Joint SG Security - OpenHAN Webinar

Monday, April 12th – 2-3:00pm EST

Chair: Darren Highfill (present)
Vice-Chair: Matt Carpenter
Secretary: Bobby Brown

Attendance

Mike Ahmadi/GraniteKey LLC
Roger Alexander/Eka Systems
Skip Ashton/Ember
Sandy Bacik/EnerNex
Vincent Bemmel/trilliant
Allen Benitez/CAPUC
Doug Brown/Pacific Gas & Electric
Julie Brown/Entergy
Kevin Brown/Enernex
Matthew Campagna/Certicom
Alvaro Cardenas/Fujitsu
Yvan Castilloux/People Power
Joseph Chiu/SCE
Anthony Cleveland/Tampa Electric
Frances Cleveland/Xanthus
Kevin Collins/Bit Stew Systems, Inc.
George Cosio/FPL
Robert Cragie/PG&E
Dave Dalva/Cisco
Steven Dougherty/IBM
Carol Fisher/Elster Solutions
Mark Freund/PG&E
Nick Gerbino/Dominion Resources
Ramprasad Golla/Grid Net
Dennis Gray/APS
Neil Greenfield/AEP
Evan Grim/Southwest Research Institute
Jason Hanna/Coincident, Inc.
James Ivers/SEI
Nakul Jeirath/Southwest Research Institute
Oliver Johnson/Tendril
Yanghwan Kim/LGE
Larry Kohrmann/Oncor
Sitaraman Lakshminarayanan/GE-Energy
Andy Laskowski/CenterPoint/IBM
Brian Lenane/SRA International
Michael Leppitsch/Gridata, Inc.
Milton Lie/Contineo Systems
John Lilley/SDG&E
Howard Lipson/CERT, SEI
Daniele Loffreda/PE Associates
Justin Lowe/PA Consulting
Zahra Makoui/PG&E
Ovace Mamnoon/HP
Doug McGinnis/Exelon
William Miller/MaCT USA
Gaylord Miyata/People Power Co.
David Mollerstuen/Tendril
Bill Muston/Oncor
Kirk Oatman/I'm in Control
Nathan Ota/Trilliant
Ward Pyles/Southern Company
Maurice Rieffel/Entergy
Louis Robinson/Constellation Energy
Brad Singletary/EnerNex
Brian Smith/EnerNex
Charlie Smith/GE
Gib Sorebo/SAIC
Charles Spirakis/google
John Teeter/People Power Company
Tom Thomassen/Symantec
Daryl Thompson/Thompson Network Consulting
Rich Tolway/Arizona Public Service
Javier Torres/IBM Corp
Michel Veillette/Trilliant Networks
Terron Williams/Elster
Andrew Wright/N-Dimension Solutions

Agenda

1. Review Agenda / Call for Items of Business
2. Old Business
    a. Perspectives and Insights
        i. Call for presenters and suggested topics
        ii. Submit name & ideas to SG Security leadership (Chair, V.C., Sec'y)
    b. SG Security Charter
        - *The SG Security Charter has been approved by the OpenSG Technical Committee.*
    c. Subgroup updates
        i. AMI Security Profile revisions
            - *Ido Dubrawski taking over for Sandy Bacik*
        ii. Third Party Data Access Security Profile review
            - *Ram from GE to head up the effort on 3PDA review*
        iii. SGSec-Risk
        iv. Lemnos
            - *Brian Smith – A "Lemnos" folder created on the SG Security WG SharePoint. The Lemnos project team currently working with DOE on contract extension and hope to provide further technical details at the next F2F meeting.*
        v. Any other active subgroups?
    d. OpenHAN
        - *Details of technical discussion on Google's comments to OpenHAN 2.0 are found at the end of this document.*
        i. Working toward OpenHAN 2.0 spec
        ii. Looking for input/discussion with SG Security
        iii. Schedule

Date	**Activity**
March 22	v1.91 available for comment
April 2	Comments on v1.91 due
April 5-23	Document editing team to review comments
April 26	v1.92 available for comment
May 3-6	OpenSG F2F meeting in D.C. Review OpenHAN v1.92 in OpenHAN work sessions
May 14	v1.93 available for comment
May 21	Final comments due
May 25	OpenHAN TF to vote on OpenHAN 2.0 document

        iv. Docs
            1. http://osgug.ucaiug.org/sgsystems/openhan/Shared%20Documents/OpenHAN%202.0/UtilityAMI%20HAN%20SRS%20-%20v1.91%20redline.doc

