention mechanisms
    - Appropriate enclosure
        - 4 walls
        - 6 walls

Detection

When protection mechanisms have failed, the AMI system should have the capability to detect the compromise and report on them.

Develop a Recovery Strategy

The AMI system is subject to many threats. A strategy for recovering from these various threats is needed in order to maintain sustainability AMI operations and a resilient smart grid.

- A disaster recovery plan must be established for “all hazards”
- A forensics capability must be established
- Incident response capability must be established

Maintain an Information Security Policy

The Information Security Policy provides the leadership for handling the organizations day-to-day operations in a secure fashion. The policy also defines roles and responsibilities of employees within the context of security.

AMI Networking Components and Functions

The AMI networking components are defined here in order to understand how they are used in the security architecture for AMI and where they may be found within the system.

Component	Description	Location	Security Function
Wireless Transceivers		Communication Services (Field)	Secure wireless communications
Virtual Private Networks (VPN)	Provides private link/circuit between nodes.	Established between AMI components	Provides data privacy and logical network separation between nodes
Switches [SW]			Support VLAN functionality
Routers [RTR]			Provide separation of networks
Firewalls [FW]	Prevent unauthorized access between networks; Permit, deny, encrypt, decrypt, or proxy traffic between security domains	Between security domains	Prevent unauthorized access between networks; Permit, deny, encrypt, decrypt, or proxy traffic between security domains
Intrusion Detection Systems (IDS)/ Intrusion Prevention Systems	Detect and report anomalies and tampering	Between security domains	Detect and report anomalies and tampering; Potentially respond to known

(IPS) [IDS]/[IPS]			attack vectors
Authentication, Authorization and Accounting (AAA) Systems [AAA]	Perform authentication, authorization and accounting (logging) for AMI network operators	Managed Network Services	Perform authentication, authorization and accounting (logging) for AMI network operators
Embedded Systems		Customer/Utility Edge and Communications	Secure information in temporary storage and transit
Network Management Software/Systems		Managed Network Services	

Table 1 - Security Components and Functions

AMI Requirements Mapping

The following diagram shows the mapping between security domains, AMI use cases and requirements needed.

	AMI SECURITY DOMAIN (SERVICES)					
AMI USE CASE	**Utility Enterprise**	**Managed Network**	**Automated Network**	**Communications**	**Utility Edge**	**Premise Edge**
Remote Meter Read	RMR-UE	RMR-MN	RMR-AN	RMR-COM	RMR-UE	RMR-PE
Remote Connect/ Disconnect						
Tamper Detection						
Demand Response						
…						

Table 2 - AMI Use Case to AMI Security Domain

SECURITY DOMAIN DEFINITIONS	
Security Domain	**Description**
Utility Edge Services	All field services applications including monitoring, measurement and control controlled by the Utility
Premise Edge Services	All field services applications including monitoring, measurement and control controlled by the Customer (Customer has control to delegate to third party)
Communications Services	are applications that relay, route, and field aggregation, field communication aggregation, field communication management information
Management Network Services	attended support services for automated and communication services (includes device management)
Automated Network Services	unattended collection, transmission of data and performs the necessary translation, transformation, response, and data staging
Business Services	core business applications (includes asset management)

Table 3 - Description of Security Domains

	AMI Physical Domain							
AMI Use Case	**Smart Goods**	**Home Area Network (HAN)**	**Meter**	**Field Area Network (FAN)**	**Aggregation Point**	**Backhaul (WAN)**	**Head End**	**Meter Data System**
Remote Meter Read								
Remote Disconnect/								

Disconnect								

Table 4 - AMI Use Case to AMI Physical Domain

AMI Specified Requirements

The following requirements should be attached to the actual process specified for the use case in order that the assurance can be realized.

The most restrictive policy should hold true on security resources (devices) that maintain multiple AMI applications (and potentially Smart Grid applications).

Remote Meter Read

The auto-capture of customer energy and demand data is expressed for this use case. Major processes supported for this use case include remotely reading meters, validating meter reads and generating customer billing. Primary security concerns that envelop these processes are maintaining privacy of customer data, integrity of metrology data and accessibility (availability) to the meter to retrieve the data.

RMR-BS - Remote Meter Read / Business Services

1. An alias shall be provided for the real identity of the customer. (FCP.3)

   Validation: The customer's system identity is not related to their real identity.

2. The meter data management system (MDMS) shall employ a mechanism to authenticate specific devices before establishing a connection. (FAT.2)

   Validation: The MDMS does not allow connections that are not authenticated.

