Session 1 - Tues AM

Tuesday, November 02, 2010

9:38 AM

1. **Notes from Plenary**
   * Face to Face Meetings in 2011
     + March 7-10, San Antonio - not confirmed
     + July 18-21, Vancouver, BC
     + November 14-17 - unknown
2. **Agenda Update**
   * Tues Morning
     + Agenda Update
     + IEC TC57 WG 15
     + Usability Analysis TF
   * Tues Afternoon
     + Collaboration with SG NET in support of PAP2
     + Coordination & support role for SG NET and NIST CSWG
   * Full Day on Wed
     + Cybersec Interop
     + ASAP SG - Blueprint for Security
     + NERC CIP SDT Update - guest speaker from Duke Energy
     + Stuxnet Video and Discussion
     + Software Security
     + NIST CSWG Update
     + Embedded System Security Interest Group
     + Vulnerability Disclosure and Information Handling
     + Planning and Prioritization

1. Looking for more interaction from the "working" group. Sessions are becoming too conference like
2. Ramp up of new task forces
   * CyberSec Interop
   * Usability Analysis
3. External coordination
   * NIST CSWG
   * PAP 2
   * PAP 10,
   * NERC CIP STD Team
     + Provide security profiles to this team from SG Security,
   * IEC TC 67 WG 15
     + SG Security does not have a direct relationship to this group
     + Relationship exists between UCA and IEC
       - Hosts pages of IEC on UCA site
       - Overlapping members
       - Can request access to IEC works in progress thru IEEE - requests to Frances Cleveland or Darren Highfill or Bobby Brown
4. Interest groups/topics of discussion
   * Embedded system security
     + Possible new Task Force
     + Draft charter in the works and ready for review
   * Software security
   * Vulnerability handling and info sharing

1. ASAP-SG looking for utility participants
   * Public-Private collaboration between DOE, EPRI, and North American Utilities
   * Separate Project from Open SG and UCA project and working groups
   * Mission: Develop system-level security requirement for smart grid technology
   * DOE looking for fresh round of utilities to participate
     + Need 8-10 Utilities to participate and provide funding
     + Other sources of funding include channels via EPRI) or in kind contributions for resource
     + Requires a $100K commitment from Utility
     + Question: How is the scope influenced by utilities?
       - Yes - scope and profiles are formed from input by those utilities have funded the project
   * A Prospectus is available to use to pitch to Management at Utilities
   * An Executive Summary is in progress that will include examples of how AMI SEC Profile worked its way through various organizations - NIST, IEC, ANSI, NERC, and PUCs
   * Contacts: Bobby Brown bobby@enernex.com or Darren Highfill darren@utilisec.org
   * Team meets twice a week via teleconference and face to face every other week
   * AMI Security Profile v1.0
     + Ratification of 1.0 in 1 calendar year
     + Security controls based on DHS catalog - tailored to AMI
     + Scope: AMI back office components to premise interface in the meter
     + Feeding into NIST CSWG AMI Security Subgroup
   * Third Party Data Access Security Profile
     + Picked up by NAESB for a standard through the work of PAP10
     + Support from Open ADE
     + Scope: Addresses the establishment, modification, and deconstruction of relationships between individuals, utilities, and vendors that involves the handling of sensitive info
   * Distribution Management Security Profile
     + Draft handed off in August
     + Usability Analysis Task Force will review after Third Party Data Access Security Profile is reviewed
   * Wide Area Management/Synchrophasors Security Profile
     + Next up on the docket to be written
   * Possible New Task: A blend of the Distribution Management Security Profile and AMI-SEC Security Profile for consideration as an IEC Standard by the IEC TC 57 WG 15
     + Scope: any endpoint in utility system for IEC standard consideration

**IEC TC57 WG 15 -**

* IEC - International Electrotechnical Commission
* TC 57 - Technical Committee 57 - power systems
* WG 15 - Working group 15 - communications security
* Active Work
  + IEC 62351 is the domain of this group
    - standards recommended by NERC to FERC for a proposed rulemaking
    - Still a work in progress
    - Parts 1-7 have been standardized
    - Part 1 is an introduction and high level ; part 2 is glossary and terms
    - Parts 3-7 are very prescriptive and are international standards
    - More parts are in development
      * Enhancements for 3 and 4
      * More security for 5 and 6
      * Part 8: role based access control
      * Part 9: key management - new work proposal
  + 61850-90-5 - synchrophasor measurement communications (IEC TC 57 WG 10)
    - ASAP-SG is providing support to this activity
    - WG 10 power system ied communications and associated data models
    - Security work on 90-5 coordinated with WG 15
    - Issues
      * Resource constraints
      * Very low latency
        + Measurement of phase angle taken and it useful life is 2 seconds or less
        + Asymmetric crypto has to heavy of load
      * Continuous service - streaming data can't be interrupted by crypto keys
    - Solution path -
      * to protect against using phasor measurements to determine where generation is coming from and going to and cause harm (i.e. Enron)
      * Signature on all messages
      * Option for encryption
      * Use public-private keys to negotiate a temporal/session symmetric key
        + Time to live, time to new key, etc.
    - Why is ASAP SG putting out a profile Wide Area/Synchrophasors?
      * Protocol level communications being addressed by IEC but ASAP SG will cover the details to ensure a secure setup with NASP NET and Wide Area Architecture
      * ASAP SG will pick up where 61850-90-5 leaves off
      * ASAP SG will address systems integration
  + Q&A
    - Is ASAP SG supporting IEC WG 10 and 15 / 90-5?
      * No. The WG are doing protocol specs (datagrams for communications). ASAP SG takes it to system architecture level and security above the protocol level
    - Are members overlapping?
      * Yes. Darren and Bobby are in ASAP SG and WG 15

