F2F BC 7.18.11 Session 1

Tuesday, July 19, 2011
12:33 PM

1. Agenda
    a. No changes or questions
    b. Presentations: http://osgug.ucaiug.org/utilisec/Shared%20Documents/Presentations/SG%20Security%20F2F%20Vancouver%20-%20Day%201,%2020110718.ppt

2. **Next Meeting: 8/8/2011**
3. Summary of Action Items
    a. OpenADR:
        i. Question - roles and actors are not aligned with nistir 7628?
        ii. Question - are there definitions for each of the actors? Unknown.
    b. Usability Task Force
        i. Teron Williams and Chris Blask volunteered to take this on: create a general overarching lifecycle for security profiles
        ii. Action: Agreed to use UML format for use cases
        iii. Protection Control 21: Labeling
            1. Action: Send question out to the utilisec-technical listserv
            2. Action: Going forward, only include controls that can be implemented
        iv. Protection Control 41 – Wireless Encryption
            1. Look at the FIPS reference to determine if it should be more specific
            2. Support to leave the language as is - agreement there is a need to protect the management of the channel.
            3. Look to include in this control or in another control, language for network authentication
            4. Need to look at what FIPS certification means

4. Status Updates
    a. NIST CSWG & PAPs
        i. AMI SEC -
            1. reworking the amisec security profile produced by asap-sg
            2. Active in looking at the use cases in the profile;
            3. reviewing the diagram flows

Question: What the final product will be and how it will be used?
Response: Deferred to later time

    b. PAP 10
        i. NAESB has put forth a documentation on ESPI
        ii. settled at the moment

    c. PAP 18
        i. Migration from sep 1.x to 2.0;
        ii. Whitepaper produces and made available

iii. Do not appear to be any active tasks in regards to security
iv. The NIST CSWG Standards work group is reviewing this work

d. NERC CIP SDT
i. Active in drafting version 5
ii. Meeting this week (july 18th)
iii. Radical change for CIP002
1. Moving towards a bulk electric system cyber asset designation
2. High med low categorization of assets
3. Designates what the criteria will be for the assets
iv. Version 4 has been approved and sent to FERC for approval - introduces the brightline concept for assets
1. Once approve, compliance is expected by the following quarter
2. Being very prescriptive on what is a critical cyber asset is

Question: Did team step away from utility identifying all assets and then stating which are critical?
Response: Not aware that this is still in the draft

Question: Is the repurposing CIP0010 and CIP0011 into change management and info protection still on the plate?
Response: Was looking to replace CIP2-9 and replace with CIP10 and CIP11 - substantial departure in approach. Ton of pushback from industry and backed off this approach. Some of this has found it way into draft of version 5.

Question: Any changes in physical separation approach?
Response: Not aware of.

e. IEC TC57 WG15
i. Met in spring 2011
ii. Next meeting in Oct in CA
iii. Focused on defining security guidance for key management

f. Produce a single document that centralizes all of the previous work
i. In draft now

g. Worked with WG10 - synchropasor communications w/ time synchronization; security was addressed in the document to get the paper produced and out to industry

Question: How does the wok with key management focus on substation only or on embedded systems as well?
Response: scope is not limited. TC13 is responsible for metering and therefore TG15 will provide security support for that group.

Question: Does it include DNP?
Response: there is a counterpart in IEC for DNP.

Question: Is there overlap with CSWG Design Principles group?
Response: No. There needs to be understanding of overlaps or misses. D. Thanos is the liaison between the groups.

h. ICSJWG Solutions Tech Subgroup

   i. http://www.us-cert.gov/control_systems/cscalendar.html

i. NERC cyber attack task force – no update

j. DOE-NIST-NERC Risk Management Framework

   i. Close to producing 1st draft of document

Question: any plans for their work to feed into the NERC CIP?
Response: This is a guidance document; not a normative reference nor intended for CIPs
Response: Draft out by 8/31; high-level document; organizational level risk management framework; no requirements.

k. Testing and Certification Support

   i. Sg security will not take on testing and certification
   ii. How do we align sg security work products to facilitate testing and certification?

l. SG Security Conformity

   i. group is looking at several standards
   ii. Need a good format of requirements to develop testing guidance/procedures
   iii. Structure and format of requirements
      1. [Subject][verb][object][parameters/constraints]
   iv. What does conformance/certification with a users group specification mean?
   v. Where are we feeding this work?
   vi. What is the eventual target?