RMR-MN – Remote Meter Read / Management Network Services

1. An alias shall be provided for the real identity of the network operator. (FCP.3)

   Validation: The network operators real identity is not related to their real identity.

RMR-AN – Remote Meter Read / Automated Network Services

1. The field device shall enforce maximum quotas of the following resources connections that meters can use simultaneously. (FAV.5)

Validation: Meters do not allow simultaneous connections that exceed the capacity of the field device, thus causing disruption to service.

RMR-COM – Remote Meter Read / Communications

1. The communications services shall prevent unauthorized and unintended information transfer via shared system resources. (FCP.11)

   Validation: Firewall filters are in place to drop invalid network traffic (e.g., invalid http requests)

2. The field aggregation device shall provide the capability to detect modification of all security function data during transmission between the meter and field aggregation device. (FIN.2)

   Validation: The meter data (metrology, command, management, etc.) is validated at the field aggregation device (e.g., using cryptographic hash function.).

RMR-UE – Remote Meter Read / Utility Edge Services

1. The meter shall preserve a secure state when the meter's power is lost. (FIN.1)

   Validation: The meter maintains the requirements specified in Appendix A: System State Security Requirements.

RMR-PE – Remote Meter Read / Premise Edge Services

1. The meter shall provide metrology information to the requesting utility edge collection point (head end) without soliciting reference to the customer's real identity. (FCP.9)

   Validation: The meter does not send information that contains the customer's real identity.

System State Security Requirements

State.1	Activities allowed during non-operational state shall be limited to system activities needed to enter initialization. (Excludes interactions w/stakeholders, execution of business functions, etc.)
State.2	Activities allowed during initialization state shall be limited to system activities needed to enter operations. (Excludes interactions w/stakeholders, execution of business functions, etc.)
State.3	Activities allowed during initialization state shall include management functions necessary for element configuration.
State.4	Activities allowed during the initialization state shall include policy establishment (i.e., creation and configuration).
State.5	Activities allowed during the initialization state shall include security domain establishment.
State.6	A system shall transition into the operational state only upon completion of the critical initialization activities.
State.7	An operational system shall perform only those activities conformant to policy.
State.8	A system shall be capable of operating in a degraded mode while in an operational state. In this mode, “degraded” refers to a system that has non-operational or impaired components/elements. While services may be denied to some components/elements in the degraded mode, critical functions and security features of the system are still in force for the remaining components/elements.
State.9	A system shall transition into the non-operational state upon detection of a critical failure.
State.10	Supporting activities pertaining to the health of the system (e.g., diagnostics, maintenance, training, etc.) shall only be allowed during the operational state. Support activities may be performed in other system states, however they will be performed by systems external to the SUD.

Service Oriented Architecture

Identification, Authentication and Authorization

Individual Service Level

Pros:

Limits access to services to create a clean audit path within service invocations

Cons:

Significant amount of Code cluttering

Authentication mechanism and storage hard wired (reengineering required to change)

Using the SOA Infrastructure

E.g., J2EE uses JAAS (Java Authentication & Authorization Service) API

Pros:

Makes monitoring the environment easy (against attacks like password guessing, DoS)

Easy Maintenance with small overhead

Cons:

Based on framework used to build SOA – May not work with legacy

Single Sign-On

Pros:

Can work with legacy components

Cons:

…

SOA Firewall

Pros:

...

Cons:

…

Security Description Languages

SAML

SAML (Security Assertion Markup Language) developed by OASIS can be used to include authentication and authorization related statement in addition to signed messages into a SOAP document

SAML has three types of assertions: authentication, attributes, and authorization

