

SG Security WG – Face-to-Face Meeting

Meeting Minutes

February 2-4, 2010 – San Francisco, CA

Attendees

See spreadsheet (SG_Security-F2F-January_2010-Attendees.pdf) for attendance list.

Summary

The face to face meeting covered several sessions over three days starting after the OpenSG opening plenary. The chair opened the sessions by providing updates covering the SG Security WG Charter, Security Profile Blueprint, AMI Security Profile v2.0, Third Party Data Access Security Profile, and ASAP-SG. Technical sessions covered the comments resolution process for v2.0 of the AMI Security Profile and the introduction of the Lemnos Interoperable Security Project as a potential Task Force or Interest Group within SG Security. Joint work sessions were also held between SG Security and OpenHAN, OpenADE, OpenADR, AMI-ENT, SG Systems, and SG Communications. The meetings concluded with an organization and planning meeting for SG Security prior to the OpenSG closing plenary.

Documents

Documents are hosted on the SG Security SharePoint site under *Meetings* and *20100204 - Face-to-Face (PGE - San Francisco, CA)*. These include:

- SG_Security-F2F-January_2010-public.ppt
- SG_Security-F2F-January_2010-Lemnos.pdf
- SG_Security-F2F-January_2010-Attendees.pdf
- SG_Security-F2F-January_2010-Minutes.pdf

Technical Discussion

SG Security WG Charter - Version 0.9 of the SG Security was posted the week of 1/25/2010 to the SG Security SharePoint for review prior to balloting. A call for vote was made for approval of the SG Security Charter. Motion made by Nick Gerbino/Dominion for approval. Second was made by Ward Pyles/Sothorn Company. There was no discussion and the SG Security Charter was approved by unanimous vote by all present.

Security Profile Blueprint - An overview of the Security Profile Blueprint was presented by James Ivers/SEI. The purpose of the document is to inform the community on ASAP-SG security profile creation process. It is revisited after completion of each profile and refined if needed. Comments and suggestions are welcome by the ASAP-SG team. A question was raised on where to send comments. Darren Highfill asked that comments be directed to him and he will forward to the ASAP-SG team.

Third Party Data Access Security Profile – Darren Highfill/SCE provided an overview of the Third Party Data Access Security Profile including roles as defined in the document. It was noted that this document has not been posted to the SG Security SharePoint yet as it has not been accepted by the SG Security WG. It has been posted to www.smartgridipedia.org.

Lemnos Interoperable Security Project - Brian Smith/EnerNex provided an overview of the Lemnos Interoperable Security Project. The project is funded by DOE and is in its final year. The project partners would like to identify a long term steward for the work after the project is complete. Brian will generate a more detailed information package for the group for further discussion. Those interested were asked to e-mail Brian Smith (brian@enernex.com)

- Action Item: Brian Smith will forward the final list of interested parties to Darren Highfill

ASAP-SG - Darren Highfill provided the WG a background of the ASAP-SG effort. At the end of the overview, there was a call for volunteers for the Third Party Data Access Security Profile usability analysis team. Those interested were asked to e-mail Darren Highfill.

- Comment: There do not seem to be any negative use cases in the Third Party Data Access Security profile.

AMI Security Profile v2.0 - The current schedule is to deliver v2.0 of the AMI Security Profile to NIST by March 1, 2010 however that will more than likely be pushed out. Sandy Bacik/EnerNex, who leads the comment resolution team, provided an initial overview of the discussion points collected by the comment resolution team as follows:

- The use of "must", "shall", and "should" and corresponding definitions of them.
 - Comment: Why spend a lot of time on this when we can use the IEEE definitions of them.
- No collaborative computing capabilities should be used in and AMI system as it is a dedicated system for one function
- AMI is a dedicated system and should not support VoIP capabilities
- Should we add a glossary and acronym section
- Should "Smart Grid Application" be part of the Smart Grid components?
- Should the security profile document be formatted to be used in RFPs?

