AMI-SEC Team Conference

Thursday, January 08, 2009
Daren Highfill, Chair

Attendees:

Aditi Dubey/Silver Spring Networks
Arshad Noor/ StrongAuth, Inc.
Bobby Brown/EnerNex
Brad Singletary/EnerNex
Darren Highfill/EnerNex
David Chambers/CEC
David Pejcha/Silver Spring Networks
Dennis Gray/APS
Dien Ly/APS
Doug Houseman/ Capgemini
Eric Robinson/Itron
Galen Rasche/Southwest Research Institute
Gary Finco/INL
Gary Ragsdale/ Southwest Research Institute
George Flammer/Silver Spring Networks
Glenn Pritchard/PECO
Greg Robinson/Xtensible Solutions
James Pace/Silver Spring Networks
Jeremy McDonald/SCE
John Lilley/SDG&E
John Mani/Comverge
Julie Brown/Entergy
Junaid Hossain/Florida Power & Light
Mark Bonfigilio/Entergy
Mark Freund/PG&E
Mark van den Broek/ Lockheed Martin
Matt Gillmore/ Consumers Energy
Michael Echols/SAIC
Neil Greenfield/AEP
Phil Slack/Florida Power & Light
Radha Swaminathan/ Florida Power & Light
Richard Tolway/APS
Sharon Li/PG&E
Viola Lee/PG&E
Zahra Makoui/PG&E

Summary

The AMI-SEC meeting was hosted by EPRI in Palo Alto, CA. The team discussed the following: Organization and Objectives of AMI-SEC & UtiliSec, AMI-SEC Roadmap, System Security Requirements, Component Catalog, Implementation Guide, Press Release, AMI Attack Methodology, National SCADA Test Bed from Idaho National Lab and 2009 Planning.

Documents

The associated documents can be found on the AMI-SEC SharePoint site:

- AMI-SEC January 2009 Face-to-Face presentation slides
- AMI-SEC Attack Methodology presentation document (Matthew Carpenter)
- National SCADA test bed presentation from Idaho National Laboratory (Gary Finco)

Technical Discussion

Organization and Objectives

Chair is speaking from the presentation slides:

- Open Smart Grid (OpenSG) is a subcommittee within the Technical Oversight Committee of the UCAIug.
- UtilityAMI Work Group (WG) was formed by the OpenSG Subcommittee of the UCAIug (UCA International User's Group) in order to resolve questions surrounding Advanced Metering Infrastructure (AMI).
- There are two active task forces under UtilityAMI WG:
    - OpenHAN - for home area network issues; the oldest task force.
    - AMI-Enterprise – started summer of 2008.
    - AMI-Network – inaugural meeting at October, 2008 F2F in Knoxville.
- The UtiliSec WG is the most recently formed organization of 2009 in order to address security issues for the OpenSG Subcommittee.
    - The AMI-SEC TF moved from under the UtilityAMI WG to the UtiliSec WG. AMI-SEC TF formed in late 2007.
- A Utility in good standing with UCA has voting rights within the UtilityAMI WG and UtiliSec WG and their task forces.
- There are no task forces (TF) directly under the OpenSG Subcommittee, only work groups.

Both UtilityAMI WG and UtiliSec WG are aimed at capturing requirements for a system from a utility perspective, as to "what" the utility system needs to do and deterring from the "how" it is done. Neither group is involved with issues of vendor implementation, nor do they tell vendors how to build a product. The UtilityAMI WG and UtiliSec WG are tasked to produce a set of system requirements.

OpenSG has an established Class D liaison with IEC. This allows circulation of IEC draft documents. Prior to this relationship it was required for someone to be an IEC member of the committee to view IEC draft documents. Circulation of IEC non-draft standards within the group is still prohibited.

The task force also has good ties with IEEE.

There is a non-formal relationship with NIST and UtiliSec is tracking their work. NIST is developing a smart grid interoperability framework that was established 4th quarter 2008. It is expected for the

relationship to continue. The taskforces in UCAIug have contributed documentation to the NIST process and there continues to be good exchange among the two groups.

ASAP support was formed after the Risk Assessment document was completed early in 2008. The level of effort that is required for these documents could not be supported strictly by volunteers in addition to their full-time jobs. Therefore in order to meet the schedule for 2008 deliverables, utilities from the AMI-SEC TF formed a collaborative to fund this work. The responsibility of the ASAP was to draft an Architectural Description, AMI System Security Requirements, Component Catalog and Implementation Guide for AMI-SEC. The task force would then go through a process of review, comment and feedback, and vote for each deliverable.

ASAP also had an objective to perform Red Team testing. Actual testing did not take shape due to agreement issues, non-disclosures, and the complexity of putting penetration testing in place. Red Team testing is unstructured and does not follow a formal test plan. The AMI Attack Methodology document is a tool kit that was developed by the team to organize approaches for testing.