Question - Do we look at other orgs that do testing and cert requirements? Sg security should not be and is not an expert in testing and cert. Who do we approach to find out what a good requirement is?

   vii. Where will the work be fed to? UCA Open SG is a users group.
   viii. UCA has a working group for 61850 and set the criteria for conformance to 61850
   ix. Number of activities around conformity in the industry right now
   x. As an int'l user groups - in Europe all about SDOs… this work would need to feed into an int'l SDOs
   xi. UCa does testing as part of 61850 part 10. uca has played certification of testers and that they are conforming to the standards and then get a cert from UCA

5. ASAP-SG Process Review & Update

   a. Review of ASAP-SG Structure and Funding
   b. AMI SP has fed into the NIST CSWG AMISEC - goal is to create a version 3 with more detail
   c. 3PDA has fed into NAESB which turned it into NAESB ESPI Req 21
   d. ASAP-SG Process Basic Steps
      i. (use slide or link to slide)
      ii. Functional requirement - yes or no

iii. Nonfunctional requirement - shades of gray
iv. Pushback from NIST AMISEC group on the failure analysis- just looks at only fails as it is intended and not malicious behavior that impacts the system…. Failure analysis looks at both pos and neg sides for both does the system do what is suppose to do and does the system not do things it is not suppose to.
v. Success guarantees - use case must complete all the way through unless there is a failure
vi. Minimal guarantees - still hold true regardless of the outcome of the use case - atm withddrawal - enter incorrect pin - get card back, no cash dispensed, and no debit to account.
vii. NESCOR Team working on failure scenarios.

F2F BC 7.18.11 Session 2

Tuesday, July 19, 2011
4:10 PM

1. Joint with SG Network
    a. Reviewed the spreadsheet that assigns CIA to the payloads identified.
    b. There were ~20 new CIA Ratings that were reviewed and accepted with little to no comment.

F2F BC 7.19.11 Session 3

Wednesday, July 20, 2011
10:47 AM

1. Joint Open Sec/Open ADR
    a. Reviewed the ASAP-SG Process for developing security profile
    b. Open ADR looking for support to help go through this process for the OpenADR use cases
    c. http://osgug.ucaiug.org/utilisec/Shared%20Documents/Presentations/SG%20Security%20F2F%20Vancouver%20-%20Day%201,%2020110718.ppt
    d. Need resources from security and business folks to step thru each case and each step in the use case
    e. 1st determine how the system operates first before
    f. Failure analysis by openADR has been done
    g. Can re-use some failure analysis and controls from other security profiles
    h. There still may be gaps for specific openADR use case failures

2. NIST AMI Sec revisiting the AMI SP in light of the of the modified ASAP-SG process (use cases and failure analysis)
    a. This work will remain with NIST AMI Sec with a review by OpenSecurity
    b. Weekly calls on Tuesdays at 1pm EST for this group
    c. All use cases are posted on the NIST Twiki

d. Review of Use Case 1 - utility sends operational command to meter - no comments or questions
e. Review of use case 2 - utility sends operational command to direct load control device.
    i. Meter may or may not be involved and is not addressed in this use case
    ii. Direct control load device connected to the AC and talks
    iii. Meter if there is just a pass-through ; not a decision maker
f. User case 3 - meter sends alarm or unsolicited/unscheduled request to utility

Question: expand use case to include what is protected from - what it should do and what it should not do. This is what the minimal guarantees is for. Over-arching concerns should be called out in the Objectives in the Security Constraints section

Question - take one use case all through the formal process including the failure analysis?
Response - take generic failures from previous Security Profiles and examine them against these use cases and determine the controls; there will be other failures specific to these use cases and develop controls for those.

g. Failure analysis is showing your homework - all the steps to get to the final answer --> justification for the security control. This is not new work - typically done in the mind to reach the justification for the security control. Ask the question why the security control is needed.

