SG Security & AMI-SEC Webinar

Monday, March 15th – 2-3:30pm EST

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

Travis Goodspeed (Panelist), University of PA
Sandy Clark (Panelist), University of PA
Allen Benitez, CA PUC
Brad Rumery, Sempra
Brad Singletary, EnerNex
Brian Lenane, SRA International
Brian Smith, EnerNex
Carlos Branco, Northeast Utilities
Daniele Loffreda, PE Associates
Danny Hines, Cleco Corporation
Dave Dalva, Cisco
Dennis Steffani, Silicon Valley Power
Doug McGinnis, Exelon
Gary Finco, INL
Gib Sorebo, SAIC
Howard Lipson, CERT/SEI
Ido Dubrawsky, Itron
James Ivers, SEI
Jose Carr, Self
Joseph Chiu, SCE
Kevin Brown, EnerNex
Louis Robinson, Constellation Energy
Mark Freund, PG&E
Matt Thomson, GE Energy
Maurice Rieffel, Entergy
Michael Northern, Deloitte Consulting
Milton Lie, Contineo Systems
Nakul Jeirath, Southwest Research Institute
Ovace Mamnoon, HP
Peter Haynes, Pariveda Solutions
Ramprasad Golla, Grid Net
Rich Tolway, APS
Rob Jepson, Lockheed Martin Energy Solutions
Roger Alexander, Eka Systems
Sandy Bacik, EnerNex
Sitaraman Lakshminarayanan, GE Energy

1. The meeting opened with a review of the agenda and a call for items of business.
2. Old Business
    a. Perspectives and Insights – A call was made to solicit presenters and suggested topics for future meetings. Presenters and topic request should be sent to SG Security leadership (Chair, V.C., Sec'y).
        i. AMI Security Profile revisions – This activity has stalled. A call for a new team lead and team members to finish work was made. The Chair stated that the time commitment will depend of how effective members are at responding to comments and/or finding help with work. The effort will involve getting information aggregated and work produced. The timeframe has slid beyond the original target. The biggest driver is to establish reference material for the third version of the NIST-IR. The work will involve estimating the time necessary to complete and develop a plan for working forward. Ito Dubrawsky volunteered to lead effort and will work on handoff with Sandy).
        ii. Third Party Data Access Security Profile review – This work has still not been initiated. Leadership for this effort is needed. A document review is needed on the initial draft that was completed one month ago; to-date progress has not been

made. ASAP-SG has accelerated this effort for SG Security; the work simply needs to be reviewed and completed. This profile describes how third-parties access customer energy usage securely.

iii. Interest Groups – Discussion was postponed other than to state that the ListServs have been established. To join please send an email to the list to participate. ListServs are: SGSec-OpenHAN, SGSec-SGComm, SGSec-AMIEnt, SGSec-3PDA and SGSec-Risk

3. New Business
   a. Open Discussion
      i. Vulnerability disclosure (guest speaker: Travis Goodspeed) (refer to slides) – Travis' presented on his findings on the Chipcon ZStack PRNG vulnerability. The vulnerability also affects other chips that followed the Chipcon ZStack. Travis displayed graph that shows the pairs of unique series of random data. This severely restricts the number of keys that can be produced. The Ephemeral key is predictable. The static key is random. The static key can be extracted by the ephemeral key. Keys can be generated in only a couple of hours. In CC1110 and CC2430, PRNG was used primarily to implement collision avoidance; but got used for security in new stack. ZStack stores keys in RAM. Chipcon 8051 does not defend RAM. There is a difficulty in patching the firmware – applications must also be patched by every application vendor for every project.

         The patch seems to fix the vulnerability. But Travis indicated that he doesn't expect devices to be fixed until months to come.

         This is version 1 or 1.1 Zigbee SEP. It is not the upcoming revision.

         Every vendor has to supply a patch for this bug. If a meter vendor roles out a patch tomorrow, the vulnerability could remain on the other devices like the PCT. Any device on the HAN could have its ID usurped.

         Q: What threat does this pose to the AMI network?
         Travis: This allows for remote attacks to be made with a device that the meter trusts. This allows arbitrary code to be run against a device to which it trusts on the network.

         Q: Is there is no remediation except for a patch?
         Travis: Not really, it can be stolen within 20 attempts.

         Q: The upgrade to the firmware – does that mean they have to be all touched or over the wire/air?
         Travis: For meters you are likely able to do over the network, but smaller devices such as the PCT would have to likely touch each one; or other HAN devices.

Q: If I'm nefarious and imitating someone, could I go back and reverse engineer these?
Travis: The HAN credentials themselves don't give authority to flash a meter – you would have to use Stack Overflow or something of that nature. Being able to determine if these remote devices have not been exploited has not been implemented.

Travis' closing statement: This problem could have been avoided, if all firms that copied this bug were made aware of the vulnerability. Slow disclosure makes this problem difficult to fix. I would like to start a skunk works mailing list to address these problems, rather than through articles. I would like engineers to subscribe to the list that are designing these systems.

Q: Will SG Security list be part of this list?
Chair: I will make sure folks will have opportunity to join list.

Travis: The presentation will be made available via email to those that request. (The Chair has distributed to the SG Security ListServ)

Travis Goodspeed – is security researcher and PhD student at University of Pennsylvania. Has experience in embedded devices, etc., etc.

b. Vulnerability Disclosure Notification discussion – The Chair opened with a question of how do we manage vulnerability disclosure notification as an industry moving forward?

Comments from members: The people that the need to know is small compared to the over-all market. I think that we can adjust what we have learned in the IT market. There is responsibility on all sides – utility and vendor. As an industry, there is need to participate in industry events and bring back knowledge to organization. The consumers may be responsible for patching their own equipment. Sometimes the engineers don't have the right information to put in the proper protections to add security in many places. If a single vulnerability brings down the infrastructure, then our security architecture has failed. Researchers may try to expose this to the public good if vendors don't respond appropriately. Vendors should indicate how they disclose vulnerabilities. Information Security and Analysis Centers (ISACs) already exist to manage this. There is also a DHS industrial control systems CIRT. We should be supporting and championing these efforts in the industry, but these can be fairly cumbersome in terms of timeframe when dealing with vulnerabilities. Time is of the essence when a vulnerability has been discovered.