        2. http://osgug.ucaiug.org/sgsystems/openhan/Shared%20Documents/OpenHAN%202.0/UtilityAMI%20HAN%20SRS%20-%20v1.91%20clean.doc
        3. http://osgug.ucaiug.org/sgsystems/openhan/Shared%20Documents/OpenHAN%202.0/UtilityAMI%20HAN%20SRS%20-%20v1.91%20comment%20form.doc

3. New Business
    a. OpenSG Q2 Face-to-Face meeting
        i. May 3-6
        ii. Ritz-Carlton Tysons Corner (McClean, VA)
    b. Parking Lot Review
        i. None
4. External Engagements, Business, & Issues
    a. CSWG
    b. SG Conformance
    c. IEC TC57 WG15
5. AOB
6. Roll Call

Google Discussion Points for OpenHAN 2.0

1. The HAN has Zero Physical Security with respect to Consumer Tampering (Guiding Principles)
    a. Any device in the home can be tampered with at any time and all devices on the network (and the network itself) become suspect.
    b. From a security perspective, it is important to assume the HAN environment is hostile to the smart grid and make requirement, design and policy decisions accordingly.

- Discussion
    - **Charles Spirakis -** Need to acknowledge that there is 0 physical security of HAN devices inside the home and very little for ESI equipment
        - How cost effective is it to add requirements that provide little additional security (due to the physical security constraints)
    - **Darren -** Are there any measures that make sense that don't make the devices expensive? Slow down the attack. More investment to compromise. Takes out the broad/general populous attacks.
    - **Tom Thomason (Symantec)** - Is it security of the utility or security of the customer? I don't want to have to cal my utility to change the temperature on the thermostat.
    - **Kevin Collins** - We have made some comments on Physical security. Has anyone done any Risk Analysis? If you assume all devices are hostile, the economics of the solutions begin to collapse.
        - **Darren Highfill** - There is a difference between assuming <u>ALL</u> devices on the HAN vs. <u>ANY</u> device on the HAN is hostile.
    - **Frances Cleveland** - Focus on the physical security as the starting point seems to be missing the point and not the right approach to take. It should not be the first guiding principle.
        - **Charles Spirakis** - It's relevant as it is often not considered.
    - **Skip Ashton** - It's also important to attempt to provide some sort of security rating for the HAN devices. Can't just assume no physical security and therefore have none at all.

2. The ESI possesses a two-way communication interface for HAN Devices which can use encryption to provide protection from eavesdropping. (Architectural Considerations- ESI)
    a. The only requirement for the communication between ESI and HAN Devices is to provide protection from eavesdropping but there is no requirement for the communication to be secure.

- Discussion
    - **Frances Cleveland** - We have to focus on privacy which goes way beyond eavesdropping. If you have distributed generation in the home, you have to go way beyond. I think this is too simplistic.
    - **Unknown Caller** - We have to be relevant to what a consumer would expect in the home. Are we exposing a consumer to privacy issues they don't even know about?
    - **Darren Highfill** - Reminder. This document focuses on the HAN and the ESI

3. Introduction of a communications technology for the home requires enhanced security in the ESI to protect the overall AMI system. (Requirements Framework – Security)
    a. Since there is a lack of physical security from tampering in the HAN environment, there is a limit as to the level of security one can expect.
    b. Specifically, provisioning, privacy (prevention of eavesdropping), end-to-end message integrity, end-to-end message authentication and confirmation of message receipt.
    c. Should the following Security Requirements be deleted?
        i. HAN Device shall control access to persistent HAN data (data at rest).
        ii. HAN Device shall control access to transmitted HAN data (data in transit).
        iii. HAN Device shall provide protection of HAN data while being processed (data in processing) (e.g., trusted processor).
        iv. HAN Device shall implement mechanisms to prevent unintended disclosure of source/originator data to unauthorized principals.
        v. HAN Device shall implement controls which limit access to audit information.
        vi. HAN Device shall detect unauthorized modification of security-related data during storage.
        vii. HAN Device shall separate security critical functionality and data from non-security critical system data.
        viii. HAN Device shall detect unauthorized modification of HAN security policy.
        ix. HAN Device shall detect unauthorized modification of audit data.
        x. HAN Device shall use tamper-resistant hardware (e.g., epoxy, etc.).
        xi. HAN Device shall support open source security methods.
        xii. HAN Device shall provide multiple security methods.
    d. Because there is no physical security for the HAN devices themselves, any accountability that is desired is handled in the ESI. Are the following the only requirements needed? Should there be requirements on the HAN device related to security accountability (e.g. detection of security related activities, audit data, searches of audit data, etc.)?
        i. Energy Services Interface shall provide non-repudiation that a message was sent from the ESI to a HAN device.
        ii. Energy Services Interface shall provide non-repudiation that a reply was received from a HAN device back to the ESI.
        iii. Energy Services Interface shall provide a mechanism for source identification of data (e.g., HAN and AMI System data).
        iv. Energy Services Interface shall provide the capability to audit system policies.

