

**IEEE P2600 Meeting #19**  
**May 23-24, 2006**  
**Hôtel Atala, Paris, France**  
**(arranged by Océ)**

**Attendees**

Chair: Don Wright, Lexmark  
Vice Chair: Lee Farrell, Canon  
Secretary/ Lead Editor (PPs): Brian Smithson, Ricoh  
Lead Editor (Clauses): Jerry Thrasher, Lexmark

Carmen Aubry, Océ  
Nancy Chen, Oki Data  
Nick Del Re, Canon  
Matthieu Helder, Océ \*  
Ron Nevo, Sharp  
Rob Robinson, Oki Data Europe \*  
Brian Volkoff, HP

\* first-time attendees

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 editorial comments may  
appear in these minutes, indicated by {braces}, inserted by the Secretary  
for clarity.

**\* Commenced at 9:05 AM 05/23/2006 \***

**Administrivia [Wright]**

The following administrative items were reviewed:

***Agenda review***

Refer to meeting slides for detail  
<http://grouper.ieee.org/groups/2600/presentations/P2600-May2006.ppt>

***Minutes and Agenda approvals***

The April 2006 minutes were approved without changes.  
The May 2006 agenda was approved without changes.

***IEEE patent policy***

Patent policy was reviewed. There were no patent disclosures made by  
attendees.

### ***Inappropriate topics review***

Inappropriate topics criteria were reviewed. Refer to meeting slides for detail:

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2006.ppt>

### ***Officers and Editors***

No changes in Officers:

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary: Brian Smithson, Ricoh.

However, it was acknowledged that Jerry Thrasher has been acting as a lead editor, and it has been decided that Mr. Thrasher will be lead editor for P2600 clauses and Mr. Smithson will remain lead editor for Protection Profiles.

### ***Meeting schedule update***

**Jun 19-20**, with PWG and TCG HCWG, Camas WA at Sharp

TCG will likely meet at a nearby HP facility

**Jul 26-27**, Rochester NY at Xerox

**Sep 6-7**, Boulder CO at IBM

There was a potential change for this meeting, to September 19-20.

Smithson noted that this would conflict with ICCC 2006.

**Oct 23-24** with PWG, Lexington KY at Lexmark

**Dec 11-12** with PWG, Orange County CA at Canon

No other schedule conflicts or issues were identified during this meeting.

### **INCITS CS1 update [Thrasher]**

- Executive board approved a project to create "minimum security guidelines for protecting personal privacy and etc", an ANSI tech report
  - to be submitted later as ISO standard
  - draft in August
- JTC1 SC28 plenary, Wright presented P2600 update

### **Action items from previous meeting [Wright]**

Refer to slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2006.ppt>

and to pre-meeting and post-meeting action items file for status of action items:

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20060519.xls>

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20060607.xls>

- June meeting info on web site, more to come
- merged docs 1-9 done
- new names in all PPs
- PP-A converted to medium robustness EAL3
  - not done
- paying for evaluations
  - DAPS can pay 10-20K
  - Lexmark at least 5K-10K
  - Ricoh mgmt is positive, likely good for 10-20K
  - Canon wanting to know what is the benefit
  - Sharp wondering also
  - Oki doesn't know yet
  - Oce talking to mgmt
  - HP also likely, mgmt is positive
- CC information
  - CCV3 version will happen in July
  - Part 2 will be based on v2.3 but modified
  - Subject/object/etc may or may not be included
  - "SEP and RVM will be removed and FCS may be incorporated into other functional requirements"
- PP-D threats/assumptions have been added back in
- Action item spreadsheet was also reviewed (see pre-meeting action items file listed above)

## **Email issues [Wright]**

Refer to slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2006.ppt>

- NIAP policy letter 13 [email from Sukert]
  - See <http://niap.nist.gov/cc-scheme/policy/ccevs/policy-ltr-13.pdf>
  - regarding acceptable TOE
  - cannot exclude any part of the product from the TOE, or justify why [Smithson]
  - need to reword 1.2.1 in PPs [Thrasher]
  - also look at wording elsewhere to ensure that PL13 is obeyed [Thrasher]
  - maybe an app note for ST writers that says they must include all available functionality in their product, or else they cannot base their ST on this PP [Smithson]
- Threat agent (actor) [Smithson]

- See  
<http://grouper.ieee.org/groups/2600/presentations/Paris/Threat%20agents.doc>
- Our threat descriptions include all of the conventional elements of a threat vector except for a complete description of the agent, or actor
- We cover equipment and expertise, but don't describe anything about the nature of the actor
- Boiled it down to four types
  - ANON is a machine or person that may be anonymous
  - AUTH is a machine or person that must be authorized to perform some kind of HCD operation
  - PRES is a physical attack that requires the actor's physical presence during the actual attack
  - REM is a physical attack that requires presence to set it up but the actor may (or may not) be absent during the actual attack
- These tags were added to the list of threats in the subject document
- Also proposed is that the detailed threat descriptions be re-ordered so as to be most logical in their presentation
- (group discussion)
- Accepted [Wright]
- Plain english SFRs [Chen]
  - NIAP said they want formal language, but we can put plain English in an application note [Wright]
  - but that leaves it too free to ST writers [Chen]
  - we make it as specific as we can, but not requiring implementation [Smithson]
- CIM vs our definitions for C,I,A,N-P [Sukert]
  - Neither is completely consistent with itself, but our's tends to refer to conditions and NIAP's tend to refer to policies, we would need to look at how we use the terms to see which is more appropriate [Smithson]
  - (additional group discussion)
  - use both [Wright]