Sandy Bacik/EnerNex followed up the initial session with a more detailed working session. Details covered in this session included:

- Review of scope and goal of the AMI Security Profile

- Prescriptive and actionable
- Vendor neutral
- Extends from the MDMS to and including the HAN interface of the Smart Meter
- "Must" vs. "Shall" definitions from IEEE
 - Shall = required to
 - Must is not used in the documents
 - Should = is recommended that
 - May = is permitted
 - Can = is able to
 - Requirements will use "shall"
 - Guidance will use "should"
- Requirements Scoping
 - Collaborative computing capabilities
 - Recommendation is not to allow. AMI is a dedicated system for one function
 - After discussion, it was decided to add requirements enhancements including:
 - When using a shared network, AMI shall be provided adequate QOS
 - The entity should perform a risk assessment in using the shared network
 - VoIP Protocol
 - After significant discussion, it was determined to remove this requirement and adding this into the requirement related to collaborative computing.
 - Encryption
 - Use existing standards (i.e. FIPS 140-2) or list our own recommendations?
 - Decided to add within supplemental guidance:
 - Level of protection needs to be applied to the data
 - Malicious Code Protection
 - Much discussion on at what level these need to be written
 - AMI Components
 - Clarify "Grid Control Center"
 - Basic Definitions
 - The instance of "reasonable period of time" will be changed to "system owner's record retention standard based on business and regulatory requirements"
 - In reference to the term "strongly authenticated", the decision was made to remove "strongly" and refer only to "authentication" in the security profile document. Additional guidance will be added to address content of policies and procedures.
 - The use of "alert & alarm" will be changed to "notify"
 - The term "flaw" will be defined as "An error in system design, implementation, or system deployment".
 - Format for RFPs
 - Comment: Where does the current document fail in supporting RFPs?
 - Action Item: Comment Resolution Team to follow up with more details.
 - Comment: The document is for more than just RFP's
 - What should be logged?
 - Do we need to provide examples?
 - Comment: Perhaps establish a baseline set of events that should be logged

- Comment: Would like to see critical parameter changes logged.
 - Do we need to provide message details?
 - Do we need to define levels of auditing?
 - Remove "verbosity" from control verbiage
- Comments/Questions
 - Comment: We need to add a statement to the intro section stating that this document was not intended to be used for regulatory compliance. This would ease the fear of some utilities that FERC will adopt and require them to meet these "as is"
 - Comment: If it is "prescriptive and actionable" then it is more than guidance.

General Comments/Questions

- Question: (Catherine Martinez/DTE) - Are there any plans to expand the "Threat Model" to address other grid applications past AMI. Answer: Not plans at this time but is a good idea. Please contact Catherine if you are interested.
- Action Item: Catherine Martinez will coordinate with those interested in this topic.

Joint Working Sessions

The chair proposed a standard format for the joint working sessions between the various Working Groups and Task Forces as follows:

- Summary of Security Requirements (presented by Other Group)
- Issues
- SG Security artifacts related to above issues
 - Existing
 - Needed
- Q&A
- Collaboration between SG Security and OpenHAN
 - Statement of Need
 - Task assignments

SG Security/OpenHAN - Sandy Bacik/EnerNex provided an overview of the OpenHAN security issues:

- Privacy
 - Different groups defining the data elements
- Securing one way communications
 - Legacy devices
 - Some of the smaller utilities are still looking at the possibility of one way communications
 - RDS systems (one way broadcast system)
 - Such as pricing signals
 - CA Title 24
 - Work has been done with PCT
 - In the public space and can be consulted/adopted/utilized this issue
 - Point made that the communications is never actually only one way
 - Out of band feedback channels

- HAN Network admissions
 - What are the requirements?
 - What entity controls are responsible for network admissions?
 - Are shared networks allowable?
 - Not looked at this issue in the current version of the AMI Security Profile (or v2.0)
 - Comment: We must assume HAN to be "hostile" or all guidance on the subject will not be accepted.
 - Comment: This is something we need to address. It has been addressed in the OpenHAN v1.0
 - Comment: The home is a partner to the network which is a little different than just being hostile.
- Application level security
 - No work as of yet to address this.
- Digital certificate authority
- Qualifying devices vs. messages
 - Comment: The model of qualifying whole devices vs. messages - If you have the assumption that the provider is sending messages down to a device or devices in the home and that is what you are securing, that's a relatively simple architecture. If you have an EMS on the same network, that EMS winds up having to be registered to the local trust authority on the network. One option is to address securing the communications and not the devices. In Texas, you may have a case where there are multiple providers within the same HAN.
 - Comment: There is going to be different model. The EMS could be receiving the signals from the utility in one case and not in another.
 - Comment: Some form of application layer security would help this issue.
- HAN considered a "hostile" environment
 - Comment: Need to consider the utility needs to be treated as "hostile" to the HAN. Don't see the robustness of the network being addressed as an issue here.
 - Comment: Trust model is thinking in the right direction. Need something such as a policy enforcement point. Obviously the industry is not there yet but we eventually need to be.
- Questions/Comments:
 - Comment: Lots of work has been done in IETF on application layer security.
 - Question: Is there a particular set of use cases we should use to model this need?
Answer: None that we know of for this purpose.
 - Question: Is there a threat analysis? Answer: Starting to consider starting an activity to take the AMI document and revise to address other areas of smart grid