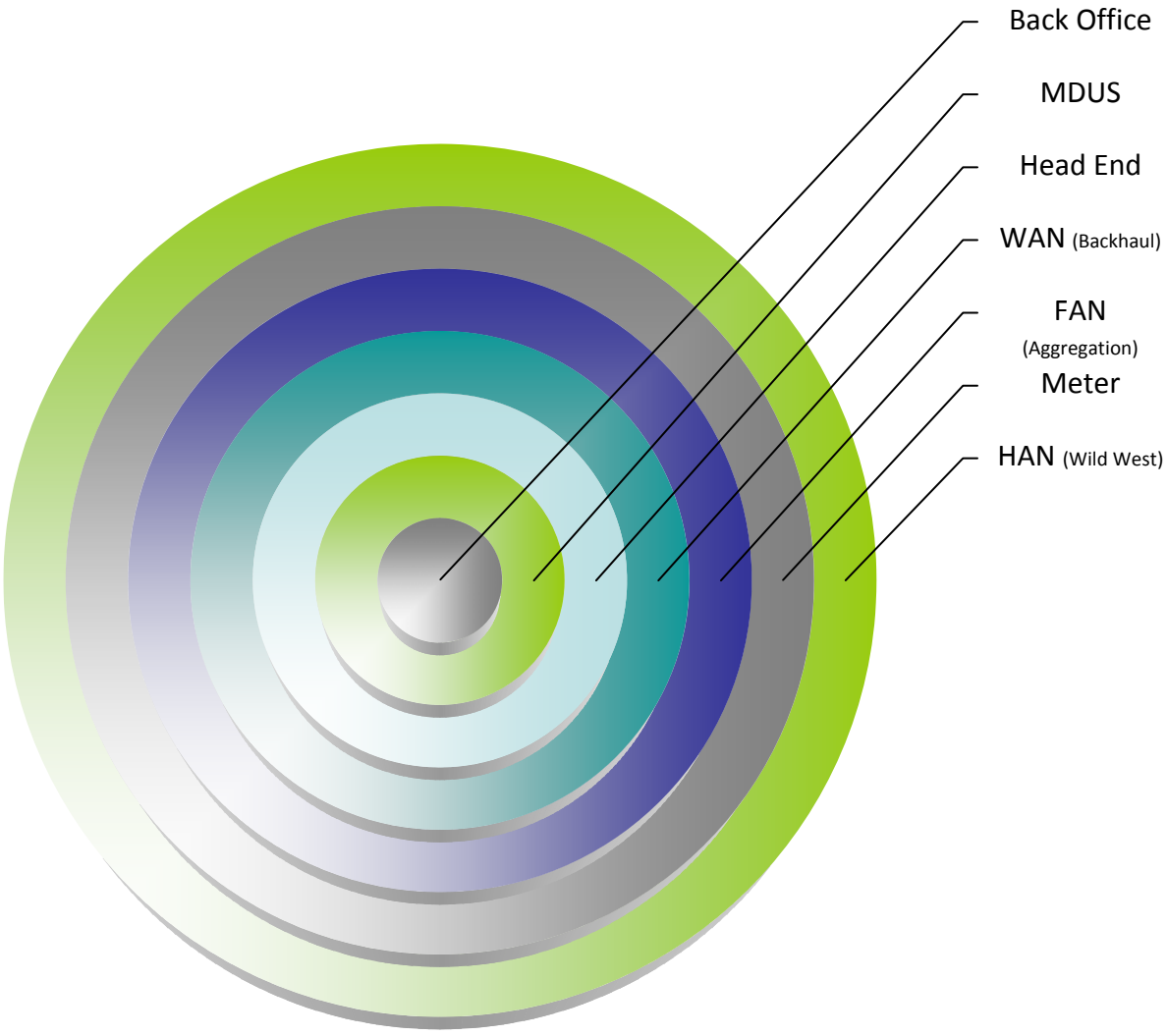
Assertion Provider – provides (optionally signed) assertion that always contains a timestamp, assertion ID, subject of the assertion (typically the user), can contain conditional info (e.g., time assertion remains valid)

