UtiliSec/AMI-SEC Face-to-Face at AEP - Columbus, OH

Thursday, July 16, 2009

Darren Highfill, Chair
Matt Carpenter, Co-chair
Bobby Brown, Meeting Minutes

Agenda:

- Introduction and Logistics
- Agenda review & update
- Orientation and Review: Mission, Purpose and Objectives
- Status Updates
- Organization and Communications
- Talk-through: AMI Security Profile
- Misuse Cases
- Task Objectives: Usability Analysis
- Usability Analysis Team Formation
- Usability Analysis Discussion
- Next Steps
- Upcoming Meetings

Documents

UtiliSec Presentation Slides, Usability Analysis Team Slides

Discussion

0800 **Introductions, Logistics** (Neil Greenfield, Chair)

0820 **Agenda review & update** (Chair)

0830 **Orientation and Review: Mission, Purpose and Objectives** (Chair)

Overview of groups mission, organizational chart, etc. (Refer to slides)

ACTION ITEM: Chair requesting volunteers for hosting April 2010 and July 2010 face-to-face meetings.

Neil indicated that there were 150 registrants for the 3 days at AEP and about 80-90% in attendance.

0850 **Status Updates**

Review of 2008 deliverables.

ListServ Subscribers ~265 to-date. Everyone should be subscribed to UtiliSec Announce listserv at a minimum. Still getting requests to join just one, but not other ListServs (e.g., AMI-SEC, UtiliSec, etc.). Chair reviewed the purpose of each list:

UtiliSec Announce = general announcements
UtiliSec Technical = technical discussions (potentially lengthy)
AMI-SEC = only AMI security related discussions

Chair described where to register on UCA.

NIST CSCTG Report

Cyber Security Coordination Task Group – large amount of overlap of attendees between groups. Was a meeting in April (~500 attendees) and May (~ 700 attendees). ASAP-SG is working hand-in-hand in development of work. These are not competing activities, but are complementary activities.

NIST has several DEWGs that address Smart Grid; and the CSCTG addresses security and is lead by Annabelle Lee. The CSCTG is focused on high-level requirements for all stakeholders/organizations as a whole, whereas, UtiliSec is focused on the organizational level for more tangible requirements and addressing. The CSCTG has 4 groups – "Bottom-up", Vulnerability Analysis, Standards, and Privacy. The information produced is being compiled in the NIST-IR (Inter-agency Report) document. Annabelle wants to get to requirements – especially threats, vulnerabilities and impacts.

The CSCTG "Bottom-Up" group is focused on vulnerabilities at a low level and abstracting up. The group has had discussions around such topics as "if Internet plays into smart grid" and is going to conduct a Risk Analysis to determine. The CSCTG is trying to put information into "buckets" so that can be discussed in meetings; they are also looking at interfaces and identifying those and apply security around them.

UtiliSec is chartered with developing detailed requirements and best practice and guidance. Annabelle Lee presented that the CSCTG is working closely with UtiliSec on its efforts. NIST has to come up with the first deliverable in September, an interoperability framework. The task group is coming up with high-level security requirements for entire smart grid. Security concerns around smart meters and AMI have the attention of government. Annabelle has asked ASAP-SG to look at AMI first because of the heightened awareness.

NIST CSCTG calls are on Monday at 11am EDT; contact Annabelle Lee at Annabelle.Lee@nist.gov for more information.

IEC WG 15 Report

Frances: 62351 Standard – There are published parts 1 through 6 and the group is in the process of standardizing "Part 7 – Network and System Management" (similar to MIBs). The working group is midway through "Part 8 - Role-based Access Control". The working group is beginning to start on "Key Management".

ASAP-SG

Member question: Which point in the process does interpretation come to play (for the AMI SSR – System Security Requirements); where to apply within the system (e.g., like NERC CIP)?

Chair: The SSR did not do good job of delineating where this control is applied. But, from the Security Profile it will leverage the work of the SSR and define which systems/assets will require which controls based on a risk assessment.

Member question: Are you talking specifically about particular assets like generation and transmission assets?

Chair: the first security profile is going to be AMI. Later on the group will be addressing other applications such as Distributions Automation, etc.

The ASAP-SG is a public/private collaborative between DOE, NIST and utilities. The intent is not to overtake the activities of the working group, but to feed the activities. This work stemmed out of ASAP from last year – the work carved out of the work done in 2008. In Q1 determined that weren't going to meet goals without funded and dedicated resources: DOE, EPRI, Utilities, FFRDCs, etc.

ASAP-SG kicked-off earlier this summer. There is a strong need for reference architectures, well defined use cases, etc. for development of security around other applications such as Network Type, Distribution Automation, etc.

