SG Security Face-to-Face

Washington, D.C.
Monday, May 4th – 6th

Chair: Darren Highfill
Vice-Chair: Matt Carpenter
Secretary: Bobby Brown

Allen Benitez / CA PUC
Austin Montgomery / SEI
Benjamin King / BSH
Bobby Brown / Consumers / EnerNex
Brad Rumery / Sempra
Brent Cain / Itron
Brian Smith / EnerNex
Bruce Muschlitz / EnerNex
Bruce Rosenthal / SAIC
Carlos Branco / Northeast Utilities
Charles Spirakis / Google
Daniele Loffreda / PE Associates
Danny Hines / Cleco Corporation
Darren Highfill / SCE
David Chambers / California Energy Commission
David Haynes / Aclara
Dennis Gray / APS
Dennis Steffani / Silicon Valley Power
Edward Tirakian / SBC
Erfan Ibrahim / EPRI
Eric Cardwell / ICF International
Frances Cleveland / Xanthus
Gaylon Rasche / SWRI
Gerald Paprocki / Elster
Howard Lipson / SEI / CERT
Ido Dubrawsky / Itron
James Ivers / SEI
Jeff McCullough / Elster
Joel Miller / Marion Group
John Lilley / SDG&E
John Stuart / TVA
Julie Brown / Entergy
Justin Searle / InGuardians
Ken Jones / Elster
Kevin Brown / EnerNex
Kostas Tolios / DTE Energy
Lindani Phiri / Elster
Lizardo Hernandez / Landis+Gyr
Mark Freund / PG&E
Matt Carpenter / InGuardians
Matthew Campagna / Certicom
Maurice Rieffel / Entergy
Michael Cowan / Elster
Michael Garrison Stuber / Itron
Milton Lie / Contineo Systems
Nakul Jeirath / SWRI
Neil Greenfield / AEP
Nick Gerbino / Dominion Resources
Ramprasad Golla / GridNet
Rich Tolway / Arizona Public Service
Ronald Halbgewachs / SNL
Scott Davis / Sensus
Sean Sherman / Triton/PPC
Shrinath Eswarahally / Infineon
Slade Griffin / EnerNex
Su Kim / PHI
Terron Williams / Elster
Tim Rains / Black Hills Corp
Vincent Bemmel / Trilliant
William Miller / MaCT

May 4, 2010

Task Forces & Interest Groups

- **AMI-SEC**
    - Lifecycle phases

Member: Is it too soon to consider Load Control into the home?

Chair: There is a fuzzy line between AMI and HAN. There are discussion groups that have been established that are covering these topics.

- **Risk** – This group currently needs support. Consideration is being made to let this group go dormant for now.

- **HAN** – SG Security looking to develop security profile starting June/July timeframe.

- **New / Potential Interest Groups**
  - **Privacy**
  - **Vulnerability Disclosure**
  - **Supply Chain Provenance** – e.g. Chisco (China Cisco) forgery. These issues are becoming more prevalent. This topic covers sub-components, software, and firmware.
    Issues considered are: What happens when components fail? What happens if they contain illicit software/firmware?
  - **Usability Analysis** – this team reviewed the AMI Security Profile and is in the process of the 3PDA.

    Member – we need to setup a pipeline so that we can run through a quick review and feed back to the SG Security group. The documents are coming out, but utilities/vendors are having problems using them because they state they are "draft".
    ACTION ITEM: John Lilley will chair/vice-chair the group to get it started. It would be good to have secretary for this group. The sub-group needs to establish a charter.

- AMI Security Profile v1.9 (Ido Dubrowski, Itron)
  - Comment resolution team – Is working on comments; they had several duplicated comments that could use the same resolution. The group expects to finish by May 10th at latest. There will be at least a 1 week review period for current version 1.1b (including red line comments). There will be a pre-version 2.0 (1.9) with all changes accepted (clean/readable). The following teleconference we will submit for vote. All comments post version 2.0 will be aimed for resolution in version 3.0.

  Looking for resolution for:
  - Definition of "safe" failure mode – not well defined in the document
    Member – we may pull from the SSR that has a section on modes and transition between them.
    ACTION ITEM: This will be reviewed by the group for what pieces may be pulled forward in the AMI Security Profile.
  - Resolution of Field Tools – there are two sections (field tools and malicious code) that talk about field tools. The suggestion was made to combine these sections. A request was also made for more guidance for field tool security or clarity.
    ACTION: Brian Smith will work with Ido Dubrowski on getting clarification around Field Tool issues.

