SG Security Meeting Minutes – Face-to-Face Detroit

July 20, 2010

Chair: Darren Highfill (SCE / Saker Systems)
Vice-chair: Matt Carpenter (Consumers / InGuardians)
Secretary: Bobby Brown (Consumers / EnerNex)

Intro and Status Updates

The Chair asked if there is interest in establishing risk assessment for AMI-Sec. The question posed to whether the same group or a third-party should compose that document (John Schwartz/ Digi). The Chair responded that it may be difficult to get the funding. Matt suggested evangelizing the effort at other conferences. Suggestion was made to set up a live lab that would show the controls in place and the value. Darren proposed starting a thread on UtiliSec-technical about how to advance the adoption of the AMI-Sec profile.

A member asked if the task force meets separately from SG Security. Currently it does not.

Someone asked if AMI covered anything except the meter.

Dave Teumim, CyberSec-InterOp Chair, gave a status update and objectives for this face-to-face.

For the SG Network effort it was suggested that we capture the rules of thumb for the CIA ranking standardization.

Objectives

SG Network Security Status Updates (Slade Griffin)

Objectives for this meeting:

- Support relationships with other OpenSG WG & TF
    - SG Network
    - Other OpenSG
    - SGIP
- (see slides for remainder.. skipped to next slide for time sake)

ASAP-SG

Summary of work – Utility-driven with DOE matching funds. AMI Security Profile is a result of this work over the last year and has a version 2. ASAP-SG has accelerated the work of these requirements and standards. Have developed AMI, Third-party Data Access Security Profiles and are completing Distribution Management (DM).

Distribution Management is current profile being completed and covers controllers, reclosers, relays, capacitor banks, etc.

Scope:

From utility end to distribution substation fence. Exceptions – substation feeder breakers, volt/var control application equipment (on-load tap changers, voltage, etc.)

Q: What about edge devices interacting with DM?

Chair: Yes, this is in scope for customer devices that interact with DM.

Q: are you talking about load control at residence?

Chair: Yes, if it deals with direct load control.

Q: Physical security is that included?

Chair: Physical security for substation is not. ASAP-SG covers logical security, but there are certain physical security where needed, but does not take a "guards, gates and guns" approach.

Q: Do you anticipate will work with timing of NERC CIP?

A: We have met with NERC CIP standards drafting team. There were questions about our process. Distribution is out of their scope right now, but the question is being asked at a national level.

John Lilley: Does profile include communications requirements?

Chair: It does talk some about the communications.

DM SP Scope – Applications – 3 families – Distribution Protection and configuration management – how do settings on equipment; Distribution System Management and Optimization is more about tweaking the system – fine tuning and tweaking the power system so that it operates within defined range; Distribution System Monitoring – help understand what the state of the system is in

NIST High-level Architecture mapping – can see operations, distribution in the diagram (see slide). The group took the high-level architecture and produced informative guidance.

The cope for normative guidance is Distribution Ops, Customer and Distribution (see slide).

Scoping examples:

Distribution Ops – outage management, mobile workforce management, etc.

(See slide for other scoping)

Technical Process (Refer to slide that describes the technical process)

Problem space – we went out and interviewed utilities.

Problem refinement

The ASAP-SG team normalized actors and roles to develop Normalized Use Cases; mapped the concrete applications to real world applications.

From the Normalized use cases we identified failures through a Failure Analysis Process.

Controls and Measures – We used DHS as inspiration and make sure we had coverage and did not do a mapping or minor edit of the DHS. The purpose was to make more actionable, prescriptive controls. Controls are more succinct and consolidated many controls. If it was general security best practice then we made reference to those controls, but did not include them. We included organizational controls, and have both technical and process controls.

Convergence – pulls it all together.

Abstract Architecture – The group developed an abstract architecture. For example in Field Deployed a device may possess all three roles (Application, Actuator and Sensor). We made where a component can be separated into multiple components to serve the roles. The arrows represent the 'primary' flow of information.

Q: Does the profile take into the resiliency of the DM?

Chair: Yes, will cover more.

Use Cases:

The group wrote their own use cases. Use cases do not have security identified on them, but are used to identify where security controls are needed. For example "Use Case 12: Control Authority processes command for actuator." Chair walks through the use case steps and roles. The team developed about 15 use cases to describe the interaction between roles in architecture.

The Bottom Line:

Controls are mapped against Roles; and Roles activities are identified in the Use Cases. Failure Analysis feed directly into the control development and understanding of failures for each Use Case.