Member question: Can you define in more detail as to what do need for developing a profile?

Chair: Please visit www.smartgridipedia.org. Posted material is licensed under creative commons.

Member question: How do you take into account for the variations in different scenarios from region to region and regulatory environment; where there may be more or less actors?

Greg Robinson (AMI-Enterprise Chair): This is what AMI-Ent agreed on as a common set of requirements. This is a building block approach, so that can be adapted to different regulatory markets.

Member question: At which point does break down to functional … For example, the actor is CIS system, there is a need to understand what functional items trying to control; for example a particular function handled by CIS on one system may be handled by the Head-end on another system.

Chair: Can't make security profile that applies to every configuration. There is some work to be done beyond baseline.

Member comment: There is a current understanding is that use cases represent ISOs and not co-ops.

Chair: Correct. There is a need to get their involvement.

Greg Robinson – Consumers is looking at use cases/Multispeak a superset.

0910 **Organization and Communications** (Chair)

(Refer to slides)

OpenSG has a draft charter and is waiting on the UCA approval.

There are expectations from working group activities. Need to provide a charter, submit project schedule and monthly status, etc.

Chair has rough draft of a charter. A one page charter will suffice – need to speak to mission, etc.

Members in good standing have the right to vote. There are attendance requirements for voting – for individuals, organizations, etc. A member must be present 3 out of 5 meetings to vote. For organizations, a representative from the organization suffices for the 3 out of 5 requirement.

A working group must supply monthly schedules and status reports. Will adopt ASAP-SG and some internal projects. Sandi Bacik worked on the Roadmap document as an example.

We have not been doing a monthly status report – to work with the Secretary.

The working group needs to schedule dates for teleconferences between now and next face-to-face meetings. The group has an established timeslot.

Structure of sub-groups/ad-hoc groups will be as necessary. About to form a sub-group this afternoon, but don't think needs to be a TF. The Usability Analysis team will be a sub-group. Assumption has been that there would be a TF for each of the applications for Smart Grid, e.g., Distribution Automation, Substation Automation, etc. Is this an effective model? Should we form around Usability Analysis or by Application?

Greg Robinson: From an AMI-Enterprise approach we are looking at a matrix approach. Service Definitions, System Requirements Specification, Use Case are verticals; horizontals are oriented toward business functions. The business functions are the task forces. The verticals are ongoing teams.

Chair: I can see this method working for us. Business function and service definition teams that are vertical across those. Any other ideas/thoughts?

Member: Basically, it is crucial to have task for SCADA, transmission security, distribution security, etc.

Greg: Would this be a way to prevent overlap between groups?

Chair: Not an easy solution but will do what can.

Chair: We will seek OpenSG approval for formal document release.

Member: Understand that voting rights have changed?

Chair: Voting rights are now by UCA membership – not just being utility member/representative.

Chair: The working group needs to seek approval for charter and seek approval today. The working group should get approval for task force and lower level chairs; the Vice-chair and secretary positions. The chair selects the acting vice-chair, secretary positions, etc. and puts before group as a vote.

Chair: The working group needs a working group constitution.

Chair: The process for information exchange for Intra-organizational and Inter-organizational: We have a form that was developed by Sharon Lee from PG&E.
ACTION ITEM: Sharon to make into a form or documents to codify.

Chair: UtiliSec/AMI-Sec has a good cross-representation from other OpenSG groups. We need to be actively involved in other group's activities. We need involvement from those groups. The Chair proposed having an internal liaison for those groups. Is this good idea?

Doug Houseman: Think that because of overlap in the groups then think not good idea to have one person represent group.

Chair: How do we get richer dialog between the groups?

Greg: Preliminary, but assuming that would have a joint security in alignment with the matrix.

Chair: I think that would be a TF for each other OpenSG group. We could align across those lines, but as long as subgroup brought back issues to UtiliSec for resolution. There would be concerned about misrepresentation/guidance.

Doug: Believe that development of several groups will result in very little time (15 minutes) to concentrate on technical issues.

Member: The matrix idea may work if each has their own working groups – if leads are invited to the other groups. Example, if ADE has security concerns then can invite security.

The Chair is going to work on how to implement exchange of information, instead of just verbal hand-off. For inter-organizational the feeling is that on that front we are doing reasonably well and that there is not much risk of lacking covered.

Chair: What is missing from UtiliSec Charter (refer slide)?

Team: editing the text of the slide. Include the word “security” in appropriate places. Include “operating”. Include “recovery”

VOTE: Charter was asked to be accepted? Motion made and accepted. Any UCA member apposed? * none

1100 **Talk-through: AMI Security Profile**

Chair: (refer to document) walk through document

Jim Nuturo (ASAP-SG/ORNL) presented the process of risk assessment for a given use case.

