Smart Grid Interoperability Panel – Cyber Security Working Group
Meeting Minutes (29 March 2010)

NIST LEAD: Annabelle Lee
If you want to be on an email list, contact Annabelle and Tanya

NIST Contacts:
Annabelle Lee, annabelle.lee@nist.gov
Tanya Brewer, tbrewer@nist.gov
Victoria Yan, yan_victoria@bah.com

SGIP-CSWG Administration
Vice Chairs:
- Dave Dalva, ddalva@cisco.com
- Alan Greenberg, Alan.M.Greenberg@boeing.com
Secretary: Mark Enstrom, mark.enstrom@neustar.biz

SGIP-CSWG Sub-Groups Information:
Listed below are the SGIP-CSWG leads for each group. More detailed information about each group is available at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WorkingGroupInfo. If you would like to join any of these sub-groups, please let Annabelle and Tanya know and you will be added to the group(s).

**Standing Sub-groups**

Architecture Group
CSWG Leads: Justin Searle and Sandy Bacik

Bottom Up Group
CSWG Leads: Andrew Wright and Daniel Thanos

High Level Requirements Group
CSWG Lead: Dave Dalva

Privacy Group
CSWG Leads: Gal Schpantzer and Rebecca Herold

R & D Group
CSWG Leads: Jessica Ascough, Isaac Ghansah, and Daniel Thanos

Standards Group
CSWG Leads: Ramesh Reddi and Virginia Lee

Vulnerabilities Group
CSWG Leads: Matt Carpenter and Matt Thomson

Crypto and Key Management Group
CSWG Lead: Daniel Thanos and Doug Biggs
Over 400 Participants on the SGIP CSWG Distribution List!

..and, the number is growing every week. This shows that many organizations are taking an interest in the group’s work. Congratulations to everyone!

SGIP CSWG Roadmap Will be Released on 31 March

The CSWG, SGAC and SGTCC are developing high level roadmaps; the CSWG is targeting the release of the draft roadmap to the SGIP Governing Board by close of business on Tuesday, 30 March 2010. Deliverables past June include education and outreach.

The draft roadmap was posted for comment on Friday, with all comments due by noon on Monday. The team received many good and useful comments that will be incorporated for the final roadmap review on Tuesday. The review will be open to everyone; Annabelle will send out the phone and webinar link to everyone. The intent of the review is to finalize any changes before submission to the governing board.

Also note that the CSWG work is being reviewed by many other groups. For example, the DHS Industrial Control Systems Joint Working Group is also developing a roadmap, and is referring to the CSWG roadmap. Great job!

April Meeting at Sandia National Labs is a Go

The meeting at Sandia National labs will take place on 20 April 2010 and will cover threat profiles and EMP; Annabelle is currently working on the agenda with Juan Torres. All attendees will need a Top Secret Clearance; in addition, any one without a TS-SCI clearance will not get into all the meetings. Please let Annabelle know if you want to attend.

Annabelle will send out the logistics to those attending the meeting. It is your responsibility to ensure your clearance information is passed from your security office.

For those not attending, Annabelle is requesting a non-classified briefing for the CSWG June face to face meeting.

Mark will add the meeting dates to the Twiki for the Sandia meeting and the June face to face meeting.

CSWG Face to Face Meeting

The face to face meeting is planned for 2 – 3 June 2010, at the Cisco offices in Herndon, VA. Dave Dalva will send out logistics information (location, hotels), and registration information once the details are firmed up. Look for that information in a couple of weeks.
Federal Register Notice not Posted

The FRN is still in review by legal, and is therefore not posted. Annabelle will again follow up with legal to find out the status. Too many delays in the release could impact the June deliverable, as we still need to account for the 60 day comment period.

Even if the June deliverable is delayed, we will still plan to have the CSWG face to face meeting on June 2 and 3 at the Cisco offices in Herndon.

SGIP-CSWG Administration Meeting on Mondays

The CSWG admin team will be meeting on most Monday mornings prior to the regular Monday morning teleconference. If you want to raise any issues or information, please let one of them know (Annabelle, Dave, Alan, Tanya, Vicky, or Mark).

Meeting Notices for Sub-Groups

If a sub-group changes the meeting times or meeting frequency (e.g., once a week to twice a week), please be sure to update the Twiki. Some people do not join every single week, and will be disappointed if they try to join the conference call and no one else is there.

EAX Mode of AEX is not Approved by NIST

A recent email exchange covered the EAX mode (vs. CCM mode) of the Advanced Encryption Standard (AES). In AES, the EAX mode is not approved by NIST for use by the federal government. However, the use of the CCM mode is approved.

Since EAX mode is included in ANSI C12.22, Annabelle is asking the persons responsible in NIST for additional information. To do that, more information will be needed from the team; Annabelle will forward the needed information categories to the crypto team. If you want EAX approved, send information stating why, etc., to Daniel – as the lead of the crypto/key management subgroup, and he will consolidate and forward to Annabelle. Please forward as many details as you can, as the person who is looking at this is a crypto mathematician and will look at the details. We want to make sure we have the strongest algorithms and modes, so the more details the better.