- <u>Discussion</u>

    - Section a
        - **Mary Zientara** - I'm not sure the ESI is just to protect the AMI system. It should also protect the HAN and other networks it's connected to.
        - **Charles Spirakis** - When we use the term HAN device, sometimes it includes the ESI. The ESI is more than a HAN device. We should have a definition for a HAN device and a definition for an ESI and they should be completely different. Trying to burden his document with ESI related stuff is causing too much confusion.
        - **Frances Cleveland**

- The term HAN device is being used in too generic form. Some may need to do some of these things, some may not. Each device should have its own set of security requirements.
- Privacy is more than preventing eavesdropping.
- I don’t see anything relating to power system reliability.

- **Zahra Makoui** - We looked at requirements from a function perspective (and therefore created a matrix).
- **Unknown Caller** - Would like to see a better classification of device types.
- **Mary Zientara** - We have a section I the back of the document that shows requirements mapping to functions
- **Frances Cleveland** - There has been a number of use cases developed in the NIST work relative to DER and HAN. (NIST PAP 7)
- **Unknown Caller** - Where do you envision the assignment of privileges happening?
  - **Darren Highfill** - This goes back to the presentation of the document and I'm not sure it is a security related issue.
  - **Mary Zientara** - The assignment of privileges to the devices is up to the consumer
  - **Darren Highfill** - The privileges that I am referring to are more like which devices might aggregate, store, or share data. Those capabilities need to have associated security controls bound to them.

- Section b
  - **Frances Cleveland** - Don’t see the point in going through them since it depends on what you are doing and what you are trying to protect
  - **Skip Ashton** - You may have different level of these for different devices
  - **Charles Spirakis** - In general, the concept comes back to there were a lot of things in this document that seem to preclude some of the lower cost devices. It does not make sense for these requirements to be in there for some of these devices. What is the absolute minimum a device must have to be OpenHAN 2.0 compliant? All other items can be optional. It very important to look at a lowest common denominator.
  - **Darren Highfill** - As I look down through this list, I don't see a whole lot in this list that I think needs to be on every single HAN device.
  - **Frances Cleveland** - Utilities have been dealing with tampering for a long time. You are never going to completely eliminate that requirement.
  - Charles - At the end of the day, it doesn’t matter if you lied about you PEV or other DER, you are going to be billed on what the meter says.
  - **Kirk Oatman** - A consumer, when they get any of these devices, they need something that doesn’t open up their entire life for someone to drive by and read. We all agree that protecting the grid is critical however we must address privacy of the consumer.
  - **Zahra Makoui** - Are these devices registered to the utility or any device?
    - **Charles Spirakis** - These cover any device registered to an ESI (which can be a utility ESI)

- Section c
  - **Charles Spirakis** - This comes back to some of the requirements on accountability for the HAN devices that popped up and puts them on the ESI. The requirements on the EMS that seems excessive and there is no guarantee that that EMS won’t be lying

anyway. The utility ESI should be responsible for making sure that messages went in and were received.

- **Mary Zientara** - Google is proposing to remove the accountability requirements and replace with the 4 suggested.
- **Frances Cleveland** - You can't count on communications at all time.
- **Skip Ashton** - Is the ESI really where you are going to hold the information or other?
- **Zahra Makoui** - In 1.0, one of the original purposes of this document was to clearly write out the requirement for the utility to go to and RFP. That's where those perspectives came from. In 2.0 is where focus is changing but we need to still capture the utility requirements.
- **Skip Ashton** - The data if you want to hold it would be in the back end system and not in the ESI
- **Frances Cleveland** - That's not the role of the ESI, it's a pass through.
- Charles - If there is a need for non-repudiation, the best you are going to hope for is to put it on the ESI. If you want to put it on the upstream, then that's fine also.
- **Frances Cleveland** - The assumption that it's going to be stored in the ESI is wrong. Non-repudiation should be on a device or function basis.

<u>Conclusion</u>

- **Mary Zientara** - I think the result of this conversation was that these requirements that were deleted are still ones we need to keep in the document. How they are mapped to devices is another story. We will leave them in and have a thorough discussion on how to map these requirements. I think we need to have accountability that could reside in the ESI or some of it could reside in the HAN device. It should be left up to the service provider on where that should be.