

IEEE P2600 Meeting #35

May 21-22, 2008

Xerox, Rochester NY

Attendees

Chair: Don Wright, Lexmark
 Vice Chair: Lee Farrell, Canon
 Secretary / Lead Editor (2600.n): Brian Smithson, Ricoh

Carmen Aubry, Océ (by phone)
 Nancy Chen, Oki Data (by phone)
 Peter Cybuck, Sharp
 Tom Haapanen, Equitrac
 Helmut Kurth, atsec (by phone)
 Ron Nevo, Sharp
 Alan Sukert, Xerox
 Brian Volkoff, HP (by phone)

In the following sections, names of speakers are indicated by [brackets]. The primary speaker for a session is noted at the beginning of the session as a default; others are noted in place. Some comments may appear in these minutes, indicated by {braces}, inserted by the Secretary for clarity.

Attendees.....	1
Administrivia [Wright]	2
Agenda review.....	2
Minutes and Agenda approvals	2
IEEE patent policy	2
IEEE WG guidelines.....	2
Officers and Editors.....	2
Meeting schedule updates [Wright]	2
TCG update [Smithson]	3
INCITS CS1 update [Wright].....	3
CCVF update [Sukert].....	3
Action items from previous meeting [Wright].....	3
PP evaluation ad-hoc status [Nevo]	4
PP Guide ad-hoc status [Farrell]	6
P2600.1/2/3/4 Comments review [Smithson]	6
PP restructuring and other issues [Smithson]	6
Production Printing environment/PP update [Lewis]	11
Schedule review [Wright]	11
Next meeting details [Wright]	11
Closing [Wright].....	11

*** Called to order at 9:15 AM 5/21/2008 ***

Administrivia [Wright]

The following administrative items were reviewed:

Agenda review

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2008.ppt>

Minutes and Agenda approvals

The April 2008 minutes were approved without changes. The May 2008 agenda was presented and approved with no changes.

IEEE patent policy

Patent policy was reviewed. See slides for the policy:

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2008.ppt>

Note that there are new patent policy slides presented at the May meeting. Slides 1-4 of the revised IEEE Patent Policy were presented and participants were given the opportunity to disclose any requested information. No disclosures were made.

IEEE WG guidelines

IEEE guidelines on such things as inappropriate topics were reviewed. No issues were identified.

Officers and Editors

No changes.

Officers:

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary: Brian Smithson, Ricoh.

Lead editors:

Editor (2600): Jerry Thrahser, Lexmark.

Editor (2600.n): Brian Smithson, Ricoh.

Meeting schedule updates [Wright]

New meeting dates have been added to the schedule.

Jun 23-24, 2008

- Longmont, Colorado (arranged by InfoPrint), with PWG (Jun 25-27)
Radisson Hotel & Conference Center Longmont-Boulder
1900 Ken Pratt Boulevard, Longmont, CO 80501
- No special hotel rates have been arranged

- Registration with PWG will be required, with an expected meeting fee of \$65-\$75/day
- Details (when available) will be on <http://grouper.ieee.org/groups/2600/meetings.html>

Aug 11-12, 2008

- Sharp Labs, Camas WA, with PWG (Aug 12-15)

Sep 9-10, 2008

- Sharp, Arlington VA

Oct 24, 2008

- Lexmark, Lexington KY, with PWG (Oct 21-23)

December 11-12, 2008 – tentative

- Equitrac, Plantation FL

No other schedule conflicts or issues were identified during this meeting. The most current P2600 meeting information is always available at <http://grouper.ieee.org/groups/2600/meetings.html>

TCG update [Smithson]

(TCG web site: <http://www.trustedcomputinggroup.org/>)

- no HCWG meetings
- waiting on PWG IDS

INCITS CS1 update [Wright]

(INCITS CS1 web site: <http://cs1.incits.org/>)

- No updates since last meeting

CCVF update [Sukert]

(No CCVF web site)

- There has been activity on the CCVF mailing list about a meeting with NSA about CCV4, and about the upcoming 9th ICCV in Korea.

Action items from previous meeting [Wright]

No action items were recorded or updated on presentation slides. The action item spreadsheet was reviewed and updated.