Elliptic Curve Licenses

Annabelle is looking at the elliptic curve license between the federal government and Certicom to find out what is covered and what is not covered.

Liaison with the SGTCC

Dave Dalva brought feedback from an interesting internal company regarding certification. The vendor community will not want this process to add new certifications and testing, and
will want to leverage existing certifications. Adding new ones will be very expensive and may harm the industry. This is critical because vendors will not want to spend millions on products only to have them be behind when finally released.

Adding additional certifications could also create bottlenecks in the testing labs. Therefore, the group needs to determine the priority focuses: interoperability, configured products, testing products independent of environment, etc.

If you have something specific you want addressed by the SGTCC, please forward the information to Dave or Mark to be raised with the SGTCC. Especially useful will be existing testing regimes that can be reused.

**High level Requirement sub-group**

Vicky is helping enhance and prioritize the high level requirements for consumption by people in the federal and state regulatory bodies. The goal is to identify the highest impact requirements. These will be prioritized for the next stage of the NISTIR.

**Standards sub-group**

The availability of standards is still an issue. This is recognized but it will not be resolved immediately. There is an ongoing effort with ANSI to resolve this issue, and all hope that this can move forward soon.

**Architecture sub-group**

The group is getting more details on the security architecture, and is adding an introduction to the section. Over the next few weeks they will get into the defense-in-depth discussion.

Sandy and Justin are actively listening into the SGAC committee meetings and will be involved in the April meeting.

**Bottom up sub-group**

The group is finishing the write-up on critical information and infrastructure. In addition, the group is addressing a new potential problem; smaller organizations that can be the subject of an aggregation attack. The basic thought is that small organizations may not have the security in place to fend off an attack. A large attack on the grid is possible if enough of them can be compromised.

The group will do a mapping of their results to the initial high level requirements to find the legitimate gaps in the requirements. The group is asking for volunteers to do in depth reviews of the requirements.
Finally, feedback on Appendix D from vendors at DistribuTECH was very positive, specifically because the section provided actionable input.

Congratulations to the team! This shows that the work is having an impact.

**Cryptography sub-group**

The first couple of meetings of the group have been good; meeting notes will be released soon. Initially, the group is moving the information from the bottom-up group to the new document and giving it more structure. Currently the document has a good outline, and the group will be filling it out. Good meeting.

Volunteers are needed to do initial work on identity based encryption. The intent of the work is not to pick favorites, but to evaluate the possibilities, and let the system designers figure out the best solution.

The group has some very good representatives from the utilities, but would like to see more involvement.

Additional discussions included the mapping of cryptography to high level requirements.

Finally, the group is looking at cryptography issues from PAPs 1 and 2. They believe they might need a liaison to the groups. Please let Annabelle know if she should get Alan involved as the liaison.

**Privacy sub-group**

Group membership is growing, including utilities. This is great, as this helps ensure the outputs are beneficial.

The group divided into 5 teams to make sure all needed information needed is included in final chapter. Additional information being added includes use cases, additional privacy concerns, legal concerns, and regulatory discussions. Once all the information is included, the group will spend a couple of weeks looking at overall discussion.

**R&D sub-group**

The group has been trying to bring clarity to some of the topics, including using virtualization as a security tool. As a point of clarification for the discussions: the group does not want to endorse a vendor or a technology; the group is bringing up topics and discussing potential actions.

The group is also looking at security design and verification tools. Daniel put out a section on this topic for review by the group; if there are no objections, he will put the section into the document.
The topic of mapping topics to the high level requirements was raised. However, it is difficult to do a 1:1 mapping, since both systems and the many existing solutions are evolving. The group will need to think about how (or if) they will address this.

**Standards sub-group**

The standards group is waiting for the responses from ANSI. In the meantime, they will address the standards they do have.

**Vulnerabilities sub-group**

The last call focused on developing the matrix. While the calls are always interesting and educational, the real work needs to be done on the matrix. To all that, the calls will shift to a bi-weekly call.

**CSWG Twiki Updates**

Mark and Tanya updated the Twiki to include links to the common terms and the CSWG outreach plans. Please take a look at both and provide comments. In addition, the PAP and DEWG involvement will be placed on the Twiki under the Liaisons tab.

All of this can be found under the SGIP-CSWG Meeting & Membership Information heading on the CSWG Twiki page.

http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

**Keep up the Good Work!**

The work of the CSWG was mentioned by Howard Schmidt in a talk at DOE last week. Many are interested in our work products. Keep up the good work!

**Next call for the SGIP-CSWG:** Monday, April 5, 11am EST.

**Call-in number:** 866-745-6097  **Participant passcode is:** 7413006

Please remember to mute your phones when not speaking.