SG Security Webinar

Monday, August 2nd – 2-3pm EDT

Chair: Darren Highfill (*not present)*
Vice-Chair: Matt Carpenter (present)
Secretary: Bobby Brown (present)

Agenda

1. Review Agenda / Call for Items of Business
2. Old Business
    a. SG Network support -
    b. OpenHAN support – had discussions around authentication, cryptography, certificates, root of trusts, etc.
    Mike: Seems to fall out of scope, but asking where is root of trust in the scope? Think this is one of the first things we need to establish.
    Matt: Agreed. Need this in order to have understanding for other architecture.
    Mike: Some discussions were around pure PKI. We need to understand the requirements we are specifying.

    c. Subgroup updates
        i. ASAP-SG (Bobby) – Team working on DM this week in face-to-face.
        ii. CyberSec-Interop – Dave (not present)
        iii. Usability Analysis (3PDA SP review) – John Lilley – met last week. Scott Palmquist is Secretary. Task Force was approved at last face-to-face. Meetings are alternate meeting times from SG Security (e.g., next week). If interested please contact John (jlilley@sempra.com). Will start working on 3PDA and are reviewing the profile. Don't have ETA for comment review and feedback yet. If want to send in comments please forward to John.
        iv. Network Security – Slade & Vincent. At face-to-face had several members interested. Currently working to finalize the charter and continue to get input on vision for this group. Want to
        Comment: What do you mean by network security?
        Slade: Example is network security architecture. Another is DHS controls aren't necessarily actionable and would like to refine these into being well defined using a common language.
        Comment: Would like to talk in terms of network requirements in terms of security. Example, an RF mesh has aspects that may make it difficult to carry out certain security functions. Some things are dependent on the network.

Slade: May need to rethink the name based on what group is undertaking.

d. F2F Review
    i. Map Security Profiles to national/SDO documents
        1. NISTIR
            a. Comparison of mapping tables – Security Profiles mapped to documents such as NIST-IR. Discussed how this would look (matrix, line-by-line, etc.).
               The original NIST-IR included the AMI Security Profile and has become a pointer reference.
            b. Line-by-line diff of controls – This would be a mapping to a sub-component of the NIST-IR.
            c. How would an organization use the NISTIR in conjunction with the SPs? – Give guidance on how to use the documents together.

               Mike Ahmadi: Annabelle had stated that the NIST-IR 7628 is not intended to be prescriptive. Not NIST's purpose for detailed requirements. It is the utilities and PUCs to determine the requirements.
               Matt: Had rejected the idea of direct mapping because the documents are separate levels. Need to address how to influence utilities and PUCs with proper guidance. ASAP-SG has had difficulty with being vendor-agnostic and specific at the same time.
               Mike: Example is the healthcare industry where they aren't prescriptive in security requirements, but there are fines associated with not being compliant.

               Mike: *Having a Smart Grid Security Conference next week. Please contact mike@granitekey.com to attend (free) – Tuesday and Wednesday of next week.*

        2. NERC CIP – The question was raised at the face-to-face, should we work on existing CIPs or look at upcoming CIPs?
           When CIP 10 and 11 were released there were over 900 comments – this has delayed the release.
            a. Resuscitate old AMI-SEC risk assessment
                i. Compare to CIP-010
                ii. Merge in current ASAP-SG failure analysis
            b. Map controls to CIP-003 through CIP-009
    ii. 3PDA SP

1. Review, Revise, Ratify – John Lilley's group. Please contact him for participation in this effort.
2. Extend to cover OpenADR – This not currently in scope for review team.

iii. SG Network support
1. Convene Network Security TF?

iv. DM SP
1. Review, Revise, Ratify

v. CyberSec-Interop
1. Review SYSLOG work – In the Lemnos project are looking at payload and standardize on the nomenclature used. So that a log event would present the same. The other issues being addressed are using IPSEC to tunnel between two end-points; LDAP; and SSH. Looking at how to use it, not when to use it.

vi. Vulnerability handling / responsible disclosure
1. Development of requirements / input / industry perspective – This may be handled by the new NESCO group.

Matt - Researchers over the last week Alex Sutteroff, Daino Disovi, Charlie Miller have issued a press release to other researchers to stop giving away the discovered bugs for free. This undervalues the work being done. They are hoping to bring a stop to this practice.

In a past case a vulnerability was found and the researcher notified the company and asked the company to be paid for the work done. He was labeled an extortionist. This particular issue was not handled well. He threatened to publish for free if they did not want to publish.

Matt - There is concern around the lack of funding for security research.

Katherine – if the researcher approaches the company in the wrong manner then is counterproductive.

Matt – Communication needs to be handled well. Researchers are addressing how to get paid and address the communication issues.

Mike – Believe researchers should get paid for the work they do. Think that it means work may go to highest bidder.

Matt – The next step need to be contact vendors; instead of vulnerabilities being purchasing on-line.

Mike – Concern is around terrorist organizations purchasing up these vulnerabilities.

Matt – a subscriber-based research to perform security analysis and have NDAs in place and allow results to validated utilities and vendors.

Bobby – what about other researchers?

Comment – what about an independent that wants to get paid and use this method.

Matt – would contract through InGuardians.

Comment – clear is to what the cost is when someone willing to pay; but what is not clear is when someone is not willing to pay.

Matt – is incentive to pay, but won't cover everything.

Ward – what are we looking to get out of this discussion for SG Security?

Matt – just brainstorming and develop

vii. Evangelism
    1. Develop collateral supporting need for security (vs. ROI approach)
    2. Demonstration of before/after for AMI SP

viii. Evidence (artifacts) of performance of secure practices
    1. Maturity model

3. New Business
4. External Engagements, Business, & Issues
    a. CSWG
        i. Annabelle has left the building – Annabelle left NIST and is being hired into FERC. Maryanne Swanson is taking the lead at NIST. Maryanne has asked each of the subgroups to review their sections. There seems to be a change in approach.

        ii. Potentially significant changes to be made to the NISTIR
        Sandy – The clarification being requested are driven from NIST management and requesting review of current activities and related NIST-IR 7628 sections. From subgroup perspective there is no changes in the near future.
5. AOB
6. Roll Call