Control Mapping table:

This table maps controls to: defense in depth (life cycle) categories, roles, failures

Network Segmentation:

From a system architecture standpoint the group has provided guidance for network segmentation. Segments in the private network are DM Control Systems Server, DM Field Network and DM Control Systems User Network. These systems cannot directly connect to each other. The Private Networks are segmented from the Public Networks.

Q: What if you are not doing this today?

Chair: We offered this as the way security should be done. You will not be in compliance with this profile if you do not follow, but if you want to be more secure then this is the way segmentation should be done.

Boundary Controls:

The chair showed example boundary controls developed by the group (refer to slides).

Home Area Network – We need to think how this builds on OpenHAN and drill down from a security prospective, look at trust, root hierarchy, etc.

WASA - Transmission Management (SynchroPhasor) – Has a mesh type configuration. The 2003 blackout took a long time to unravel what happened. From a consumer standpoint we think that when the lights go out is a black out – but it isn't necessarily – usually a service interruption; but when the grid is an unusual state and impacts in major outages. If we had had visibility (WASA) we would have been able to prevent the 2003 blackout.

The 2003 blackout was due to exceeding operating limits and having an event occur to reroute power demand – causing rolling blackout.

NASAPInet (North American SynchroPhasor Initiative) – There are two tiers of PMU information – 1) local to the local utility and 2) neighboring utilities (subset of information). Neighbors need lower level of visibility to foresee an event that is about to happen.

SG Network Joint Meeting

Matt Gilmore – SG Network Chair

CIA ranking feedback:

- There are about 1,400+ new requirements and CIA requirements that will need to be done 880 have been complete, but likely need review
- Darren: Would like to establish the process and define CIA

Reference: SG Network >Shared Documents > Interim Release 4 > Diagrams

SG Network took the NIST conceptual model and extended into real deployments with utilities. They mapped interfaces between components on the model. There is much more information added on the latest version. There are several more information flows defined – there are many ways information can flow (e.g., field network, AMI network, etc.). There will be requirements for every conceivable path. Hopefully there will be some of the same CIA level based on information.

Comment: Some say that the CIA was based on the logical network. If the data crossed a separate network then the CIA level would (possibly) change.

Matt Gillmore: It's important to look at each payload individually. Propose that through the next layer of mapping can do by domain and break into domains – e.g., AMI, DM, etc.

Darren: From a security standpoint folks will divide work.

Darren: Issues that were identified with assigning CIA.

"CIA feedback on v30 draft 2" file was shown. In columns QRS show the original CIA assessment. Columns WXY show the results of SG Security's assessment of CIA.

Comment: Can look at SP800-60 as an example of using the CIA classifications to show the justification for the selection of High, Moderate, Low. Use this as a model, not as-is. This will be used to determine what security is needed.

Comment: based on what made up payload could identify CIA level. For the same payload it was the same CIA.

Ron Cunningham: there are several paths that the same payload can take. The same payload would have the same CIA values. The CIA categories change depending on the network it traverses.

Comment: The path that the payload takes doesn't matter as much as the payload CIA identification.

Comment: If a payload has a High for Integrity you don't let it traverse a system with a Medium or Low Integrity identification.

Actions:

1) SG Network will document in the SRS payload attributes; i.e. textual attributes.
2) SG Security will identify the C-I-A on the payload (approximately 175 identified payloads) and identify the justification for each classification of C, I and A for each payload.
3) SG Security and SG Network will assign controls and mitigation measures to individual interfaces

Interface #x	**Confidentiality**	**Integrity**	**Availability**
High	[controls]	[controls]	[controls]
Medium	[controls]	[controls]	[controls]
Low	[controls]	[controls]	[controls]

4) Identify the payloads across each interface and establish high-water mark. Based on high-water mark identify controls necessary to meet or exceed the CIA identification.

Vulnerability Handling Discussion – Ralph Mackiewicz (SISCO)

Chair: what does a proper process for a vulnerability (discovered) look like? What are the responsibilities of the researcher, vendor, etc.

Ralph: Going to outline the issues and stimulate discussion.

For this group: Establish recommendations and policies for vulnerability handling needed for Smart Grid applications.

Disclosure – who gets to know and when?

Remediation – how are the vulnerabilities corrected?

Support

The range of options – one end everything is public immediately; the other end everything is secret indefinitely.

The generally accepted practice in IT (NIAC) – Vulnerabilities that are discovered private are kept private until remediation is available.

If detected "in the wild" are disclosed to public immediately.

Developers are expected to be diligent in pursuing remedies.

Public disclosure is common for not being prompt. Can go out and buy 0-day for a price. Look up product online.