**Usability Analysis TF, John Liley, SDG&E**

1. Always looking for more volunteers
   * Meet every 2 weeks , 10am pacific, 1pm eastern
   * Next meeting 11/8/2010
   * Distribution list
   * Contacts - John Liley, Daniel Thanos, Scott Palmquist, or Darren Highfill
2. Charter under development
   * Final draft under review by the Task Force
   * Separate Evaluation Criteria Document (criteria doc for analysis)
     + Scope and goals
     + Mapping to requirements
     + Use cases
     + Lifecycle
     + Procurement
     + Security levels
     + Component wise security - do requirements map back to specific system components?
     + System architecture - does it fit into the overall architecture?
     + Bobby suggested other criteria - testability?
       - Can be included but the TF needs a paragraph describing the criteria
   * Analyze docs referred by SG Security
3. Team
   * Utilities and vendors - review is collaborative
4. Reviewing Third Party Data Access Security Profile
   * Final editing
   * Consolidated comments
   * Drafting analysis report - (guidance for approval of document by open SG Security)
   * Ownership vs. Privacy Rights of Data
     + Ownership implies control - gives the owner the right to grant access to the data
     + Risk is loss of privacy
     + Replace resource owner with energy user? Define Resource Owner?
       - Customer has expectation of privacy of usage data but does not own the data
       - Comment - ownership defined by State and use the terms data subject and custodian/trustee; data subject is used in privacy realm of other industries
       - Comment - issue of ownership becomes politically charged and energy user may restrict the use of the document; who is generating the data? - data subject captures that meaning
       - Comment - data subject does not always generate the data about themselves
         * Comment - that distinction is ok, nearly 100% of time data subject is generating the data
       - Comment - replace all references with data subject and data custodian?
         * Comment - makes sense and makes the document consistent
       - Initial use of the resource owner was hard to distinguish between the end device (meter, appliance) and the data itself - the term maintained flexibility that may no longer needed
       - **SUGGESTED CHANGES:**
         * **Change resource owner to data subject**
         * **Change resource custodian to data custodian**
         * **VOTED and CARRIED by show of hands**
     + Question - Is there a clear definition of PII in this space?
       - Response: NIST CSWG Privacy group has delved into this topic extensively and have a solid handle on this issues. Both Operationally and Legally.
       - Response: Reference the work done by the NIST CSWG Privacy Subgroup
       - **Comment: John Liley - PII is referenced in the document and needs to be pulled out**
5. Reviewing Distribution Management Security Profile
   * Comment period still open -
     + No comments from SG Sec WG yet - LAST CALL FOR COMMENTS!!!!!!
   * Analysis begins 11/8/2010
   * Resolution meeting late Nov/early Dec
     + Resolution process is 2-4 weeks
   * Final Review Dec/Jan

**PLANNING ITEM FOR SG Security: Review of Actor Mapping of 3rd Party Data Access and NISTIR 7628 Actors, work done by John and Sandy**