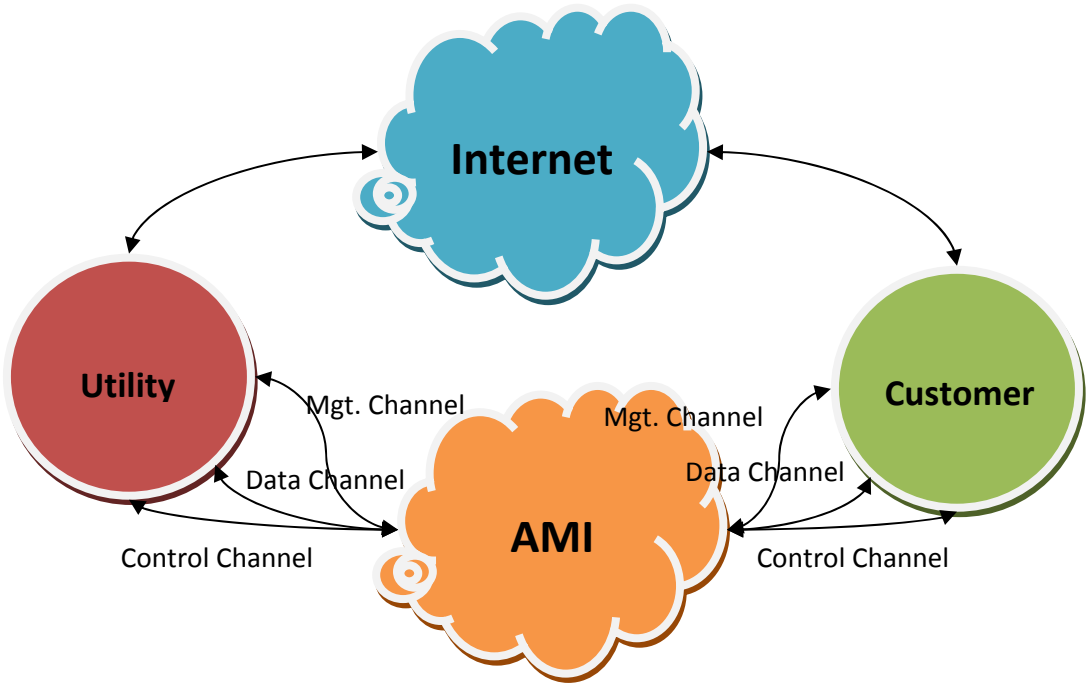
WS-I

WS-I Basic Security Profile developed by Web Services Interoperability Organization

Defense-in-depth

Need defense-in-depth approach. The concentric circles represent divisions of trust and boundary protection.


Back Office
MDUS
Head End
WAN (Backhaul)
FAN
(Aggregation)
Meter
HAN (Wild West)



Why different (logical) channels?

- Separation of duties, i.e., sys admin, operator and customer service
- Application of security mechanisms
- Utility owned vs. third party provider

Security Architecture

Use this tool to provide traceability, completeness, divides tasks/effort.

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual (Business)	Business Functions	Risk Assessment	Utility Process Model (ESB?)	Utility Organization & Relationship	Utility Geography (Golf course)	
Conceptual (Architect)	Architectural Description (Use Cases)	Security Objectives (Controls)	Security Specification	Security Entity Model & Trust Model	Security Domain Model (Periscope)	
Logical (Designer)	Information Model (SOA)	Security Policies	Security Profile	Entity Schema & Privilege Profiles	Security Domain Definition (Bull's-eye)	
Physical (Builder)	Data Model (Control, Management, Information)	Security Requirements	Security Mechanisms	Users, Apps, Services	Reference Network Architecture (Column Diagram)	
Component (Tradesman)	Detailed Data Structure (CIM)	Security Standards (RFQ)	Security Products & Tools	Identity Mgt. (People & Devices), RBAC, MAC	Processes, Nodes, Addresses, Protocols	
Operational (Manager)	Assurance of Operational Continuity	Operational Risk Management	Security Service Mgt. & Support	App. & User Mgt. Support	Security of Sites, Networks & Platforms	Security Operations Schedule

Recommended Practices

- Intrusion Detection
- Staging area for patches/updates – scan for virus/malware, test, etc.
- Authentication of system-to-system
- Host-based protection - intrusion detection, viral protection
- Physical access needed to (black box) systems; e.g., if see hostile traffic then can shut down device
- Engineer to contain and Isolate (security domains)
- Secure info about network, devices, configuration management, etc. – chain of information/custody maintained
- Wireless AP in field should have encryption and VPN capability
- Trust model with 3rd parties for backhaul
    - Manage by tunneling/encrypting across third party systems
- Testing security devices in specific environment before deployment
    - IDS/IPS (Location, Configuration, etc.)
        - Needs to be trained
    - Firewall/Filtering
    - Single Sign On
    - Multi-factor Authentication
    - AAA (Radius, TACACS)
- Alerting on abnormal activity
    - Messages
    - Who is alerted
    - Filtering of messages

        - Type of alert
        - Frequency of alert
- Testing security integration
    - Role-based Access
    - Service-based Access (SOA Integration)
    - Management capability and scalability
    - Scalability
        - Do required management resources outrun value?
        - Standardized approach/methodologies
            - Sys Op guide
            - Device security functions
            - Device locations
            - Process for scaling system
- Security Implementation/Best Practices Guides
    - Virtualized Environments
    - Core Network Services
        - NTP
        - DHCP
        - Etc.
    - Storage
        - SAN
        - NAS
    - Third Party Backhaul
        - AT&T
        - Sprint

        - Verizon
        - Etc., etc.
    - VLAN Management
- Incident Handling Procedures
    - Notification
    - Reporting
    - Reaction steps
        - E.g., pull power on device
    - Recovery