Some "white hats" are beginning to demand payment

Public disclosure with remedy availability.

What is appropriate for Smart Grids?

Pros to early disclosure: This is the way "everyone" does it. Everyone has a right to know. Bad people already know this

Cons: Real-time operations <> general IT. Public is affected, but they are not responsible or lack capability. Sometimes systems can't be patched (updated firmware in 3 mil meters?)

Is a Little Discretion Better? (Disclosure Rules)

- Vulnerabilities with remedies are disclosed to those with a need to know. Who needs to know? DHS says asset owners. What about developers/vendors?
- If systems aren't (or can't be) fixed, does public disclosure serve a good or bad purpose more?

Is this a way to keep vendors honest?

Mitigation Issues:

- How quick must remedies be applied? Microsoft seems to be fairly quick at handling. Three months seems to be not unusual (the norm).
- What if systems have to be taken off-line? Big problem in plants.
- How serious of a problem requires replacement or on-site service or equipment? Are short outages to restart acceptable?

Support Issues:

- How about old systems?
- How many generations back must be tested, maintained and updated? Some older version are not maintained and updated? Patches are not publically being rolled out. Microsoft's support is 8 years by default and privately beyond that.

  Chair: A distribution control station at a mid-to-large size utility. What kind of changes occur over the years.

  Ralph: Most systems are not updated unless functionally. The company would hire the SCADA vendor to come in and fix. There are not many updates. But the vendor will support them indefinitely. There are customers that have software that are operating on VAX systems reliably today and they are being supported. Newer systems costs have come down on keeping systems up-to-date. They have customers now that are running on Windows 95.

  Chair: on systems being designed today, are you seeing a shorter life being designed into the products?

  Ralph: Yes. The products are costing much less too – so there is a trade-off. There is a migration cost to older systems. The hardware components (chips) don't even last that long anymore.
- Is a new version a new generation?
- Custom systems versus "shrink-wrap"/OTS?
- Home-grown systems? There are no vendors. The systems were built by the utility themselves.

Why it's important:

- Recently disclosed was involving fixed RDBMS login for a SCADA. Vuln used for industrial espionage
- Was propagated using a previously known remote code execution vulnerability via shortcuts on thumb drives even if auto-run is disabled (Exploit: W32/WormLink.A)

- First time a new zero-day vulnerability was discovered via a SCADA attack vector
- No remedy yet
- Affects ALL windows versions
- Microsoft Security Advisory (2286198)

Some Resources:

- NIST SP800 and SGIP
- NAIC Vulnerability Guidelines (now DHS)
- DoE – NSTB
- DHS – CERT ICSWG
- IEEE, IEC, ISA

DHS Activities:

- US-CERT CSSP ICSWG of DHS: http://www.us-cert.gov/control_systems/icsjwg
- Needs more direct involvement from energy sector

Discussion:

- Ralph: thinks that there should be a process that vets people for having access to information. Blackhats can work anywhere – but should at least make an attempt; would hate to see it be a government run process
- Government orgs seem to be a way off from sharing information needed to fix the problems
- Chair: Is the government lead efforts useful? I think we as a group represent vendors and utilities can guide the process. I don't think we would be the body that runs this, but the point is that we can contribute value to the space representing the industry (user) perspective. We can move quickly and feed SDOs.
- Comment: SP99 is working with FERC and NIST. Starting to bring together best practice. One thing falling short on doing background checks. Incident where employee was trying to create a chlorine leak at a chemical plant. The background check did not go far enough – he was a foreign national attempting an attack. Much of the work is starting to come together to address these issues.
- Ralph: we need customized for electrical systems; if best practices don't work – how do we deal with them? From a national security perspective I (a vendor) don't need to know because I don't

have a government security clearance. I think there is a way to do this that will help us address national security concerns and fix them.

- Chair: closing thoughts: I think there is a tremendous and increasing need from our representation of stakeholders in the industry. Seeing more and more issues about vulnerabilities. The smarter the grid gets we start seeing more of these things. Is hitting the main stream media. We are positioned to provide value to this space. We can show leadership to the industry. We could form a task force for doing this, but we don't have to go through these hoops. We have the technical listserv and can use that to capture expression of requirements from a users group perspective for a system that handled and dealt with vulnerabilities. If enough interest we can create a task force. The onus is on us – a calling for us.

Usability Analysis: John Lilley (and Daniel Thanos (not present))

- Charter – is in progress. Framework discussion today.
- Pending Work – Third-party Data Access

Scope:

- Documents selected by SG Security WG are analyzed by the group and provide comments back to SG Security for the approval process. There needs to be a clear set of criteria for evaluation. Need to understand where in the risk model that falls into.