Session 2 - SG Sec & SG Network Joint Session

Tuesday, November 02, 2010

12:54 PM

* Overview
  + SG Network looking at data payloads requirements to support the work of PAP 2
  + SG Network requests SG Security to help in specifying security requirements
  + Several rounds of work have occurred to date
    - Taking data payloads and assigning CIA to each
    - Assigning HML to each data payloads
    - SG Network took an educated guess at HML
    - Work was split up amongst SG Security- inconsistent criteria for HML!
    - Process discovery by trial and error but nailed down now
* Question: Do the groups need to agree and what the actors are and what domain the actors are in?
  + Agreement that this needs to be done
  + Coordination with existing NISTIR groups
  + EX: meter with ESI and meter without ESI
* SG Conceptual Actors/Data Flow Diagram
  + Payload examples - meter read request, meter read response, etc
  + Are security requirements different based on the components involved?
* Spreadsheet has identified 180 payloads
  + What is the CIA requirement for each of these?
    - Work that SG Network requested of SG security
  + But
    - SG Security - Analysis was performed looking at the data versus the interface it was going across
    - SG Network - Analysis was performed based on use cases and the interface being traversed
  + So, 2 different approaches used. How to harmonize or produce a united document?
    - Suggestion - Do it now at the meeting
    - Suggestion - Use a template created by SG Network to aide in the process
  + So, the Template
    - Captures payload name, payload type, parent requirement, SG Network Logical Interface Category (LIC), NISTIR 7628 LICs, Vetted LIC, NISTIR 7628 LIC Description, SG Network CIA/HML, NISTIR 7628 CIA/HML, Vetted CIA/HML, and column for Rational/Comments
    - **Missing description of the data fields/attributes - SG Network task**
    - Discussion ensued on the fact there are different CIA/HML ratings based on the interface involved in delivering the data payload.
      * Comment - emotional response to the interface therefore CIA is different
      * Comment - NISTIR CIA/HML are end to end payload and more generalized vs. the details of the payload point to point
      * Comment - NISITR CSWG working at a high level and not looking at the details of the payload
      * Question - should there be a single CIA/HML for each payload or is it dependent on the interface?
        + Suggestion - use some sort of agreed upon criteria, discuss how to interpret the criteria, and assign a single CIA HML for each payload, then look at the interfaces & analyze the interfaces security and use the high watermark of the interfaces for the other interfaces, compare against NISITR 7628 as a crosscheck
        + Comment - if all interfaces end up HHH and therefore all payloads get elevated to HHH - no point
        + Comment - example : head end to collector - icmp ping of meter or firmware update along the same channel - high watermark is HHH for firmware and then applies to icmp ping as well (not technically feasible)
        + Comment - still exposed to hacking if using different security for each but if you employ link layer encryption, this can prevent denial of service attacks. Requires additional analysis
        + Comment - agrees with just looking at payloads, then drill down to system/interface, and then maybe the link layer; NISTIR muddles these together
        + Comment - Agreed. Do a payload tagging for HML as long as the documentation is clear on what was done may not be sufficient to secure the system. Lose defense in depth if you don't look at the interfaces and the links
        + Comment - Agreed. More to be done to secure interfaces and links. Add 2 more columns to the template - what does the payload mean to an attacker/hacker?

Attacker/Hacker was tried but did not work very well

Use these columns for rational/comments/etc

* + Question: How are the CIA ratings for HML get applied in practice?
    - Not enough detail to build a system
    - SG Network developed a "Implications and Rationale" Document
      * Comment - resembles the failure analysis used by SG Security in developing security profile for Distribution Management (DM Security Profile)
      * DM Security Profile - What information is being exchanged between actors and what happens if this step fails or is compromised ---> leads to a set of security controls --> security controls are assigned to the steps or actors
      * DM Security profile Covers most of the payloads of SG Network (in the spreadsheet)
        + mapping needs to be done between SG Network payload and the DM Security Profile Use Cases
        + Walked through a use case for field application requesting data from a sensor or another field application and applied to audit\_app\_event payload
      * Comment - was CIA assigned to the failures in the DM Security Profile?
        + No, but could be done but would not change the security controls assigned
      * Question - How will this be used (CIA ratings HML)? Build a system? Or after CIA rankings for NIST CSWG - that is a different goal?
        + Comment - add CIA to the failure and HML impact to use case step into the DM security control
      * Comment - NERC CIP does this at the critical asset level. Should this model be adopted?
        + Response - No. NERC is moving away from this method of critical asset to systems based. And, even if critical cyber asset remains, this is for the bulk system and not distribution
* **NEXT STEPS - compare data payloads to the use case diagrams/steps in the DM Security Profile**
  + **The term role needs attention when doing the mapping - an actor may map to multiple roles**
  + **Mapping Example** 
    1. **audit\_app\_event from SG Network maps to:**
    2. **DM Security Profile Use case 3, step 1b, sensor role**
    3. **--> use case 3 step 1b shows failures 1,2,3,5,6,13,18**
    4. **look up failures on control mapping table for security controls for the actor name (sensor)**
    5. **---> then look up the detection number (11)**
    6. **---> detection table shows the control for that detection (fips 180 or fips 185)**
    7. **---> lookup fips 180 or fips 185--> etc.**
  + Comment - seems very complicated. Can SG Security provide SG Network classifications to do the lookup for the control?
    - Response - complicated because the whole process has been explained; the mapping is somewhat straightforward
  + Question - what business requirements were used to determine the controls?
    - Response - determined if the data was not correct and cause a bad decision to be made
    - Sensors are not designed or equipped to do hashing or signatures (fips 180/fips185)
    - Comment - DM security profile has not been reviewed by the community or industry - still in draft (v0.12)
    - Comment - Security analysis at payload tied to SG Network requirements of latency for time to complete command that includes encryption, tls, or whatever security control
* **ACTION: SG Network to continue capturing CIA/HML for each payload**
  + Comment - DM Security profile is out for comment
  + Comment - not appropriate to apply CIA to payloads but to systems
    - Response - no response at this point
  + Question - what does this mean for collaborative work for nist cswg
    - Response - mapping of CIA for payloads against each interface is a deeper dive
* **ACTION: New listserv for group to formalize the group that did the initial work on the CIA mappings** 
  + Work with PAP2 is enhanced through all of this work
  + Can look at a set of controls and apply it to the system and determine the impact to the wireless system
  + Can more accurately determine the overhead security controls will impose