SG Security Webinar

Monday, January 24th – 2-3pm EST

Chair: Darren Highfill
Vice-Chair: Bobby Brown
Secretary: Nick Gerbino

Agenda

1. Review Agenda / Call for Items of Business – No changes to the Agenda
2. **NEXT meeting – February 7th, 2011**
3. Old Business
    a. Subgroup updates
        i. ASAP-SG
            1. Synchrophasor Security Profile in development
                a. Have linked work into NISTIR 7628
            2. Finished facte to face interviews in Pittsburgh
            3. Start the failure analysis next
        ii. CyberSec-Interop Task Force
            1. An engineer from Toshiba sent in wide-ranging suggestions for refining the IPsec spec out on the Sharepoint site. We will be evaluating those suggested changes.
            2. Continuing to work on the white paper for syslog standardization, and the LDAP and ssh interoperability profiles.
        iii. Usability Analysis Task Force – John Lilley
            1. Third Party Data Access Security Profile
                a. finalized evaluation report
            2. Distribution Management Security Profile –
                a. consolidated comments and had initial discussions
                b. comment review to be spread across groups
                c. comments to be discussed at next meeting

        QUESTION: Any overall themes at this time?
        Response: Not yet but will share comments. Still gauging the responses

        QUESTION: Has the Distribution Management looked at identifying threat vectors?
        Response: No, that is not part of the profile.

        iv. Embedded Systems Security Task Force - Rohit
            1. 3 calls to date
            2. Defining foundational elements of embedded systems

3. Working on the Constraints Framework for class of devices – cpu, thermal limits, cost, etc.

b. Ad-hoc tasks
    i. SG Network support (C-I-A rankings)
        1. Increased communications from Ron Cunningham – coordinating between CSWG, SG NET, and SG Sec.
        2. Huge kudos to Sandy Bacik for large amount of work done behind the scenes
        3. On the spreadsheet – need to writ e the process and though process behind the rankings
            a. Request a review by SG SEC/NET.
            b. To be distributed to appropriate group

QUESTION: Is there a timeframe for getting feedback in?
Response: No timeframe; mostly being done on an ad-hoc basis, so get your comments/input in sooner than later

4. External Engagements, Business, & Issues
    a. NIST CSWG & PAPs
        i. NIST CWG AMI SEC - Review of the AMI Security Profile to make sure requirements are testable
    b. NERC CIP SDT
        i. Taking a breath to determine their next direction
        ii. Deep requests from FERC for change or issues that need to be addressed
            1. Unsure of how to proceed to address these requests
    c. IEC TC 57 WG 15
        i. Conversation about certificate management – single way to manage/reference certs across 62351 and DNP
        ii. Work going on role base access control
        iii. Emerging work on key management
        iv. Some work in synchrophasor measurements
            1. GDOI (RFC 3547) has been preliminarily selected as the key exchange protocol to build upon / extend for IEC 61850-90-5. While slightly "heavier" than some of the others considered, it also provides for additional functionality that may be of considerable use in other (future) smart grid applications.

Question: What was the IEC workaround for certificates?
Response: It is an overarching activity. 62351 have some places that specify certificates or requirements close to certificate; other places where certificates could be used but are not presently. (Aside: DNP is an enormously deployed SCADA protocol and also have need to leverage or use the functionality of certificates.) Members of IEC TC57 WG15 and the DNP Technical Committee are trying to converge and come to consensus of how to use certificates.

.

Question: Does this dovetail into the IEC 60870-6 telecom protocol (ICCP)?
Response: Not sure. Darren Highfill will follow-up with appropriate groups.
Follow-up: Yes. IEC 60870-6 is covered by IEC 62351, and therefore in-scope.

d. ICSJWG Vendor Subgroup
    i. Action item from today's meeting – reach out to all members to determine who is working with external groups
    ii. Upcoming conference is looking for abstract/papers to be submitted
        1. The Industrial Control Systems Joint Working Group (ICSJWG) 2011 Spring Conference will be held from **May 2-5, 2011**
        2. http://www.regonline.com/Register/Checkin.aspx?EventID=934568
    iii. Group to put on a workshop and speak at Smart Grid Security Summit East

5. New Business
    a. FERC Technical Conference / IEC Standards
        i. Technical Conference on Jan 31st in Washington, DC
        ii. Feedback on 5 IEC Standards recommended to FERC ?
            1. Include links
        iii. Questions FERC is looking to answer:
            1. What is industry's position on these standards?
            2. Have these standards reach industry consensus to go forward for rulemaking

    Question: What is in the security standard that is in error?
    Response: DH will not get into specifics about the standard but talks to that the standard need updating. Notes that there are technical issues with standard and would pose issue if adopted.

    Question: Why weren't these voted on by SGIP?
    Response: SGIP voting structure is relatively new and is still evolving. The point when NIST moved forward was before SGIP consensus process was completed.

    Question: What will Darren Highfill be speaking about?
    Response: What is NERC referring to about consensus process? – What was the process? It is not the process that is in place today with SGIP. 62351 have issues and what happens if it is adopted? If there are errors, how is the standard updated/managed. The entire engagement process needs to be understood – decision making process for FERC, interaction with SGIP, and the process for reviewing/revising/editing the standards going forward
    Response: How do you implement these standards or determine compliance by local governing bodies. What does adoption mean? What does consensus mean?

6. AOB
7. Roll Call
    a. Alan Rivaldo, Public Utility Commission of Texas

b. Allen Benitez, CA Public Utilities Commission
c. Bobby Brown, Enernex
d. Brian Smith, EnerNex
e. Bruce Rosenthal, SAIC
f. Daniele Loffreda, Fujitsu Network Communications
g. Doug McGinnis, Exelon
h. Gary Finco, INL
i. Gary Ragsdale, Southwest Research Institute
j. John Lilley, SDG&E, a Sempra Energy utility
k. Jose Guzman, Schweitzer Engineering Laboratories
l. Mark Ellison, DTE Energy
m. mark freund, pacific gas & electric comapny
n. Mike Ahmadi, GraniteKey LLC
o. Nakul Jeirath, Southwest Research Institute
p. Neil Greenfield, AEP
q. Nick Gerbino, Dominion Resources
r. Ricardo Lopez, Itron, Inc.
s. Rich Tolway, aps
t. Rohit Khera, PG&E
u. Sam Clements, Pacific Northwest National Laboratory
v. Sandy Bacik, EnerNex
w. Scott Palmquist, itron
x. Slade Griffin, EnerNex
y. Stephen Chasko, Landis+Gyr
z. Tam Do, Southwest Research Institute
aa. Tim DeLoach, IBM
bb. Will Arensman, Southwest Research Institute