Open SG - Teleconference 01.10.2011 Minutes

Monday, January 10, 2011
12:54 PM

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

Agenda

1. Review Agenda / Call for Items of Business – Accepted and No New Business
2. Old Business
3. Subgroup updates
    a. ASAP-SG – Darren Highfill
        1. Showed the group the Process diagram with updates
        2. How we are going to start integrating profiles into NISTIR 7628?
        3. Update to process to developing security profiles
        4. Map use cases to the use cases in 7628
        5. Map roles to the actors in the 7628
        6. Map security and operational objectives to use case security objectives in 7628
        7. DHS requirements to the NISTIR 7628 controls
            i. Have been using the DHS catalog
            ii. Extract the actor control mapping from the 7628
    b. Explained the ASAP-SG group and their goals and objectives – Bobby Brown
        1. Working on the Wide Area Situation Awareness (WAMPAC)
        2. Working with a budget of (~3 million per year)
        3. Need more contributors
        4. Looking at HAN and substation automation & DA
        5. Work very closely with NIST and their security guidance
        6. End game – to feed into the standards development with CSWG and PAP efforts
        7. IEC, IEEE, NERC, State Commissions, PUC's etc.
        8. If you would like to know more, contact Bobby@enernex.com or Darren@utilisec.org
        9. "Situational Awareness" due date is the end of February-April timeframe
        QUESTION: How do you take the NISTIR 7628 and the ASAP-SG blueprint to make a security profile?
    c. CyberSec-Interop Task Force – Dave Teunim
        1. Final Interoperability Profile from Lemnos is out on the Sharepoint site;
        2. an engineer from Toshiba will be sending in his suggestions for refining the spec within the TF by end of January
        3. Working on white paper for syslog standardization, and the LDAP and ssh interoperability profiles.
        4. The Lemnos project has been extended till January 2012, so we have plenty of time to work the issues in the TF
    d. Usability Analysis Task Force – John Liley
        1. Working on the Charter - Complete

2. Evaluation Criteria – Complete
3. Third party data access
    i. Completed first round
4. Started review of distribution management security profile
5. Next meeting 1/24
6. Meet every 2 weeks

e. Embedded Systems Security Task Force – Rohit and Daniel

1. Are working on a charter
    i. Currently do have something they are happy with
2. Device management and robustness
3. How much resistance without compromises functionality
4. Working on broadening participation in the group
5. Need hardware manufacturers, automation control devices, etc.
6. Meetings are being held Wed every 2 weeks
    i. May need to move meetings based on overlapping schedules

4. Ad-hoc tasks
    1. None
5. New Business
    a. FYI Discussion: IEC 62351 / DNP developments FYI Discussion: IEC 62351/DNP
        1. A lot of discussion around this standard lately
        2. Would like to discuss before FERC meeting
        3. Need to identify common issues or how we might resolve these issues
        4. We constitute the user group for this standard
        5. Not officially an international standard YET!
        6. Grant gave a brief update on the Working Group WG15 activities
            i. Originally formed with the mandate of security the IEC protocols
            ii. Including IEC 61850 & IEC8070-5, CIM (and many more)
            iii. Mandate: secure all of these protocols
            iv. End to end power system security issues
            v. 62351 parts 3, 4, 5, 6 specify requirements for these protocols
            vi. Ongoing questions on how to secure CIM
            vii. Part 7 has not been mapped yet (SNMP, DNP, detecting attacks)
            viii. Part 8, RBAC is almost ready for release
                1. Standardize roles and credentials
            ix. Have been asked to provide an overview or draft white paper
            x. An overview or reference to the NISTIR
            xi. Review the encryption algorithms references in Part 6
            xii. Concern around the encryption being used = currently specified as a symmetric algorithm, asymmetric did not meet performance objectives
            xiii. Part 6 currently has an asymmetric digital signature on every message that goes out
                1. Too much time to compute all signatures…not fast enough for a lot of these devices without accelerated crypto
                2. During the testing, they did not use ECC
                3. ECC would have to make a significant difference to make that work

4. Have been leaning towards using a keyed HMAC or symmetric algorithm (block cipher)
    1. Still working out the details (TBD)
5. Want to look at using one certificate for all of 62351 – Darren please clarify in the final notes

7. DNP Secure Authentication Mechanism – in the spirit of RBAC
    i. Would like to generate credentials using standards software
    ii. Maybe useful to have a 62351 certificate extension
    iii. A object ID has already been registered
    iv. Registered with ISO
    v. Standardizing the way credentials will be exchanges through all routing protocols

6. External Engagements, Business, & Issues
    a. NIST CSWG & PAPs
        1. AMI security subgroup is starting to get in to more technical work
        2. Use cases down to a more
        3. Need more participation
    b. NERC CIP SDT
        1. Version 4 of the standard
        2. CIP 005 – issues around remote access did not pass
    c. IEC TC 57 WG 15
        1. See above discussion
    d. ICSJWG Vendor Subgroup – Mike Ahmadi
        1. Had discussion about embedded security subgroup
        2. May make a similar group at NERC???
        3. Mike holding his second smart grid security conference
        4. www.smartgridsecurityeast.com
            i. February 28-March 2
            ii. AMI Security workshop
            iii. Should be some very good SmartGrid security speakers
7. From Marianne Swanson – many thanks to her - important information regarding the FERC Technical Conference on January 31st, 2011
    a. Below are the relevant links for the FERC Technical Conference:
        1. http://www.ferc.gov/EventCalendar/EventDetails.aspx?ID=5571&CalType=%20&CalendarID=116&Date=&View=Listview
        2. http://www.ferc.gov/EventCalendar/Files/20101221145852-RM11-2-000TC.pdf
    b. Also, members of the CSWG interested in following FERC's progress in this matter should use our eLibrary system (http://elibrary.ferc.gov/idmws/search/fercgensearch.asp) and search for the docket number "RM11-2." This docket number will have the agenda once it has been finalized.
8. AOB - None
9. Roll Call

    Mike Ahmadi GraniteKey LLC

    TJ LaPorte Landis+Gyr

    Mark Ellison DTE Energy

Daniele Loffreda Fujitsu Network Communications

Allen Benitez CA Public Utilities Commission

Grant Gilchrist EnerNex

Heidi Nielsen FERC

Daniel Thanos GE

Tam Do Southwest Research Institute

Sandy Bacik EnerNex

John Lilley SDG&E, a Sempra Energy utility

Ray Palmer Federal Energy Regulatory Commission

Howard Lipson CERT, Software Engineering Institute

mark freund pacific gas & electric

Dennis Gray Arizona Public Service

Nakul Jeirath Southwest Research Institute

Ward Pyles Southern Co

Doug McGinnis Exelon

Ricardo Lopez Itron

Roger Delight Pacific Gas and Electric Co.

Slade G EnerNex

Alan Rivaldo Public Utility Commission of Texas

Neil Greenfield AEP