Chair: (refer to spreadsheet) present the rating system for categories confidentiality, integrity and availability. We found it interesting that the characteristics behaved differently as you walked through the sequence diagram.

The team made an assumption that at whatever step was started with for confidentiality then the level could only be elevated, because confidentiality at lower level could compromise another part of the system

The team made the assumption that integrity was opposite – starting at the tail of the sequence diagram.

The assumption for the minimum availability requirement had to be made for the whole system (based on actor expectation)

Member: This is a good mechanism for analysis on electric system, but wonder what impact is on the electric grid perspective?

Chair: The spreadsheet shows analysis for actors that are critical to the process, e.g., can an actor/asset stop the mission of the process?

Jim: If can justify a requirement that could prevent mission to the system, then requirement/control shouldn't be mandatory.

Howard Lipson (SEI): Threat/actions are many scenarios are called mis-use cases or abuse cases; after lunch like to talk about how to create abuse cases

Member: One approach is to base response on percentage. Some percentages may be acceptable and still meet mission goals; same thing for is it just a single customer, multiple customers, etc.

Chair: The team didn't decide that confidentiality propagated one way, or integrity propagated another way. Some seem to apply to actors, others on messages/information, other on behavior. The interesting thing was when put these together then got coverage. Got what drove the requirement / not what limited the requirement

1200 ***Lunch***

1300 **Misuse Cases** (Howard Lipson - SEI)

(Refer to slides)

Points in the scenario where a misuse case exists; for example: a car rounding curve has vector on course of the road, but the vector of inertia is headed off a cliff. It is not necessary to determine what cause the car to skid off cliff (e.g., drunk driver, ice, etc.) but examine what controls may need to be in place to prevent skidding off the cliff.

The goal is to find gaps in security requirements and determine needed recommended controls the Security Profiles.

The UtiliSec Technical list should be used to continue discussion on this topic.

Member question: Should we have a TF for misuse/abuse cases?

Chair: recommend we have a group that would work against particular profiles

Member question: Is this a threat-vulnerabilities team?

Chair: this is a brainstorming activity looking at vulnerabilities and prioritizing them in a structured format.

Member: Suggestion to call them "Anti-pattern analysis".

ACTION ITEM: Bobby to get listserv setup for this group and send out slide deck. Work with Howard on "official process" of identifying missing security requirements

1400 **Task Objectives: Usability Analysis**

Chair: (Reference Deliverable 4 – Usability Analysis in the Prospectus document). The architectural team and authors of the material would not make good checkers of the process, etc., hence, the need for a usability analysis team. The process is iterative and is the reason UtiliSec members are seeing at such an early stage of the Security Profile. The community is getting into the development of this project at an early stage.

Daniel Thanos has been asked to lead the Usability Analysis team. He is going to give his thoughts on organizing the team and work.

1420 **Usability Analysis Team Formation** (Daniel Thanos)

(Refer to slides)

Daniel presented a straw man approach to Usability Analysis that is to be incremental. One initial action step is to define what is meant by term 'usability'. The group's structure should be broad representation. There will be cross validation to support that notions being made are fair. The team wants to make sure subgroups have good representation from domains.

Group meetings – as starts to evolve would align with when ASAP-SG Architecture group meets; they should be open and give fair analysis of what is going on.

Work Products – UA Document, UA Criteria Document – level set to say what is meant by usability, UA Reference Model – have reference model.

1500 ***Break***

1520 **Usability Analysis Discussion** (breakout groups)

Chair: Breakup in groups based on sections of the security profile document (3-7). Sections 6 and 7 have not been worked on yet. Good representation of domain expertise in each group should occur (refer to slide that Chair developed, e.g., SCADA, Networking, etc.).

1600 **Next Steps**

ACTION: Members that took notes in break-out sessions should supply to Daniel Thanos.

Chair: Recommend UtiliSec calls for UtiliSec to stay Thursday @ 2-3 PM EDT every other week and 3-4 PM EDT for subgroups. (See upcoming meetings below)

1700 Adjourn

Upcoming Meetings

Teleconferences:

July 30th at 2:00 PM EDT (**Wednesday)

Aug 13th at 2:00 PM EDT

Aug 27th at 2:00 PM EDT

Sep 10th at 2:00 PM EDT

Sep 24th at 2:00 PM EDT

Oct 8th at 2:00 PM EDT

Face-to-Face:

- October 20th-22nd hosted by EnerNex in Knoxville, TN
- January 5-7, 2010 hosted by FPL in Juno Beach, FL