Proposed Charter:

- The UA group is founded to provide a clearly reasoned, documented, and independent process that represents all industry stakeholders when it comes to evaluating the applicability and general usability of OpenSG Security standards. This is both from an operational and technology development perspective. We will provide a report for each published standard that makes recommendations for improvements and future refinements to that end, as well as helping establish comment resolution teams and processes.
- Chair: Participation will allow to get comment in early and see product in earlier stage
- Chair: We have the criteria met to instatiate the UA TF.
- Motion made to instantiate the UA Task Force by Robert Former; David Tumim second. Floor opened for questions – no questions.

  Resolution: vote made a passed to create the Usability Analysis Task Force.

Criteria Areas:

- Mappings – requirements and use cases
- Lifecycle
- Procurement
- Security Levels
- Component
- System

Possible Gaps and Issues:

- Completed Risk Assessment – would be nice to look at a failed control to see where in risk assessment
- System/Security Architecture
- Others?

Members to date:

- All volunteers, looking for representatives directly impacted by each document. May get something hardware based, software based, etc. several different systems that have to look at. General idea is to participate in something that can contribute to.
- Current roster – Daniel, John, Mark Freund

Proposed meeting time:

- Alternate Mondays with SG Security WG
- Next Meeting, 2-3 PM ET, 7/26

Action Items:

- Charter completion
- Define analysis criteria
- Identify gaps related to analysis context
- Third Party Data Access review – impacts utilities, hosting parties, vendors, data custodians, billing companies, regulators, customer advocates. Touches into the privacy area. How to give permission to data.

Contact Information:

- John Lilley, jlilley@sempra.com
- Daniel Thanos, Daniel.Thanos@ge.com

Insider Threat – Slade Griffin

What is a threat:

- Vulnerabilities, Actors, Motivation
- Threat x Probability x Impact = Risk

Insider Threat Research:

- Sources: http://www.cert.org/insider_threat
- http://Ussecurityawareness.org/highres/insieder-threat.html
- Others

Threats are easy to spot

- Jeff Moss example: works for DHS previous creator of Black Hat and Def Con

What is an insider?

- Several stories – government facilities, banks, hospitals, private companies, public companies (Fortune 5)

Policy:

- We have a policy for that
- Auditors check for existence of policies but not effectiveness
- Do people know the policies

Closing:

Insider threat hasn't been looked at closely. Think this is an area that needs lots of attention. Will be happy to demonstrate exploit of Utility Manager after presentation.

Open Discussion: Roots of Trust

Chair: need to discuss prior to OpenHAN meeting tomorrow; would like to get issues out.

Public Key Certificates:

- Relevant domain in question: HAN
- Q: How do we manage trust to and from devices in the customer premise? – Authentication of end devices. Proposal: require installation of public key certificates
- Other smart grid domains are important to keep in mind
    - How might this apply to AMI equipment?
    - Is there any overlap with DM?
    - What about other utility field-deployed assets?
- Millions of devices deployed

Who is Root?:

- Root for each "certified" technology?

  Q: What does "certified" mean?
  Comment: Edge Conformity group is working on requirements and definition for this.

    - How is technology certified?
    - Do we allow uncertified technologies? What impact does this have on innovation?
    - What happens to end-to-end security when an application has to cross technological boundaries?
- Root for each application?
    - Who determines who is trusted and who is not? How are "white lists" generated> How are they maintained?
    - Varying MAC and PHY – does this prevent/inhibit the use of gateways and force devices to act only as a router?

Comment: the edge conformity group is developing the requirements for private certificates being issued (testing).

Suppose that device has a pre-installed public-private key pair. What happens when trying to send a message across multiple technologies – differing CAs with each device?