## **P2600 clauses 1-8 review [Thrasher]**

Refer to original file:

[http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\\_P2600\\_v19b\\_ncb.pdf](http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v19b_ncb.pdf)

- participant list needs an update
  - proposed: list only those who had voting right has at one time EXCEPT those who were at one of the founding meetings
  - should make the web site list the same?
  - yes

- 1.4 how to use this standard is covered in 4.4.4
- "operational environment B is typically a whatever environment" <-- better word for environment?
- decided to remove some refs to HIPAA/etc, too US centric
- DOS is low priority for OpEnv A?
  - should be changed to moderate
  - Brian S will go through old spreadsheets and figure out what happens in Annex E
- change def of T.DOS.FAX.LOOP to "sending or receiving" -- applies to any PP?
- Changes were made in place and after review

Refer to updated file:

[http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\\_P2600\\_v20a\\_working.pdf](http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v20a_working.pdf)

## **P2600 clauses 9 review [Thrasher]**

Refer to original file:

[http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\\_P2600\\_v19b\\_ncb.pdf](http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v19b_ncb.pdf)

- ordered list vs unordered lists [Wright]
- what to do with recommendation entries where there are "none"? [Wright]
  - how about putting the rationale for why there are no recommendations? [Robinson]
  - OK [Thrasher]
- should the paragraphs be fully justified?
  - IEEE style guide doesn't specify, but its example is fully justified (as is the style guide itself) [Smithson]
  - the template is justified also [Thrasher]
- Changes were made in place and after review

Refer to updated file:

[http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\\_P2600\\_v20a\\_working.pdf](http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v20a_working.pdf)

## **PP-D review [Aubry]**

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-d-19b.pdf>

- update actor definitions to be consistent with PP-A [Wright]
- what about those definitions that aren't needed in this profile?
  - Would be best to leave them in until the end and then clean them up (in all PPs) [Smithson]
- roles in PP-D, roles like administrator may be the same as user
  - we should have a general statement that roles are distinct from people in all PPs [Farrell]
  - note after Actor table should appear in PP-A,B,C [Wright]

- we should have an app note in section 2 about why we included EAL2 stuff in an EAL1 PP – so that ST authors know they can use them or not [Smithson]
- what about threats/assumptions/objectives with same name, different meanings in PP-A,B,C,D? [Nevo]
  - (good point, no resolution?)
- minor edits made during the meeting, changes accepted

Refer to updated file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-d-19c.pdf>

## PP-C review [Chen]

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-c-19a.pdf>

- misc action item changes
- are SFRs ccv3 compliant? [Wright]
  - yes, for EAL2+
- Matthieu was unclear about whether users needed to be authenticated at the time they submit a print job, or just at the time they want to retrieve the job [Aubry]
  - they need to auth to submit, because (1) it identifies the owner of the data for subsequent auth to retrieve and (2) so an anonymous user can't submit malicious jobs [Smithson]
  - we should make that explicit in the PPs [Aubry]
  - maybe in an app note? [Chen]
- minor edits made during the meeting

Refer to updated file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-c-19b.pdf>

## PP-B review [Nevo]

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-b-19a.pdf>

- issue of difference between PP-A and PP-B -- PP-A needs to require encryption, PP-B needs to NOT require it
  - there isn't a practical alternative for mitigating T.UD.SNIFF [Aubry]
  - action item to PP editors to resolve
- PP-A and PP-B need to modify T.UD.PHY.OUTPUT in table 11 (to correspond with changes in table 10)
- are SFRs and SARs up to date for ccv3 eal2? [Wright]
  - yes
- minor edits made during the meeting

Refer to updated file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-b-19b.pdf>

## PP-A review [Smithson]

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-a-19a.pdf>

- need to merge T.TSF.CRED.DISK in table 11 back into T.TSF.CRED
- SFRs/SARs need to update to EAL3
- minor edits made during the meeting

Refer to updated file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-a-19b.pdf>

## **Standard versus Recommended Practice? [Wright]**

- look for shalls, etc
  - standards must have them
  - otherwise we are a recommended practice [Thrasher]
- what are we trying to be? [Farrell]
- put some shalls in clause 8/9, maybe saying you shall do one of the recommended practices [Thrasher]
  - there's a danger that we don't have exhaustive lists of all possible options [Smithson]
- I thought that we'd be requiring one of PPs, not certification but conformance [Smithson]
- we'll put it on the discussion list for next meeting [Wright]

## **Closing [Wright]**

See you in Camas, WA \* **Adjourned at 2:10 PM, 05/24/2006** \*