

## **AMI-SEC Team Teleconference**

Wednesday, April 30, 2008.

Daren Highfill, Chair

Please find Security AMI Security Architectural Description attached.

### **Summary**

The AMI-SEC meeting was hosted via teleconference and web-conference using GoToMeeting.

### **Documents**

System Security Architectural Description

### **Technical Discussion**

The scope of AMI-SEC is being sent to UtilityAMI working group for approval.

The System Security Requirements (SSR) document has not experienced much traffic since last meeting. Additional material and commentary has been generated for the document, but has yet to be incorporated. Requirements and threats are cleaned up and mapping of threats has been completed. Others are working on functional requirements and cleaning up items to be consolidated.

Comments were made about a traceability-matrix, being careful with version control between documents, and tracking requirements through other documents. The Chair stated that version control is not a real concern right now because of the immaturity of documents at this point, but there will be a need to finalize when a certain level of detail is attained. Statement was made that we will begin use of spreadsheet to track document revisions after the roll up of contributor's notes. At this point if a change is made in a document it would have a ripple effect through other documents; someone would have to walk through each document to adjust accordingly. Comment was made that SharePoint has some versioning capability. The Chair suggested that we use a procedural method for maintaining versioning for now and not use a special application.

Discussion continued with coverage of the System Security Design document. The group adopted that we change the name from System Security Design to System Security Architectural Description to align with the role of the document and IEEE 1471-2000 terminology. The purpose of the document is to represent a logical, platform agnostic architectural description of AMI Security. The document is to tell the story of the architecture at the highest level of abstraction from the points of interface for the system. Three primary interfaces have been identified as Customer, Utility Enterprise and Third Parties.

The team discussed the struggle with resolving sources and corresponding levels of control in the various parts of the system. Between Utility Enterprise and the meter exists a virtual cloud with

numerous variables that can be filled with several types of control. The sources of control have interaction on both ends of the AMI system. This interaction is significant to the requirements of the system. The customer interacts with the system in various ways; e.g. review of automated bill, control of the Programmable Communicating Thermostat (PCT), etc. Third parties may be a regulator trying to assist level of access for the retailer. There exists an entirely separate group of third parties that are service providers to AMI; e.g. contracted areas and the network itself. It was noted that some of these distinctions will aid in explaining the requirements once more detail is achieved.

The Architectural Description (AD) discusses the environment (context) of the system and presents viewpoints and views as described in IEEE 1471-2000. The views are the worker bees of the document. The AD also describes the stakeholders and stakeholder concerns of the system. All users of the system are stakeholders, but not all stakeholders are users.

There was dialogue about taking care not to delve too deep into the functional requirements of the system and losing focus of security. Enough description of the system needs to be conducted in order to describe the security architecture. At this point we may need to place question marks where the system has not been defined and we learn more, since the overall system is still evolving.

The AD is available for all members to contribute. ASAP will continue their efforts to fill in and complete the document.

The question was asked if the AD document would reference demonstrations of systems that have currently been implemented and explain the interfaces for interoperability. The chair noted that the goal at this point is not to define specific interfaces for interoperability – that this non-trivial work may be covered in another task force or slated for next year.

Software Engineering Institute (SEI) recommended that the group focus on picking views at this point and not worry about details. Next, determination of concerns, methods to be used, and viewpoint language (what kind of information to put into the view) should be considered. Recommendation was also made to be selective when choosing views and not to waste time picking too many; that there will be considerable overlap.. Design rationale should also be part of this document that describe why choices were made the way they were, including trade-offs; for example security for performance or security for operability.

## **Upcoming Meetings**

The next teleconference for AMI-SEC is scheduled to be held Wednesday, May 14th from 1-3 PM EDT. An email will be sent containing dial-in number and web-conference information prior to the next meeting.