July 21, 2010

NERC CIP SDT – Coordination

- SDT working on version 4 of CIP Standards

- Changes include moving to Risk assessment approach
- Original intent – develop CIP-010 to replace CIP-002 and CIP-011 to replace CIP-003 thru 009
    - 010 – looks at what makes something a high, medium or low – process for risk assessment
    - They have gotten 900 comments back from industry from the draft
    - Industry is really concerned. There is $1M per incident per day fine – there is a lot on the line to make sure can meet standard (regulations).
    - RA based means more context sensitive – more interpretation in the mix. Fewer places to see how dealt with elsewhere.
    - Other industry regulations have years and years of interpretation – there is more uncertainty for initial releases on how regulation will be dealt with. This is understandable.
- Concern CIP-010 and 011 may not pass by EOY
    - There is pressure to get something out this year by the NERC SDT
    - There is concern that these will not be accepted/passed this year
- Current (interim) plan: Take High and Medium bright lines from CIP 010 and merge into CIP 002
    - This would allow to get something out this year and continue development of CIP 010 and 011
    - This is subject to change and the Chairs interpretation of where things are going now
- NERC SDT / ASAP-SG joint Meeting in Pittsburgh
    - Previewed ASAP-SG DM SP (during lunch & learn session)
    - Strong engagement and interest, positive response – looking to collaborate and coordinate going forward
    - Need to perform analysis of CIP requirements against DM SP controls
    - The SDT is very interested in the WASA/SychroPhasor security profiles on the agenda for ASAP-SG to develop; also interested in the current DM
    - As a result – need to do analysis (differences) and see if there is anything they are requiring that we don't have in the ASAP-SG profiles. Expect that the profiles that the ASAP-SG develop will be more aggressive than the CIPs. The profiles are best guidance

that are being developed now – and trying to avoid watering down the requirements needed to secure Smart Grid systems

- Need to paint a clear picture of how these bodies of work complement each other
- Looking to possibly have NERC SDT join us in November FPL Juno Beach face-to-face
- Sharron Edwards: The next version of the CIP-002 will just have an extension. The NERC CIP standards provide the "what" and tell what to do for mandatory compliance. The ASAP-SG profiles give the "how" and help align. She saw a real value in what is going out to the industry in these efforts
- The "what" and "how" show how these efforts complement each other
- Will actively seek to coordinate with NERC and provide service to the SDT. Will provide analysis and input to NERC SDT
- Sharron: Would be good to get the CIP leads involved and setup contact points for the analysis
- There is a need to do the mapping between the SG Security WG Security Profiles and the CIP Regulations. We (SG Security) could do the legwork
- Sharron: this would help work on this in smaller teams (current team is about 30 members)

Cyber Security Interop – Dave Teumim

Background:

- Designated as SG Security WG at last face-to-face
- Spinoff from DOE NSTB Lemnos
- Lemnos Partners: EnerNex (Prime Contractor), TVA (Utility), SNL (FFRDC), SEL (Vendor)
- Lemnos develops *Interoperable Configuration Profiles* for widely accepted Internet Protocols
    - Looking to hand these over and become OpenSG SG Security documents
    - It is the hope that they documents and effort will live on beyond the Lemnos project within the SG Security
- These Interoperable Configuration

Goals:

- Get organized – Secretary, Charter, Listserv, have first meeting (have accomplished)

Interoperable Configuration Profile for IPSec – Draft Specification ver. 3 (Joe McCormick/ Data Track)

- Use ESP (Encapsulating Security Payload)
- Use Tunnel mode
- Use HMAC
- Use IKE v. 1 (moving to ver 2 in 2011)
- Use DH-5
- Configuration parameters (e.g., ike_life: 10800s; ipsec_life: 3600s)
- The person setting up is given specific instructions on how to setup; it is not expected that the person doing the VPN setup is a technician
- At DistribuTECH this was shown to work effectively
- These systems will need Tunnel/VPN technology; there is going to be need for QoS technology

Proposed Tasks/Goals for TF

- Provide review and feedback on Lemnos 2010-2011 Interoperable Configuration Profiles:
    - Syslog standardization input (RFC 3164 and RFC 5424 (more flexibility)) – inter-process, inter-thread
    - LDAP
    - SSH
- Technical feedback subgroup to the Lemnos Team and Participating Vendors
- Member: is this group part of the Conformity WG?
- Dave: working with Bruce Muschlitz to see how to interact; will be attending Security Conformity group tomorrow; discussing setting up test harnesses, etc.
- Other suggestions?
- Invite participation from SG Security for the Task Force and form a technical feedback group and help with Syslog standardization; one task will be to help formulate structured Syslog as it is manifest in RFC 5424; Sign-up sheet is being passed around; Need members with: Crypto, Syslog experience and specification and writing experience

Discussion:

- Where might this be applied after Lemnos is de-funded? Soliciting ideas. What could this evolve to?
- DOE and utilities talked about Lemnos and talked that this type of endeavor was essential so that solutions could be deployed.
- Part of the Open SG – SG Security goal is to feed into SDOs; The documents will likely be reviewed and ratified within this group; these profile help people implement the standards
- Frances: WG 15 has standards that reference other standards; They spell out parameters for use of other standards; This is framing the requirements for use in the utility industry; if IETF is not going to pick this up then could become another IEC 62351 Part. An example is TLS under 62351
- Dave: We were shopping around for a group that would accept us. The UCA is a group that accepted us and was willing to work with us. No one has taken on this effort and is a bit of the grunt work
- Frances: This is important and seems basic, but is really needed
- Dave: Example: a company stated have logs from all around the world without UTC timestamp. Need this kind of standardization
- Dave: The UCA approach works fast by getting vendors, utilities, consultants and government orgs working together.
- Frances: This is the way the IEC work can get done via the liaison status with SG Security

---

SG Network Security TF – Slade Griffin/Enernex and Vincent Bemmel/Trilliant

- Exploring the justification and development of Security around Network Security
- Would like to have a system wide view

Proposed Charter:

- Focus on Smart Grid network security topics; working closely with SG-Network TF
- Address SG-Security network-related items
- Identify best practices
- Establish a common framework / language

- Identify actionable requirements
- Engage with the SGIP CSWG on network security
- Add value / avoid duplicate efforts

OpenSG focus areas

- SG-Sec
- SG-Communications
- SG-Systems
    - OpenHAN network security topics

SG-Sec – SGIP

- Flesh out ASAP-SG / NISTIR 7628 / CSWG high-level requirements re: network security

SG-NET Security:

- Continue work beyond CIA mapping (e.g., recommendations for 3x3 CIA/HML controls at SG interface
- Additional OpenSG network sec topics
    - Include in SRS

Best Practices Guide

- Produce Best Practices guideline to SG security – see where can use existing best practices, see which ones don't want to use and
- Separate document?

Common Language:

- Establishing common language requirements
- Confidentiality – Encryption, FIPS 140-2, Integrity – Digital Signatures, FIPS 186, etc.
- Can specify the common best way to do things; understand the ways not to do things
- Looking to make things like the DHS documents more actionable, guidance

Actionable Requirements:

- Looking to do the "How" beyond the "what" that many standards specify

- Example: taking DHS controls and mapping to network security best practices and getting into the “how”

Discussion:

- TF?, Group Interest?, Volunteers?, Other topics?, Next steps?
- Chair: would you see potential for controls writing and revising feeding into 3x3 matrix?
- Slade: If we had these controls established then would make easier to do work vs. looking to match and lookup several standards
- Comment: This group will have lots of work to do, but how to we avoid becoming over prescriptive?
- Chair: Not sure how to answer. We have a spectrum, but think we are at the loose end of the spectrum and think we are not prescriptive enough to know the “how”.
- Comment: there are lots of “what” out there but not much “how”
- Chair: As a user’s group we have been aggressive in trying to define how systems are built and I think we keep in mind how we move forward in keeping innovation. We would look for vendor pushback where getting too prescriptive. We would be looking for a group of vendors
- Slade: would be looking for the consortium to vet work; if we go down best practice guideline – if can’t comply with guideline then write down why for audit situation
- Comment: We are so far down the other end of the loose-end of the scale that there is not much concern of vendor lock-in
- Comment: As a vendor, we are not in danger of being over prescriptive. We are looking for more prescriptive guidance and don’t see it as a stumbling block
- Chair: Need to get charter into a written format and need to get a utility representative
- Chair: would like to talk about this group and prioritization of work at end of session

---

OpenHAN & SG Security

Agenda:

- Is the document ready for release? Have we adequately addressed security for the current industry environment? Any security issues remaining?
- Issues: 1)Threat model, 2) Certificate and Roots

Threat Model:

- Proposal (Robert Cragie): Compliment impact assessment in HAN SRS Appendix with a trheat model
    - Type of devices which may be potential targets for compromise*
        - Any device on the HAN with firmware (where can be uploaded/replaced) is a problem (commissioned/registered)
        - Matt: like concentric circles of privilege escalation – from outside non-commissioned device, but could find a way to be commissioned (threat increases – public info access), once commissioned then can find way to get registered (threat increases – private information access), then find way to established enrolled state (two-way communication)
        - Comment: need to focus on the “registered”
        - Comment: What devices are more attractive targets? Example, PEV where have large load and advantages to compromise
        - Targets (logical devices):
            - All logical HAN devices types (listed in table 1 page 36)
        - *The above bullets turn into a table where the subsequent bullets are answered for the type of devices in the first bullet
        - Darren: We need one person to lead this effort. Otherwise need to push this off to a later version of the document.
        - Comment: would recommend that use a reference document, like NIST, as a common language
    - Environment for each device
    - Ingress points on a device
    - Potential adversaries
    - Potential attacks
    - Motivations for an attack
    - Manifestation of an attack on a device
    - Scaling of attacks (attacking many devices using the same fundamental attack, e.g., drive-by attack)

Robert Cragie: Take this assessment and apply to the Use Cases.