3. **Question - roles and actors are not aligned with nistir 7628?**
4. **Question - are there definitions for each of the actors? Unknown.**

F2F BC 7.19.11 Session 4

Wednesday, July 20, 2011
1:10 PM

1. Embedded Systems Security
    a. Presentation: http://osgug.ucaiug.org/utilisec/Shared%20Documents/Presentations/SG%20Security%20F2F%20Vancouver%20Embedded%20Sec%20TF%20July%202011.ppt
    b. Chairs: rohit khera, mark ward
    c. Biweekly calls - wed 10am pst
    d. Reviewed security profile for components
    e. Reorg of the task force
    f. Device Security:
        i. Crypto hardware
        ii. Random number generator
        iii. Device identity
        iv. Secure Protocols
    g. Device Authen and access contorl
    h. Key management
    i. Device Security Management
        i. Device management - looking for a primary owner for this subgroup

ii. Miscellaneous
iii. Ciphers

j. Device Robustness and Resilence

Question: Are these areas defined?
Response: Look to the Charter for a description though does not call these groups out individually; refer to the organizational slides shown by Rohit.

k. True Random Number Generation

Standards do exist.	German Federal Office for Info Security - AIS 31 Class P1 - less sensitive Class P2 - highly sensitive	True Random number generation not covered by FIPS 140-2, NIST 800-90 (these are for deterministic random number generator)

Question: where does device entropy fit into all of this?
Response: Part of the challenge process.

Question: Seed the random generator many ways. Why was the acoustic method chosen?
Response: Any analog signal can be use and in a random way.

Question: GAP in the NIST and SGIP. Does this feed into the NIST groups?
Response: If it is a gap, then need to raise awareness to the NIST design and Principles group. Reformat so that it can be handed off the group without much explanation

Question: Does this pull from other spaces? Defense?
Response: Exists anywhere there are embedded devices that is making its own keys

Question: Has this been resolved elsewhere or is the group trying to resolve a novel problem?
Response: some has been vetted out in the Smart Card Industry standards. Take is back to the broader group for further information.
Response: If a novel problem, then need to reach out for assistance. If not, then pull lessons learned from other spaces. If the former, there is a concern that this may be beyond the scope of OpenSG Security.

l. Performance Numbers

i. Mocana provides some information on this for several algorithms
ii. www.Mocana.com/nanocrypto-performance-metric/
iii. Need to be careful about recommending a subset primitives. The NISTIR gives lots of options for primitives.

m. Secure MCUs

n. Device Robustness and Resilience

i. Hardware principles
ii. NICS

iii. CPU Resource Conservation
iv. Memory and Storage Conservation
v. Battery and Power Conservation
vi. Continued Operation Under Adverse Conditions

Question: Concern that trying to protect a fly against a fly swatter - very difficult to do
Response: There are other embedded devices in the network space that does provide protection against some of these attacks.
Response: at least provide for notification by device when under attack

Question: Is there a FIPS 140-4?
Response: The numeration is around the validation of the crypto.
Response: 2nd motion for a last gasp notification when under attack or heartbeat notices
Response: Covered by device management in security events may be a the place to cover this.
Response: Prioritization of messages needs to be considered.
Response: Still need to protect because hacker could stop the notification mechanism

2. Device Management
    a. Conversation is focused on what device types are out there in the landscape
    b. Management of firmware updates, device settings, data storage, etc.
    c. Challenged by legacy device vs. "green field" dilemma
    d. Might be cheaper to swap the device vs. rolling a truck to update/fix

3. Secure Protocols - to provide guidance on the performance characterization, implementation guidelines, pki/key mgmt integration of secure protocols
    a. IP Based - d/tls, ipsec, ssh
    b. Authentication - radius/diameter, eap/pana, ldap, kerberos,multicast
    c. Non Ip Based - dnp secure authentication, aga-12, ieee p1711, eap, wpa2
    d. Other - xmpp

    Question: there is overlap with WG 15 work - the groups should sync up. POC of Herb Falk with SISCO.