- ASAP-SG
    - Overview of ASAP-SG was presented
    - Status of Deliverables (AMI, 3PDA, DM – future: HAN, WASA and SA)
    - Distribution Management Scope – includes DA, stops at distribution substation fence except for substation feeder breakers, Volt/VAR control application equipment (e.g.: on-load tap changers, voltage regulators, capacitor controls)
        - Customer end: DM and controls functions in direct communications with appropriate customer equipment (logical boundary) (e.g.: distributed generation equipment, energy storage, direct load control)
        - System protection and AMI is out of scope
        - Chair review of DM SP Scope – Applications table
        - Chair reviewed diagram describing relation of DM to NIST Smart Grid Architecture
        - Chair presented the ASAP-SG technical process – diagram showing the paths
            - Description of steps through FMEA and deriving controls
- OpenADE
    - Review of OpenADE compliance against 3PDA
    - **ACTION ITEM**: Need to compile a list of concerns for further investigation as the team reviews it.
    - Request for OpenADE members to review 3PDA and provide back comments
- OpenADR
    - Approach for OpenADR
        - OpenADE with extensions may be one target
        - SEP2 may be another target
        - Options for other exchanges not targeted for one of the two profiles listed above
    - Point to point vs. Proxy
- Ed presenting:
    - "Simple Two Party Interaction" (refer to slides)
    - Exchange of DR signals; multi-level interactions (aggregators)
    - DR Communications channel controlled by intermediary (e.g., AMI)
    - DR Signals sent to Intermediary

  Discussions around roles and context for OpenADR – third-party acts as proxy in relationship to Resource Manager & Owner.

  Takeaways:

    - No new roles. All relationships covered.
    - Behavior of resource itself is not covered – out of scope.
        - Scope is limited to Resource Owner's ability to exercise control over access to their Resource.
    - Load control signals are not covered

May 5, 2010

- **LEMNOS Presentation** (Brian Smith; Dave Tumim): Refer to slides.

- Motion made and passed to form CyberSec-InterOp subgroup. Vote for formation of CyberSec-InterOp Group passed; Draft charter has been developed (this vote is not on the charter but on the formation of the group).

- **NIST-IR discussion**: The Chair asked if this group should continue to work on standards – Annabelle responded "yes" that this group should continue on requirements. NIST is focused on high-level standards and will be looking at requirements around things like crypto later. SG Security will not be responding to the NIST-IR Draft as a group.

- **Privacy**: Ward Pyles gave a presentation on Privacy concerns (refer to slides).

- **Vulnerability Disclosure Lifecycle**, Sandy Clark and Travis Goodspeed (University of Pennsylvania): Sandy – Proactive, rudeness, risk and vulnerability disclosure as part of email chain. Nobody agrees on vulnerability disclosure, but for smart grid we have too. What makes the Smart Grid different from everything else? One thing – we are going to deploy an enormous system. The vulnerabilities are not additive they are exponential. For first time in US history there could be a single point of failure that brings down the US economy. Attack could come from a source of very little resources (e.g. teenager in grandma's basement). The best countermeasure seems to be to patch as quickly and fast as possible – putting fingers in dikes. This seems to work well so we should continue to do this.

  Member: We have to acknowledge that smart grid is no different than our current grid. DOE did a research that says we can take it down in 15 minutes. The number of devices is much greater, but the problems are still the same. The National SCADA Test Bed (NSTB) and US government are supplying information about what problems are but not the tools used to detect or create problems.

  Sandy: Whose butt is on the line if problems don't get fixed? The issue is we need to fix these.

  Member: We need to define what is and is not smart grid. Is it all the things that can consume power, generate power? Is it things that can be aggregated that are inside and outside the perimeter of the Utility?

  Chair – Let's pretend I, as a researcher, am paid to research a home gateway and find an important vulnerability that will allow the gain of a leveraged attack against an AMI system; and speculate that a large amount of systems can be manipulated. What am I (researcher) responsible for? What are the different stakeholder interests?

Member: Would be the agreement with you and your company. In most cases it is non-disclosure. The company owns the research.

Chair – so what is responsibility of the company?

Member – recommend TelOps

Member – If it is a meter issue then you should notify the meter manufacturer; if it is a component then should notify the component manufacturer

Travis – what time should be allowed for fix from time of notification?

Member: Can't address this.

Member - IEC was looking at subcomponents – the vendor of the device is responsible for components. There is not a requirement to be able to do remote upgrades, so it depends if it is a HAN device. NERC would say the customers need to be informed. I think there is a notification of 1 month – then 6 months to test it. I don't know that we ever want to do vulnerability disclosure.