Pre-meeting:

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20080516.xls>

End-of-meeting meeting:

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20080522.xls>

Post-meeting reconciliation:

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20080530.xls>

- AI #246 (IEEE copyright issues for PPs) is still being worked on
- The call for sponsor ballot on the PPs will expire sometime in June (six months after it was originally made) and will need to be reissued unless we can start sponsor ballot before that date

PP evaluation ad-hoc status [Nevo]

- Contract with atsec has been issued
- Backgrounder has been updated to reflect the approval of 2600 as an IEEE Standard
- rechartered this ad hoc for managing the evaluation process and informing the WG about progress [Wright]
- since the charter has changed, can members join or leave? [Smithson]
 - that is always possible [Wright]
- As of the last meeting, NIAP was only interested in PP-A and it would require some approval from Audrey Dale to accept other PPs for validation. I spoke with Ms. Dale and she said that NIAP is now reporting to NCSC in NSA, which has more of an outward focus on industry and commercial interests. [Smithson]
- Previously NIAP was only doing work for NSA DoD customers, but the NCSC also considers homeland security issues and may have more support for lower-level evaluations and non-DoD customers [Cybuck]
- Ms. Dale will be meeting with NCSC and will bring it up with them and then let us know. She said that it would help if we could identify some government agency that would express interest in PP-B or C or D, it would help make her case for validating more than just PP-A. Also, she understands that the work required for validating four related PPs would not be 4X the work required to validate one of them. [Smithson]
- In the end, if NIAP cannot do more than PP-A, then we are faced with a decision of whether to take all of them to another scheme or split them across two schemes. [Smithson]
- Another idea is to get PP-A done in the US and also get PP-A/B/C/D in Germany. [Nevo]

- If atsec uses a delta approach to evaluate PP-B/C/D, then they a scheme would also need to validate all four. [Wright]
 - The NIAP version might have a different title, like “US Government PP”, but otherwise they could be the same [Smithson]
- The German scheme is pretty busy with projects that came out of the US, so we may have some problem getting into that scheme. Sweden is another possibility, but they do not have any experience with PPs. [Smithson]
 - Is there an issue with IPA if we get the PP validated in the German scheme? [Cybuck]
 - As far as I know, the IPA is most interested in seeing the CCRA logo on the certificate [Smithson]
 - Our previous proposal using a packages approach wasn't quite legal from CCRA because it had options in the security problem definition, objectives, and requirements. The new proposal does not have options there, it puts the optional parts outside of the PP in SFR packages [Smithson]
- We would have a problem if we got the PP validated, but then someone writes an ST based on that PP with packages and IPA refuses to validate the ST unless all packages are included. [Wright]
 - That is the issue that Ueda-san brought up [Farrell]
 - I think we are OK because we have put the options outside of the PP [Smithson]
 - IPA only looks at the CC language and it does not allow options. We should check this with IPA [Nevo]
 - The question to ask IPA is whether they would accept an ST based on this PP if the ST did not conform to all of the packages [Wright]
 - IPA already said that the conformance rules we specified in the family of PPs was OK, and we have done something similar in the packages proposal, but now it refers to packages and not to PPs in a family. [Smithson]
 - Can we state in the PP that, for example, if you don't have fax then you don't need to conform to the fax package? [Wright]
 - Or you conform to the package by eliminating fax [Cybuck]
- We should get atsec's recommendation on how to do this and have them ask IPA [Nevo]
 - This is the approach that atsec recommends, but there is an issue of whether or not IPA will accept it. [Smithson]

PP Guide ad-hoc status [Sukert]

- meetings held on May 6 and 19
- possible restructuring of PP is delaying production of the guide
 - chapters 1-3 should be OK to start [Smithson]
- goal is to have some initial text for August meeting
- would some part of the guide help explain a new PP structure to IPA? [Nevo]
 - maybe parts of chapter 5 or 6
- current plan is that initial text of the guide will be available for the August meeting, but will likely contain partially completed sections, and we will see if we are on the right track
- rechartered this ad hoc for continued work [Wright]

P2600.1/2/3/4 Comments review [Smithson]

Refer to comments:

http://grouper.ieee.org/groups/2600/comment-tracking/P2600_2008_05_v01.pdf

And comments with resolutions:

http://grouper.ieee.org/groups/2600/comment-tracking/P2600_2008_05_v02.pdf

- {most comments were not controversial, see the resolution document for details}

PP restructuring and other issues [Smithson]

Refer to the prototype PP:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.1-36b-proto.pdf>

And to explanation document:

<http://grouper.ieee.org/groups/2600/presentations/Rochester2008/Explanation%20of%20PP%20restructuring.pdf>