The joint working session between SG Security and OpenHAN concluded with a call for volunteers for a SG Security/OpenHAN interest group. Darren Highfill/SCE will setup an e-mail list for those interested in SG Security/OpenHAN. Those interested were asked to e-mail Brian Smith/EnerNex and he will forward these names to Darren.

- Action Item: Brian Smith will forward list to Darren Highfill.
- Action Item: Darren Highfill will create a Listserve for SG Security/OpenHAN

SG Security/OpenADE - Steve Van Ausdall/Xtensible Solutions provided an overview of the biggest concerns with OpenADE and a summary of OpenADE security requirements:

- Privacy vs. Security
 - How do we enforce privacy considerations
- Securing the actual data exchange
- OpenADE is to allow third parties to get customer data from the utility
- Utilities are responsible to protect the customers sensitive information
- Tendrill, Microsoft Hohm, and GOOGLE Power Meter are examples of third parties

Darren Highfill/SCE provided an overview of the Third Party Data Access Security Profile:

- Developed by ASAP-SG
- Currently posted to Smartgridipedia.org
 - Action Item: Darren Highfill and Ed Koch to post 3PDA to appropriate OpenADE venue.
- Vision is that the Security Profile will address both OpenADE and OpenADR
 - Question: Does the Security Profile address OpenHAN. Answer: Currently the document does not address HAN message exchanges. A separate Security Profile(s) are planned to deal with these issues.
- Darren provided a brief overview of the Third Party Data Access Security Profile including roles defined in the document and how they mapped to various utility models, security related constraints, use cases, controls to roles matrix,
 - Overview of the Use Cases
 - Controls to Roles matrix
 - Controls to Use Case Steps matrix
- Comment: We may be able to now remove the security requirements from OpenADE requirements document and reference this document now.
- Question: A question regarding a "what if" scenario on an electric vehicle being charged at a location other than the car owners home. Answer: The document covers the exchange of information between the three identified roles and this scenario is out of scope as far as the intent of the document.
- Question: Does that mean ASAP-SG's work is complete? Answer: ASAP-SG work on the Third Party Data Access Profile is complete. SG Security will be responsible for taking the current draft to the v1.0 status. ASAP-SG is going to be working on more security profiles for other areas of the smart grid.

SG Security/OpenADR - The session began with a summary of OpenADR security requirements by Ed Koch/Akuacom. It was noted in the summary that there seems to be some direct correlation between the current document (Third Party Data Access Security Profile) and OpenADR. Outstanding issues identified included:

- Use of public networks
- The need for application layer controls
- Voluntary DR programs with pricing, weather, special days, etc. over different communications channels
- Security lessons learned in current OpenADR deployments
- NERC CIP

- NERC CIP is going to be very relevant when we bring signaling (i.e. controls) into the scope of the document. As it is, it is limited to usage data exchange and therefore does not factor in NERC CIP.
- Question: At what level are these controls (Third Party Data Access Security Profile) written? Answer: They are currently at the level as they were written in the DHS catalog. The exercise of the Usability Analysis Team is to determine if these are at the proper level or need to be adjusted.

SG Security/SG Communications Joint Session - Darren Highfill/SCE opened up the session and noted the objective is to identify how the SG Security WG can assist the SG Communications WG. Don Sturek/PGE then presented a summary of issues where the SG Communications WG needs assistance including:

- Commissioning, Configuration and Maintenance
- Edge firewalling
- Design for conformance test
- Software/firmware update
- Security provisioning and revocation
- Question: Are there use cases for these needs? Answer: Use cases are from Zigbee/Homeplug MRD

Matt Gilmore/Consumers Energy then presented further details of the SG Communications WG activities including:

- SG Communications has identified the data flows. Would like guidance on how to secure these data flows.
 - Comment: High level requirement containing in the 2nd draft of the NISTIR may be the best starting point to identify the security requirements.
 - Comment: The 2nd draft of the NISTIR has a new version of the architecture in a unified view.
 - Comment: SG Communications is looking for information that has implications on the size of the data that becomes overhead in the data exchanges.