Member - If doing AMI disclosure, for example bad meter reads, then we want to disclose, but if in T&D then we are dealing with taking out whole sections of the grid and affecting the system. We can't get into 0 day patches and vulnerabilities – there is a whole process of validation to make sure the patch doesn't break something else causing more problems that the fix. Maybe like the difference between a patch for MS desktop vs. a major Cisco upgrade.

Member – someone is going to have to say they are willing to accept the upgrade – say to a thermostat.

Sandy – that shifts the risk and responsibility, but it's not your problem if you accept and it breaks it.

Member – If there is a vulnerability and the customer doesn't patch then they are vulnerable.

Sandy – should service be discontinued if patch isn't applied?

Member – I have a third-party that is managing my service, but utility isn't involved.

Member – we are going to have to define; like the human body consists of an autonomous nervous system and somatic nervous system that allows to do things like play an instrument; there is a clear boundary between the two.

Member – there are laws and regulations that prevent shutting power off if they don't comply to patching.

Member – look at the model of the Internet – enterprises access through the ISPs, but ISPs aren't allowed to push router configurations to the enterprise.

Member – this has occurred – and has been due in most to bad coding.

Chair – As the independent security researcher, let's pretend I have notified the vendor; and the vendor eventually responds and hasn't told what kind of time frame that they are going to address the issue and it is not for certain that they will address the issue at all; but they acknowledge the email. How long is reasonable before taking action?

What is purpose for disclosure 1) people are made aware so can fix 2) people affected notified so that can take mitigating actions; 3) people made aware to put timeline on the fix – whole world can vote by choosing not to buy the product, etc. It's not the guy with the Programmable Communication Thermostat (PCT) in his home that has the power, but it is the ones that buy in bulk that have the relationship with the relatively small group of vendors.

Member - Don't be too myopic and thinking that smart grid is the meter; it is millions of devices that can include PEVs and washing machines – the grid could not respond to an event that each of these would switch load at the same time. It is important that the entire eco system is secure to the point of not dropping the grid; not just inside of large switches and generation – but in all devices in aggregation that can shift load.

Member – one of the big distinctions with critical infrastructure is impact; much more so than an IT system. The impact of a compromise is huge.

Chair - If I am unsatisfied with a vendor what is my course of action?

Sandy – One of the reason to disclose vulnerabilities is to put pressure on vendors to fix: 1) problems that are not disclosed do not get fixed 2) there are tons and tons of problems, the bad guys will find the problems – it is highly profitable to find vulnerabilities, it is highly profitable the economics have changed; 3) the systems are so enormous that due to unexpected interactions there are new security problems.

Vice Chair – Not all disclosure is done by good people for good purposes; In many scenarios it doesn't make sense to …; We need a place to go that can not only determine the importance of a vulnerability but who needs to know, and how to respond.

Member: The HAN devices – are they consumer electronics? What's the warranty on a HAN device? It's not a warranty issue. If looked at from a warranty device then gets fixed in the next version. This doesn't help the financial issue.

Member - there used to be an effort under DHS to do control systems CERT. There is an ICS CERT. The regulation needs to be in place to have control industry to follow. Only regulation through NERC or whomever will force to be disclosed – need to be washed and cleansed so that a user isn't.

Member - Vulnerability disclosure needs to be easy (like the big red button). Other CERTs need to be aware of it.

Member - The operator is more impacted than the vendor. What level do the operators get involved if there is a central group that his hearing and being aware? There are financial impacts.

Member - There is a time factor involved with the process – downloading patches; pushing out, etc.

Member - WG15 was working on this and is available. There are good researchers and bad researchers. Good – I have discovered a vulnerability, (if I had a tool) here it is. Bad – You've got a vulnerability, they don't tell how they create it, they don't provide tools, and when it isn't fixed they go to CERT. Makes it very difficult to fix. Becomes a trust issue. Need to establish trust.

Vice Chair - Not all researchers that find bugs are technically capable to exploit them.

Member – Should say that NERC should become the authorized certifiers for researchers so can separate the chaff from wheat and can work hand-in-hand with vulnerability database owners?

Matt - How do motivate people to be certified?

Member - I think it has to be legislated.

Travis – what about vulnerabilities in toys; can change IM-me toy to packet sniff that uses Chipcon 1110; but now I can sniff all products that use this chip and can sniff a meter in disguise. We can't push a certification for all industries.

Member – There are CC labs (11 in the US). If all the equipment manufactures go through test labs then components will get tested.

Sandy – labs were in charge of certifying voting machines; they were certified – but are so broke I can get you voted president.

Member – These are in-home devices. We have seen this with set-top boxes years ago. They put an exploit to get all premium channels, then there would be a patch; then became cat and mouse game.

Sandy – People don't have a place to look and see if their device is broken or has a vulnerability.