Augmented Impact Assessment:

- Proposal (Robert Cragie): Extend the existing impact assessment in the HAN SRS Appendix
    - Impact of an attack on a device itself (in what way the device becomes compromised)
    - Impact of an attack on a device's environment
    - Impact of an attack on the system
    - Severity of resulting compromise due to an attack
    - Operational mitigation based on one or more compromised devices

Chair: if this is dependant on the threat model and other work, then we need to table for the next version.

RESOLUTION: Recommend that we table this until next version of the OpenHAN document.

Darren: Can we get Threat Model and Augmented Impact Assessment done within a week?

Mary: I think we see what we can get done today and we can work the rest out in future versions. We can put in an appendix. It will not be a deal stopper if we miss some things.

Darren: I think we can work from the primary issues and capture a few thoughts and be productive.

Darren: Can the device impose a threat to the system? Trying to determine what things are a threat.

Certificates and Root Certificate Authorities – Proposal (GraniteKey):

- 1. A mechanism to set the root(s) of trust for mutual authentication is required – and must be clearly defined
- 2. Any entity issuing identity must clearly document their policy for issuing identity and how the root is used to provide the credentials
- 3. A trust chain for delegation should be allowed:
    - It should contain no more than 1 level
    - "Sub-roots" do not need to be secured and are generally presented during the authentication sequence
- 4. Meter (for authenticating HAN devices)

    - The utility (or meter mfg.) identifies which vendors are authorized to connect ot the HAN via the ESI and thus which roots will be provided in the meter
    - The root(s) of trus5 are to be embedded in the meter firmware as a table…
    - Optional: The table can be updated by using same mechanism to securely update the firmware
- 5. HAN (for authenticating the meter)
    - The consumer device mfg. indentifies which meters or utilities are valid to connect…
    - The root(s)…
- Robert: Have looked at this in Zigbee and have two certificate – a mfg. certificate (has a lifetime) and an operational certificate (dynamic and has lifetime). Have two tier CA. The operational certificate is self-signed by the ESI. The root would be the ESI itself and the head-end would participate as well.
- Darren/Matt: Who is the root of trust. If we can't figure out the root of trust then we can't talk about secure PKI.
- Matt: What is to be gained?
- Kirk: we have to be careful because this is fluid and there are several different implementations
- Darren: Trying to determine if any discussion in a root CA helpful in the document? We have a specific proposal on the slides.
- Paul: The infrastructure, example Zigbee, where Zigbee would be the root of trust. Cable did not protect the certificates, but we should do better at this.
- Darren: Cable and HAN market are different. We are trying to create a rich eco system around the HAN for the energy market. Don't see a one-to-one with the cable market.
- Paul: This sounds like a cost issue. The only way to secure is a certificate-based solution.
- Robert: There is a model already using certificates and mutual authentication and running on low-cost devices.
- Paul: disagree that cost is an issue and believe the cable market translates
- Darren: concern about being able to get this into a wide variety of devices. Like a cable card that can't get from anyone except my cable company. See a difference with getting authenticating to cable company vs. utility.

- Robert: look from a requirements point of view from HAN device to HAN device like PKI, symmetric key… to some extent can look at from an SRS point of view (high-level). Would argue that certificate based is less of a geek/sophisticated method to understand.
- Nathan Ota: Understand that have mechanism to handle authentication and make configurable
- Robert: Certificates can be provisioned in the factory. The private key is confidential and public key isn't – makes distribution easier.
- Nathan: would what we have today exclude this proposal?
- Robert: would say yes.
- Comment: Security integrity is done in accordance with security policy assumes the policy will be established to handle
- Nathan: think that mutual authentication is needed for bi-directional communication. Propose that allow devices

Darren: This is not currently mentioned anywhere in the current documentation and think we need to address.

Matt C.: Root trust and push to devices. Without issuing guidance to their use is a long path down a short plank

Nate Ota: We have been focusing on the "what" and not the "how" as an approach for the writing of the document.

Darren: maybe the "what" ends up being an authentication method that says you need a root CA.

Darren: do we want to add any terminology in the security requirements for certificates without adding the "how"?

Paul: Zigbee is requiring a mutual certificate based authentication (SEP)

Comment: What about Wi-Fi?

Comment: If Wi-Fi and SEP then it will use certificates. Wi-Fi is part of the alliance

Comment: I don't think we want to compel what was said, but for the identity I think we would want to do that.

