SG Security Webinar

Monday, May 17th – 2-3pm EDT

Chair: Darren Highfill (present)
Vice-Chair: Matt Carpenter (present)
Secretary: Bobby Brown (present)

Allen Benitez / CA PUC
Brian Lenane / SRA International
Brian Owen / OSI Soft
Daniel Thanos / GE
Darren Highfill / SCE
Dennis Gray / APS
Doug McGinnis / Exelon
Ed Heberlein / Centric Consulting
Efrain Gonzalez / SCE
Eric Cardwell / ICF International
Howard Lipson / SEI / CERT
James Ivers / SEI
James Pace / Silver Spring Networks
Javier Torres / IBM
John Lilley / SDG&E
John Mani / Comverge
Julie Brown / Entergy
Kevin Brown / EnerNex
Lindani Phiri / Elster
Louis Robinson / Constellation Energy
Mike Ahmadi / GraniteKey LLC
Nakul Jeirath / SWRI
Neil Greenfield / AEP
Nick Gerbino / Dominion Resources
Ramprasad Golla / GridNet
Rich Tolway / Arizona Public Service
Scott Palmquist / Itron
Sean Sherman / Triton/PPC
Shrinath Eswarahally / Infineon
Slade Griffin / EnerNex
Tom Thomassen / Symantec

Agenda

a. Review Agenda / Call for Items of Business - No agenda changes. No new business items.

2. Old Business
   a. Perspectives and Insights
   b. Subgroup updates
      i. AMI Security Profile revisions – Ido Debrowski is trying to wrap up work on version 1.9 for review by the group and vote.
      ACTION ITEM: Gather eligible voters list from face-to-face.
      There will be 1 week period for review and call for vote after the version 1.9 release. Instructions will be clarified with distribution of AMI SP v1.9. Upon approval, 1.9 will be given a 2.0 version number and it will be posted to Smartgridipedia.org and submitted to NIST.
      Note: Mike Amani - California PUC is using the AMI Security Profile requirements including full sections and parts. The application level security is definitely adequate. They will have their document up for review in about a week. They are looking at OpenHAN for the HAN also.
      ii. Usability Analysis (3PDA SP review) – John Lilley (Chair) and Daniel Thanos (Vice Chair) – The group does not have a Secretary yet. The UA task force is working on getting documents reviewed as documents come through. The group will

establish team for reviewing. We anticipate that reviewers will vary by document.

Jerry Gray has passed along comments.

There will be separate (sub-) distribution lists for:
Usability Analysis Team, Comment Resolution Team, CyberSec Interop, OpenHAN, SG Communication, etc.

ACTION ITEM: Darren to resend lists for members to decide if they would like to join.

iii. CyberSec-Interop – No group members present to report. There is a description of this activity in the slide deck from Washington DC meetings.

iv. Network Security – Vincint Bimmel (Trilliant) – working on security for the OpenSG Network group; looking for Chair and VC for network security TF; and likely a secretary as well. Darren looking for those with interest to send email.

3. New Business

a. OpenHAN support – this group anticipates pushing this document out this week. Mary Zentara leading the effort for this document. We will be using the UtiliSec Announce for information and not using AMI-SEC for the HAN security. Mary has been reviewing the NIST-IR document and it notes that the OpenHAN HAN document discusses several security items. There are references for CIA (confidentiality, integrity and availability), categorizing impact, FIPS Pub 199, etc; and anticipates giving SG Security a reference for the Impact (Risk) assessment. Comments need to be submitted this week so that OpenHAN has time to respond.
ACTION ITEM: If you have a comment please provide a recommended change – do not submit comments that only state that "this is broken". This will be incorporated into version 1.95 and will be out for approximately 1 month for review before vote.
ACTION ITEM: Darren to check on AMI SP to see if used a single column for risk (CIA) to keep the documents similar. (Brian Owen)

b. SG Network support – Refer to SG Network TF "Smart Grid Conceptual Actors – Data Flow Diagram" slide. This is similar to the NIST high-level architecture. This document has more actors and new actors not listed in the NIST diagram. The SG Network diagram also includes clouds. ASAP-SG also identified that there are peer-to-peer relationships in the components in the FAN gateway. There is also a spreadsheet that identifies the messages and payloads that can be found throughout the drawing containing a Requirement reference, data flow reference and use case reference, actors, payload name identifiers, type of payload, daily clock periods, reliability, latency, etc. There are three that are important to them that are Confidentiality, Integrity and Availability. SG Network needs SG Security to review to make sure these values are accurate.
ACTION ITEM: In the very near term we need to do sanity check to make sure these make sense.

Long term SG Security needs to develop security requirements for the different communication links.

The team walked through validating one of the data communications between CIS / Billing and MDMS (1Aa). Use the FIPS 199 definitions for High, Moderate, Low. NIST is proposing that communications CIA property with low will not be encrypted. For example, if confidentiality is low then data will not be encrypted, but if integrity is medium, then the data may be signed.

ACTION ITEM: Darren to put out a set of instructions on how to update the document. If you disagree with a classification then would need to do so in respect to impact to system. Privacy is not in scope for this exercise. Current volunteers: Darren Highfill, Matt Carpenter, Slade Griffin, Daniel Thanos, Scott Palmquist, Shrinath Eswarahally, Doug McGinnis, John Lilley.

4. External Engagements, Business, & Issues
    a. CSWG – the vice-chair wanted to note that SGIP CSWG is not creating law, but security requirements.
    b. SG Conformance – working on three work items: reporting and communications, high-level conformance requirements, and technical use cases. Kevin Brown working on tool selection for testing use cases.
    c. IEC TC57 WG15 – Met in Paris, France last week. Worked on defining RBAC as it binds into IEC 61850. Is going to start work on security architecture. Working on standard for Crypto and key management. Looking at security with DNP3 and found some potential problems.
5. AOB
6. Roll Call