Annabelle - CC is focused on testing product not systems and is for classified systems; big difference between IT and control systems; confidentiality is bottom of list for Control Systems and IT is opposite

Member – certifying every person that is doing this research is impossible; The whole idea is to encourage people to do this vs. to put out into the wild; we need to put into organization where it can be sanitized, etc.

Closing comments – Travis: when there is a component vulnerability then have an obligation to publish openly when it is a product that is cross industry (e.g., appears in consumer products (toys) and meters, etc.)

Presentation: TC57 WG15 – NWIP Proposal (Herb Fauk)

- E.g., France does not want US to dictate vulnerability disclosure; they all have their own.
- IEC can't do the disclosure process and no government agency should do the disclosure process; the problem is that if the government is managing it, then they don't want to do it under the other government's rules
- There are complexities to testing and patching
- Need a FAST TRACK to update standards
- Looked at current CERT process (6 years ago) (see slide deck) came away with:
  - Is it reproducible? If no, then should be really disclosed?
  - What are common mechanisms to do diagnosis? (e.g., capture network traces)
  - What if vendor doesn't have 24x7 response? (timeliness)
  - What is availability of version/environment of customer OS and software?
- Proposal to get utility input; and there was no support from US (first) and others followed with no in supporting this effort

OpenHAN Comments:

- The concern is around risk to grid resulting in power loss, explosions vs. money
- There is a need for a risk/threat assessment for HAN to determine what mitigations are needed
- Need to remove the motivation for the HAN devices to be exploited
- Need to design HAN to limit the impact of vulnerability/exploit
- The OpenHAN needs clarity on what attack approaches are out there
- Concerned about upstream access from HAN device exploited (e.g., into SCADA)
- ASAP-SG will start on the HAN Security Profile, but will take time. Need to start looking at a few recommendations now. Will feed into the OpenHAN as these mature.
- IEEE P2030 - Have evaluation of use cases for smart grid would like to pass along document.
- Principle: just because I don't' trust a device doesn't mean I can't communicate with it.

Scope of Compromise:

Potential targets: Thermostat / HVAC, PEV, Direct load control, Distributed Generation / Storage Displays, Appliance, ESI

- Singular device within a single HAN
    - Concerns:
        - Magnitude of associated load or energy supply
        - Credential / key information
        - False messages
            - Humans
            - Other devices
        - Metrology / revenue information
        - PII theft
        - Loss of functionality (including medical devices / human safety)
    - Values:
        - Utility / service provider (Low)
        - Consumer (Medium)
        - Premise owner (Low)
        - Vendor (Low)
        - Regulator / policy-maker (Low)

- Multiple devices within a single HAN / all devices within a single HAN
    - Concerns:
        - Amplification of concerns for singular device
    - Values:
        - Utility / service provider (Low)
        - Consumer (High)
        - Premise owner (Low)
        - Vendor (Low)
        - Regulator / policy-maker (Low)

- Multiple devices within multiple HANs (single neighborhood scale)
    - Values:
        - Utility / service provider (Medium)
        - Consumer (High)
        - Premise owner (Medium)
        - Vendor (Low)
        - Regulator / policy-maker (Low-Medium)
    - Concerns:
        - Service availability to neighbors (i.e., transformer fuse)
        - Mayhem / public distrust
        - Damage to distribution system asset

        - Synchronistic events (e.g., resource contention)
        - System stability

- Large number of HANs (multiple neighborhoods)
    - Values:
        - Utility / service provider (High)
        - Consumer (High)
        - Premise owner (High)
        - Vendor (High)
        - Regulator / policy-maker (High)
    - Concerns:
        - Service availability to neighbors (i.e., transformer fuse)
        - Mayhem / public distrust
        - Damage to distribution system asset
        - Synchronistic events (e.g., resource contention)
        - System stability

- Extension into a network beyond the HAN
    - Values:
        - Utility / service provider (High)
        - Consumer (High)
        - Premise owner (High)
        - Vendor (High)
        - Regulator / policy-maker (High)
    - Concerns:
        - Compromise of gateway (C&C) to route information upstream into the Network
        - DoS to wide area
        - Compromise of a third-party
        - Damage to a distribution system asset
        - Loss of revenue
        - Misuse / abuse of system
        - Breach of sensitive information (e.g., PII, corporate sensitive info…)

Restful vs. SOAP (Matt Carpenter)

- Restful is an architectural approach/style vs. and SOAP protocol (refer to slides) (a bit of apples and oranges)
- They both make security mechanisms available (single sign-on, federated trust)
- We need to look at the security considerations of each; how to define a policy around each
- Business decision will drive which to choose from between the two