SmartGridipedia (www.smartgridipedia.org) is a website developed to serve as an external reference repository, similar to Wikipedia, to post smart grid information under Creative Commons (CC) attribution. Material posted to SmartGridipedia is protected from aggressive intellectual property rights.

2008 Deliverables

- Risk Assessment (needs cleanup and updates to the relevance of the other deliverables; was put out 1st qtr, 2008)
- Architectural description (combined into the AMI System Security Requirements)
- AMI System Security Requirements
- Component Catalog
- Implementation guide

Roadmap

The Roadmap document was developed in 2008 and is a work in progress document. It currently needs updates (refer to action items).

The intent of the Roadmap document is to give to readers enough information to know what UtiliSec/AMI-SEC is, what is being accomplished, and the plan of how the TF is going to provide deliverables. The Roadmap sets the stage for the issues, concerns and technology surrounding the AMI environment. It explains the overall process and how to get involved in UtiliSec activities.

Diagrams in the Roadmap document are based on real implementations. Utilities are asked to review the Roadmap for updates and changes.

When referring to the Roadmap regarding the Architectural Description and the System Security Requirements, they were originally two documents and have now become one document due to similarities that was causing repetition in both documents. Architectural Description is the background information for the requirements. System Security Requirements document actually became more than requirements; therefore the title was given "System Security Requirements and Guidelines". For a UtiliSec certification program, guidelines are good. However, the group does not prefer the title to include "guidelines," in that it dilutes the main purpose of strictly being requirements.

Charter and Purpose Statement

There are some changes made to the Charter and Purpose Statement. "AMI-SEC" has been changed to "UtiliSec" in the document. Section on participation has been removed. Voting on an agreement to change the Charter Statement will be done at the next Face-to-Face meeting.

AMI System Security Requirements (SSR)

Motion made and second to remove "Guidelines" from the title of the AMI SSR. Vote was passed with no opposition. Members commented that from procurement prospective if the document were to be interpreted as guidelines then requirements may or may not be abided by. Members suggested that the term "guidelines" lends itself to the idea of certification.

The modified AMI SSR document will be posted to the AMI-SEC ListServ and on the SharePoint. Login credentials are not needed for access to the documents on the SharePoint site. Please review it and let us know if there's a need for further changes.

The SSR was ratified at version 1.0 as of Dec. 17, 2008. There are a few differences between version 0.93 draft and 1.0, but no changes to the framework. The AMI SSR is also posted on the SmartGridipedia site. The Component Catalog will also be put out on SmartGridipedia located under Security>Smart Grid Security>AMI Security. This wiki will serve as an information sharing and learning tool for utilities, vendors and the general public.

Component Catalog

The Security Component Catalog explains how the components implement security mechanisms to meet security requirements at the logical layer. It discusses the security mechanisms that should enforce policy and requirements. The catalog identifies the structure of how to get components need to be added into the SmartGridipedia. The standard layout is 1) name, 2) definition, 3) domain and 4) requirements they fulfill for AMI-Security. A "references and examples" section has also been added to give practical examples and references to existing bodies of work.

Implementation Guide

The Implementation guide is still in development and will be available when there is a more stable version. The Implementation guide will provide a sanity check to the overall process and validate that steps have not been left out or bypassed. The implementation diagram references between system

requirements and architectural description (refer to slide). Entry points are labeled relative to the "effort and resources" needed by the utility to address the problem space.

ASAP Presentations

AMI Attack Methodology

Presenter: Matthew Carpenter, ASAP Red Team Lead

Presentation slides available on the SharePoint site.

Utilities that participate in ASAP will use this guide for internal testing and to understand what a third party should provide in the way of policies and principles. It is also an effort to assist the utility to do their own system testing and help the vendors prepare. The Attack Methodology is geared towards embedded systems. The plan is to move on to the more traditional systems in the future, however, it is important to address things that are not well known. Security issues with Intel x86, etc. are already well known.

The current analysis target does not specifically address insider threats and those against the head-end. The insider could gain access control to the systems and hack in to the head-end which would cause awful things to happen, but the head-end has a smaller attack surface. The head-end is where the higher cost and impact lies but mature security knowledge and guidance exists for this type of equipment and environment, whereas very little knowledge or guidance is available for securing embedded systems. Getting at the head-end is also more difficult depending upon the application. It is important to do assessments on a regular basis for any system.

It is important to look at the complete system and define in depth what is important in order to develop a mitigation strategy so that utilities can survive some level of compromise. This is why we evaluate not just the meter, but to the meter and the communication system that comes with it. It's important to start thinking about what's downstream from the meter.

This document will be publicly available 6 months – 1 year. Currently, it's only available for ASAP funders and vendors committed to participating in ASAP testing.

NSTB SCADA Test Bed, Idaho National Laboratory Presentation

Presenter: Gary Finco, Idaho National Laboratory

Presentation slides available on the SharePoint site.