The group then worked on identifying a Statement of Need proposal as follows:

- SG Network should look at the high level requirements in the NISTIR and determine mapping of SG Communications use cases to NISTIR interface categories.
- SG Security will map NISTIR interface categories to AMI Security Profile.
- SG Security will identify which technologies can meet the requirements.
- SG network will identify how these technology options meet data latency and application payload sizes.

The joint working session between SG Security and SG Communications concluded with a call for volunteers for a SG Security/SG Communications interest group. Darren Highfill/SCE will setup an e-mail list for those interested in SG Security/SG Communications issues. Those interested were asked to e-mail Brian Smith/EnerNex and he will forward these names to Darren.

- Action Item: Brian Smith will forward list to Darren Highfill.
- Action Item: Darren Highfill will create a Listserve for SG Security/SG Communications

SG Security/AMI-ENT Joint Session - The session began with opening comments from Greg Robinson/Xtensible Solutions. Mark Ortiz/CMS Energy then provided a summary of the AMI-ENT security requirements as well as the AMI-ENT services spreadsheet.

- Comment: NISTIR 7628 has high level interfaces defined
- Comment: Perhaps we can start with a sub set of use cases (i.e. connect and disconnect) and work with those.
- Comment: Is there anything that identify at what level (i.e.. application layer or payload) the security is applied.
- Comment: On the surface the initial thought is that the payload would need to be encrypted
- Comment: This is more communications inside the enterprise rather than outside the enterprise. For that environment, the first thing that comes to mind is the Security Domain approach used in the AMI security profile.
- Comment: If we can identify a sub set of use cases, we could possible use the same process as has been used to create the security profiles to customize controls for AMI-ENT.
- James Ivers/SEI provided an overview of the logical architecture view created in the AMI Security Profile. It was noted that the scope of this effort extended from the HAN interface on the smart meter to the MDMS. This does not include all business use cases involving the MDMS.
- Comment: There seems to be a lot of redundant work between the AMI Security Profile and AMI-ENT.
- Comment: With the amount of information that is in the AMI Security Profile, its is now reasonable for the business people to add these requirements to the use cases.
- Darren Highfill/SCE provided a brief overview of the Security Service Domains covered in the AMI Security Profile.
- Comment: Expecting PII to be shared by Resource Custodian similar to what is done today under HIPPA.
- Question: Do we have the swim lanes for the AMI use cases? Answer: Yes, they are on smartgridipedia.org
- Action Item: Action item for AMI-ENT to review the use cases that the services are based on and identify steps where the security requirements can be added
- Action Item: AMI-ENT to validate Actor harmonization
- Action Item: SG Security will create a mapping table between use cases and/or security domains to recommended controls for the AMI Security Profile.

The joint working session between SG Security and AMI-ENT concluded with a call for volunteers for a SG Security/AMI-ENT interest group. Darren Highfill/SCE will setup an e-mail list for those interested in SG Security/AMI-ENT issues. Those interested were asked to e-mail Brian Smith/EnerNex and he will forward these names to Darren.

- Action Item: Brian Smith will forward list to Darren Highfill.
- Action Item: Darren Highfill will create a Listserve for SG Security/AMI-ENT

Closing Session

The closing session included discussion on:

- The use of the OSI model as a roadmap for communicating with the other Working Groups and Task Forces.
- Discussion on how to make joint sessions more productive in the future. All agreed that these joint sessions are very important.
- Interest Areas/Lists to be formed
 - Several new lists will be created to address specific interest areas
 - OpenHAN Support
 - SG Communications Support
 - AMI-ENT Support
 - Lemnos
 - Risk Assessment
 - Third Party Data Access
 - Usability Analysis
 - General Interest
 - **Action Item:** Sandy Bacik/EnerNex will aggregate list for interest in Application Security and forward to Darren Highfill/SCE
- Prioritization/Action Items/Assignments
- Call for Presenters/Topics
- Additional Items
 - **Comment:** Understand we want to move our use cases into the standard format.
 - **Action Item:** Darren Highfill/SCE to send Kay Stefferud /Lockheed Martin a copy of the Visio file used for the Third Party Data Access Security Profile use cases.

Upcoming Meetings

Face-to-Face:

- April 26th-29th (Location TBD)
- July 19th-22nd (Location TBD)
- November 1st – 4th (Location TBD)

Teleconferences

- Monday, February 15 at 2:00pm ET
- Monday, March 1 at 2:00pm ET
- Monday, March 15 at 2:00pm ET