- reasons for restructure [Kurth]
 - redundancy [Kurth]
 - complexity [Kurth]
 - difficult for ST authoring [Kurth]
 - difficult to evaluate [Kurth]
- conformance [Kurth]
 - validation would need to include all combinations of PP and packages [Kurth]
 - examples of similar approaches include PKI and also medium robustness kernel [Kurth]
- it is not disallowed by CC, but it is not explicitly allowed [Kurth]
- CC does allow packages and does allow packages of SFRs [Kurth]

- how to convince IPA that this is OK? [Wright]
 - contact IPA ourselves [Kurth]
 - atsec contacts IPA [Kurth]
 - put it on the CCDB agenda [Kurth]
 - who is on the CCDB? [Wright]
 - representatives from each scheme, so you would need a scheme to bring it up [Kurth]
- are we the first to bring this up? [Wright]
 - not really, NIAP did it for some of their own PPs but other schemes were not interested in them [Kurth]
 - so we would be the first to get IPA to look at it [Wright]
- IPA looked at the PKI PP and said it was not part of CC definition, it is a NIAP approach [Nevo]
 - PKI was more loosely coupled to CC than the P2600 approach, it had many packages that could be combined [Kurth]
- atsec could write a discussion paper to submit to IPA, and also to other schemes to bring up in the CCDB [Kurth]
- we have talked about pushing some requirements to the environment so that they can be either satisfied externally or internally, for example audit storage/management
 - if we push too much to the environment, doesn't that remove the meat of the PP?
 - the WG needs to decide what must core functionality provided by the TOE [Kurth]
- could we keep some requirements internal and then allow an ST author to satisfy them outside of the TOE and be demonstrably conformant?
 - No, you can only pull things in from the environment, you cannot push things out to the environment [Kurth]
- Could we do that with a package? [Wright]
 - You could do that. You would have an assumption that it is in the environment, and if the ST author wants to pull it in, they use the package [Kurth]
- There are three cases, internally provided, externally provided, or both (as an administrator option); if the ST can do both, would they need to be defined as modes of operation so they need to be evaluated separately?
 - Yes, that would be the way to do it. You may also use the SFR for multiple authentication methods if you're dealing with internal and external authentication. [Kurth]
- What about the use of data export instead of specifying encryption for protecting data from offline salvage? We have three cases: no hard disk, hard disk for which encryption is performed by the TOE, and hard disk that has built-in encryption (outside of the TOE).

- The problem with export is that for user data it only defines exporting with or without attributes. You can use the inter-TSF data transfer data confidentiality SFR. How you provide confidentiality is open, physical or encryption or whatever. The ST author must specify how it is done and provide crypto SFRs if the TOE does encryption. [Kurth]
 - One way to make it possible for us to specify this in the generic PP without implying a requirement for a hard disk is if we can apply it to both nonvolatile and volatile storage. Would the SFR be satisfied in the case of volatile storage automatically by virtue of the data going away on power-off?
 - You need to differentiate between removable from non-removable storage. Non-removable storage is protected by the environment. You also need to protect user data and also the corresponding SFR for TSF data. So you say that confidentiality protection is required for all storage that can be removed from the system, then if you have removable volatile storage the ST author would say that it is provided by erasing on poweroff. [Kurth]
- How does that address data across the network? [Wright]
 - This was for data at rest. [Smithson]
 - For data on networks, you can use trusted path if you have mutual authentication, or you can use trusted channels if you don't authenticate the other end of the communication. You can restrict the requirement to a specific kind of channel, but you need to make an assumption for other channels that it is protected by the environment.
- What about incoming confidential data? [Wright]
 - You can't enforce the other end, unless you use a trusted channel. SSL and IPsec are examples of trusted channels. [Kurth]
- What about the strength of confidentiality? [Chen]
 - That is part of the evaluation of a specific implementation of the requirement. A product using weak encryption should fail the evaluation. It is specified in the CEM in the AVA section. [Kurth]
- We have talked about FDP_RIP, and we have not been using it correctly. Many customers ask for data overwriting for deleted documents, so we tried to use FDP_RIP to make that requirement.
 - That is not the intention of FDP_RIP. It was intended to require that residual data from one process is not available through normal interface mechanisms to another process.