The Idaho National Laboratory (INL) was asked to assist with a deliverable on the ASAP project. Gary Finco discusses an overview of Idaho lab:

INL is located in 890 sq. miles of high desert plain. It is a no-fly zone because of weapon testing. The history is in nuclear, with National SCADA (Supervisory Control and Data Acquisition) Test Bed (NSTB) as one of the areas since 2004. It is a cyber security test bed with the only city sized wireless test facility. It is testing 3G/4G wireless communication, wireless LANs and Land Mobile Radio system. The lab has its own power grid test bed, 61 miles of dual loop, seven substations and three commercial feeds.

Vulnerability testing is shared is with vendor partners. DOE is supporting the activities. Vendors don't want the information going out to everyone. Historically, once legalities are set, INL conducted vulnerability testing and gave results that back to vendors as a follow-up to make sure mitigation measures have been put in place. The vendors get the benefit of the assessment. This is the blue print used, to date.

The lab has been asked to do a tabletop analysis; they did an open source. A procurement language guide was developed for SCADA and process control systems. To close the loop, the vulnerability was determined and identified mitigation strategies with the vendors worked with. What was applicable from the procurement guide was put it in a standards guide. It is in review and will be put out on the SharePoint site for external release.

When vulnerability is found that cannot be addressed, workarounds are done. Some of these systems and the software is 20-30 years old (e.g., proprietary protocols); therefore, with wireless, there are issues that nothing can be done.

If vulnerability is found that cannot be addressed, there is a hierarchy for reporting to NERC. There are specified documents used by DOE. The one used when they have funding is PRATA, which allows the lab to share with vendor partners.

Press Release

The Chair discussed the press release for the AMI SSR document. Minor modifications need to be made by the group at this time. Press release is reviewed and read by the Chair for changes. Chair states that it needs to be kept simple. The press release was revised at the end of the day.

Two utilities are not in favor of the press release at this time, one utility is in favor. Concerns are that there are things that are ready to be released in the document but not in its current entirety. There also needs to be credit given to external sources.

Chair requests that after the AMI System Security Requirements are revised that the press release be pre-approved for the wording. The quorum responds with a "yes".

2009 Planning

UtiliSec 2009

Development for AMI will continue and extend to Smart Grid. The vision is to take the set of deliverables developed by the AMI-SEC TF and extract out and abstract up all portions that are relevant to smart grid.

This smart grid foundation elements would become the Smart Grid Security Specification, which would then be paired with a tailored risk assessment and set of requirements to create a Protection Profile for each smart grid application.

One of the approaches with the Vulnerability Assessment is to tie it into the use cases and requirements that protection engineers understand. The vulnerability assessment will be traceable, to understand what the consequences are to the system. Risk management will also be balanced.

This group is the authoritative source regarding what is developed.

AMI-SEC – Tasks to plan for:

- Network management, key management operation security
- Completion of Component catalog and Implementation guide
- Need a one-liner task description with a group of people; then build a timeline around it

There are sources that are derived from sources of policy - NERC, FBI, etc., a number of outside agencies that may be the stakeholders that address security issues with the grid and AMI. There are a number of stakeholders for providing the security system, e.g., Department of Defense with the Pentagon.

Other plans:

Transformation of AMI-SEC deliverables to Smart Grid deliverables -

- Traceability between documents
- Multiple smart grid applications
- Clean-up pass
- Firming up survivability requirements

Action Items

Eric – Lead revision of Risk Assessment document.

Utility Members - Charter and Purpose Statement Revision out for review; vote to be cast at next teleconference.

Bobby – Add announcement on AMI-SEC homepage about AMI SSR and link

Jeremy, John Lilley – Work with ASAP/Darren to resolve open issues with SSR before press release

All - If you are not on the AMI-SEC mailing list, you can find a link to the SharePoint site at the end of the presentation slides: http://osgug.ucaiug.org

All - The Roadmap Document needs review and updates

All – UtiliSec/AMI-SEC needs ideas on how to address vendor products and understand what products are available on the market. There needs to be a mechanism for mapping that context. What repository might be out there, with value added somewhere else. This is a living deliverable. We need your ideas, involvement and feedback.

Upcoming Meetings

Planning for the upcoming Face-to-Face sessions will now be all day sessions. Teleconference meetings will be moved out to a 3 week schedule session, beginning January 29th. The teleconferences will be held on Thursdays at 2-3p.m. EST.

2009 Teleconferences on Thursdays:

- January 29th from 2-3pm EST
- February 19th from 2-3pm EST
- March 12th from 2-3pm EST
- April 2nd from 2-3pm EST

2009 Face-to-Face Meetings:

- April 14th -16th hosted by FPL in Miami, FL
- July 14th-16th hosted by AEP in Columbus, OH
- October 20th-22nd hosted by EnerNex in Knoxville, TN

2010 Face-to-Face Meeting:

- January, hosted by FPL in Miami, FL