Robert: Depending on the requirements for the credentials then could depend on that; it does not mandate a user interface, etc. What credentialing information has to be in place at point of mfg.? of operation?

Matt: how do you do mutual authentication in this arena?

Robert: Authenticate on network and then as part of the program (enrollment)

Matt: how does device know who is talking to?

Chair: We are expressing security requirements to be deployed on the HAN (at the business level), like authentication credentials should be traced to the same hierarchy (root CA)

Robert: looking at mechanism to purport the identity

Matt: talking about very trusted devices, but from a technology point what does the other end look like? Going the other way many devices may not have a significant user interface that has a true

Paul: to do this you have to have it burned in at mfg.

Matt: the utility will not have this certificate

Paul: upon startup will authenticate with manufacturer; then will allow to connect to next in chain

Matt: how do we make a requirement for mutual authentication, when we have device that spits out a chain of bytes – how do we confirm

Comment: Do I need to know that I trust the person connecting the device (from a business sense)? And the device is allowed?

Paul: This is massively deployed technology. This is not new infrastructure. Example: Cable labs have millions of devices

Matt: but on a private network

Paul: irrelevant

Matt: but these aren't devices owned by the consumer

Sam: How do I know that is connecting to my home and not my neighbor's home? In Bluetooth can make a point searchable and go the other device and say find device.

…

Proposed security requirement:

The credentials for authentication of a HAN device shall be established and validated in a manner by which they can be ensured that they were issued by the Service Provider and/or manufacturer and shall be protected and updated by a mechanism that cryptographically ensures proof of origin at consistent with the mechanism used to update the firmware.

Propose modification of Security.Reg.1:

- HAN device shall support Mutual Authentication for enrolled devices and optionally support for registered devices.

Paul: this begs the issue of how the firmware is securely updated.

Comment: there are about 10 ways specified on how this can be done already.

Darren: Any issues with proposed requirement?

Justin: Propose to change Security.Integrity.16 Add "shall validate the integrity and authenticity"

Prioritization & Planning – Darren Highfill (Chair)

- Coordination with:
    - NIST CSWG – signals were crossed as how interaction would occur. We assumed would provide work products to NISC CSWG and would get incorporated into the NISTIR. This was not the full case. The NISTIR is intended to be a standalone document. If we want to show how our work interacts with the NISTIR then can do a mapping, etc.
        - OpenSG says that the SG Security should develop the mapping between the SG Security and NISTIR.
        - We can't expect that the NIST CSWG stop work and review the Security Profiles
        - There is a tentative meeting scheduled for August to meet with Annabelle and discuss coordination efforts
    - NERC CIP
- Comment: what else is on the plate for SG Security?
- Chair:
    - We are close to end of support for OpenHAN.
    - On the upslope of supporting SG Network
        - Developing Security Network TF
    - The Third-party Data Access profile has been waiting for 6 months and needs review, editing and approval
    - Soon coming is the DM SP
    - **PRIORITY ITEMS**: Need to do map Security Profiles to:

- NISTIR – **ACTION**: John Lilley to help
- Do mapping and comparison on controls since they are derived from the DHS controls in both cases (NISTIR Appendix D has mapping to DHS and NERC CIP)
- Line-by-line diff of controls

- NERC CIP – **ACTION**: Steven Chasko to lead effort
  - Resurrect the old AMI-SEC risk assessment
    - Compare to CIP-010
    - Merge in current ASAP-SG failure analysis
  - Map controls to CIP-003 through CIP-009 - **ACTION**: John Lilley to help

- Need guidance on how an organization uses the NISTIR in conjunction with the SPs?
- CyberSec-Interop:
  - Review Syslog work
- Extend Third-party Data Access to cover OpenADR
- Vulnerability Handling / responsible disclosure
  - Development of requirements, input and industry perspective
- Evangelism – **Action**: Robert Former/Itron; Steven Chasko
  - Develop a program to evangelize need for security and get past the need for ROI for security
  - Some of the other groups appear to ignore security
  - Demonstration of before/after for AMI-SEC for AMI SP (Will not be how Itron does it, but an agnostic view)
- Low Priority: Evidence of Secure Practices
  - Artifacts that show that a utility has addressed security the right way
  - Effectively a minimum bar checklist
  - Maturity model

- Chair: Am leery of waiting on the security profiles to release to start work; ASAP-SG is going to continue to release security profiles;

Next Teleconference:

- August 2nd at 2pm
- Bobby to send out meeting announcement, call in and webinar info.