- So we would put a generic FDP_RIP SFR in the common PP. [Smithson]
- So what about removable storage and the overwrite requirement? [Farrell]
 - That doesn't make sense. You should just encrypt the whole disk, including the empty sectors. [Kurth]
 - Some people wear belts and suspenders [Wright]
 - Using the two together can create a new threat [Kurth]
 - There are products that do both [Cybuck]
 - We could handle that by not putting overwrite in the PP and let people add it to their ST if they want.
 - It would be a good app note [Sukert]
 - I don't know how to specify it. The only thing we came up with was FDP_RIP, and that isn't correct.
 - We did overwrite in a product and used FDP_RIP, and that was accepted by BSI, but we did not actually specify overwriting. [Aubry]
 - NIAP comments seemed to indicate that there was a threat of analysis of removable storage [Cybuck]
 - NIAP is expecting some kind of protection, from the environment or the TOE. We have done many evaluations with NIAP of operating systems, and they included FDP_RIP, none of the disks were encrypted, and the evaluations were accepted [Kurth]
 - If you don't use FDP_RIP for removed data, what do you use? [Sukert]
 - You can use it, but it is difficult to satisfy because you get into scheme-specific interpretations of how to protect data from offline analysis. It is not just for deleted data, it is for all data, because if you mark data for deletion but leave it on the disk, what is the difference between that and live data? [Kurth]
- In the FoPP, we had some concerns about referring to data coming from another TOE. The concern was that it made a dependency between PPs.
 - You could use import/export functions, but in your case it is one TOE. You should not represent the different parts of the family of PPs as TOEs, they should be represented as "parts of the TOE". [Kurth]
- We were wondering what to do if NIAP will only accept P2600.1, can we do the others in BSI? [Aubry]
 - It is possible, we would need to talk to the schemes. [Kurth]
 - How about if we do P2600.1 in NIAP, and also do all four of them in BSI? [Nevo]

- It is also possible, again we would need to talk to the schemes. [Kurth]
- If we do P2600.1 in two schemes, is that OK? The one in NIAP would likely have a different title but could otherwise be the same.
- I think there has been a case where one PP was validated by two schemes [Kurth]
- Are there some unpublished work packages during an evaluation? [Cybuck]
- We could submit the same work packages to both schemes, other than perhaps changing the title and references to a particular scheme [Kurth]
- What about evaluator's comments? [Cybuck]
- Those might be different, but it would not matter [Kurth]

{walkthrough of the explanatory document}

- We have some conformance rules in the FoPP that say you must include some PPs if you have certain functions in your product, and the schemes haven't complained. We plan to do something similar in the packages approach. Are there CC issues with that?
 - It is not addressed by the CC. We brought up something like that with BSI, and they said it was not allowed, but we countered that it was also not prohibited. Since it made sense to do, it was OK [Kurth]
- We have misused the concept of subjects and objects in the FoPP
 - It is used, for example, in multilevel operating systems where a user authenticates and then specifies their role, and then the user plus role inform the subject operating system process of what security attributes to apply. In your case, you can use a default that user attributes and subject attributes are identical. If an ST needs to, it can refine that. [Kurth]
- Referring to the prototype, is there more that we would see in a complete draft? [Aubry]
 - Maybe some diagrams, certainly some app notes, but not more rules that I know about.
- critical item is to get IPA decision
 - get a whitepaper from atsec and send to IPA
 - evangelize the packages approach to other schemes and get their endorsement
 - get the packages approach on the CCDB agenda
 - update/improve the prototype draft

Production Printing environment/PP update [Lewis]

Refer to document:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.5-34a.pdf>

- This is updated to include the updates to PP-A version 34a, one version behind the current draft
- Not much else to report; waiting further news from Harry Lewis and AFPC

Schedule review [Wright]

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2008.ppt>

{Schedule has been updated}

Next meeting details [Wright]

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2008.ppt>

and to the meeting web page for most current status of upcoming meetings:

<http://grouper.ieee.org/groups/2600/meetings.html>

- P2600.1/2/3/4 PPs are under change control
- Deadline for posting documents: June 9 2008
- Deadline for posting comments: June 16 2008
- Next meeting will be June 23-24 at the Radisson Hotel and Conference Center Longmont – Boulder in Longmont CO.
- No hotel arrangements have been made.
- PWG will meet at the same location June 25-27.
- In addition to the usual P2600 RSVP, register through PWG (estimated meeting fee is \$65/day). Refer to the P2600 meetings page for details.

Closing [Wright]

** Adjourned at 12:00PM, 5/22/2008 **