    Question: PANA does not exist, no foothold. EAP is the choice by far. Both have issue with mesh network

    Question: What is the intent of this work?
    Response: Start out with a set of prevalent protocols in the IETF.
    Response: Trying to provide real world impact of these protocols. Start with what you know and do not declare winners or losers. Keep a running list of protocols.
    Response: This is around guidance and provide objective performance impacts of these protocols on embedded devices

4. Call for Action: More Utility participation!!

F2F BC 7.19.11 Session 5

Wednesday, July 20, 2011
4:01 PM

1. Usability Analysis Task Force
    a. Presentation: http://osgug.ucaiug.org/utilisec/Shared%20Documents/Presentations/SG%20Security%20F2F%20Vancouver%20Usability%20Analysis%20Task%20Force%20Update%2020110720a.ppt

2. DMS SP
    a. 2nd comment period completed; 5 sets of comments
    b. Comment resolution in progress; eta is 7/25
    c. Document to be updated based on comments; 8/5
3. WAMPAC SP
    a. 3 sets of comments
    b. Additional comments will be accepted
    c. Document review pending completion of DMS SP
    d. Comment resolution period August to September
    e. Waiting for DMS SP to be completed
4. DMS SP Discussion
    a. Commenting best practices -
    b. Proposed resolutions to address concern -
    c. Limits of comment resolution team - limited number of volunteers
    d. Discussion topics - take it to the utilisec-technical listserv
    e. Intended Use - Common comment
    f. Risk management vs. controls
    g. Suggest lifecycle and clear component definitions

Comment: ASAP-SG will produce an artifact on how to use a security profile. And, that is part of the lifecycle. Does not address the entire lifecycle. Open SG Security should look to take up the activity to create a lifecycle document.

Question: how do we spin up activity to create a lifecycle document?
Response: Usability TF should guide that work. Need additional resources added to the TF. Put out a call for participants in taking this on.

Action: teron williams and chris blask volunteered to take this on: create a general overarching lifecycle for security profiles

Question: Are Security Profiles forward looking or apply to existing legacy systems?
Response: Maybe the lifecycle addresses this, is appropriate but there needs to be a discussion among OpenSG Security
Response: Need to maintain forward looking. Need to know the endgame before addressing legacy systems - could be cheaper to replace the legacy systems.
Response: Shouldn’t lower standards to match all requirements for all devices.
Response: Support for forward looking. Drawn the line in the sand
Response: Still need guidance for legacy systems but this is the first step in defining where to go; get the endgame and delta between where you are and that endpoint; then address legacy systems.

5. Use of UML to describe Use Cases
    a. Standardize diagramming to better integrate with other OpenSG working groups
    b. Opensg security is here to support the other groups and by all means we should standardize and use the appropriate tool
    c. Several tools available to produce UML swim lanes for use cases

Action: Agreed to use UML format

6. Protection Control 21: Automated Labeling - any existing systems that do this - automatic labeling?
    a. No response… it seems this is a control that can't be implemented.

Action: Send question out to the utilisec-technical listserv
Action: Going forward, only include controls that can be implemented

7. Protection Control 41: Wireless Encryption
    a. If using tls or ipsec, why force additional encryption at link layer?
    b. Weakened access to the link layer reduces the effectiveness of a layered defense in depth approach.
    c. Link layer encryption is required for encryption for control systems to maintain control of the tunnel
    d. Protect the channel from others using it or finding a way to jump onto the channel
        i. Prevents man in the middle attacks
    e. There is a concern about network latency in that could impact time sensitive commands
    f. To protect the channel itself; also need authentication within the network - should language be modified to include this?
    g. Should explicitly state which FIPS? FIPS 140-2 instead of FIPS
    h. Should vs. Shall/Must - was changed to shall to support testing and conformity

Action: Look at the FIPS reference to determine if it should be more specific
Action: Support to leave the language as is - agreement there is a need to protect the management of the channel.
Action: Look to include in this control or in another control, language for network authentication
Action: Need to look at what FIPS certification means

8. Distinction between substation and line base devices
    a. Generalized actors
    b. Differences in controls due to location base trust
    c. Is a distinction necessary?
    d. Never trust any device - insider threat exists
    e. Exception may be Devices in Control Room - cctcv, with six-sided enclosure, badge/key cards etc.
        i. there is a distinction between that device and devices on poles or in the substation in terms of trust.
    f. Location based trust language poses an issue
    g. Location and physical controls change the level of trust of the device but still need to monitor the devices in the control center
    h. Devices may connect directly into the control center and are on a pole

Answer: Same control objectives but use different controls to protect. There is no need to modify the security profile

F2F BC 7.19.11 Session 6

Wednesday, July 20, 2011
6:33 PM

1. LEMNOS /Cybersec-Interop Project Update
    a. Presentation: http://osgug.ucaiug.org/utilisec/Shared%20Documents/Presentations/SG%20Security%20F2F%20Vancouver%20Lemnos%20Update_OpenSG_20110720.ppt

    b. Security functions and protocols
        i. Syslog - messaging
        ii. Ldap - centralize authentication
        iii. Ipsec - secure channel
        iv. Ssh - secure remote access

    c. If you choose to these protocols, this how to use them - Interoperable Configuration Profile
    d. Testing at TVA continues
    e. Lab Testing w/ Vendors at EPRI
        i. June 2011 - ipsec and syslog
        ii. Aug 2011 - ipsec, syslog, ssh,ldap
    f. Goals
        i. Reestablish relationship with OpenSG Security Cybersec-Interop TF (similar to ASAP-SG relationship with OpenSG Security)
    g. Preserve lemnos work after completion

Question: Can Lemnos provide a how to use an ICP?
Response: Can be looked at.

    h. Challenges for Cybersec-Interop
        i. Versioning of the ICPs
        ii. Certification and conformance

Roll Call
, Berkowitz, Don
, Browning, Stephen
, Craige, Robert
, Demeter, Mike
, Eswarahally, Shrinanth
, Owen, Bryan
, Ward, Mark
AEP, Greenfield, Neil
AlienVault, Blask, Chris
APS, Tolway, Rich
BC Hydro, Anderson, Ken
BC Hydro, Rogers, Mike
BC Hydro, Vandenberg, Steve
Bit Stew, Winter, Jeff
Boeing, Jones, David
BSH, Reigmeyer, Juerger
Dominion, Gerbino, Nick
DTE Energy, Ellison, Mark
Duke, Stuebing, Gary
Elster, Williams, Terron
Enernex, Brown, Bobby
Enernex, Griffin, Slade
Enernex, Smith, Brian
EPRI, Lee, Annabelle
Exelon, McGinnis, Doug
FreeScale, Dow, Mike
GE, Buckman, Adam
GraniteKey, Ahmadi, Mike
L&G, Chasko, Steve
MacAffe, Hatchell, David
Oncor, Helm, Donny
PG&E, Freund, Mark
PUC Texas, Rivaldo, Alan
Ruggedcom, Harada, Richard
S&C Electric, Khera, Rohit
SCE, Highfill, Darren
SDG&E, Lilley, John
SICO, Mackeiwicz, Ralph
SWRI, Jeirath, Nakul
Toshiba, Kanda, Mitsuru