

**IEEE P2600 Meeting #20**  
**June 19-20, 2006**  
**Sharp Labs, Camas, WA**

**Attendees**

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

Peter Cybuck, Sharp  
Nick Del Re, Canon  
David Freas, DAPS  
Tom Haapanen, Equitrac  
Harry Lewis, IBM  
Ron Nevo, Sharp  
Alan Sukert, Xerox  
Brian Volkoff, HP  
Bill Wagner, Konica-Minolta  
Craig Whittle, Sharp  
Sameer Yami, Toshiba

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 06/19/2006 \***

**Administrivia [Wright]**

The following administrative items were reviewed:

***Agenda review***

Refer to meeting slides for detail  
<http://grouper.ieee.org/groups/2600/presentations/P2600-June2006.ppt>

***Minutes and Agenda approvals***

The May 2006 minutes were approved without changes.  
The June 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. No issues were identified.

Refer to meeting slides for detail:

<http://grouper.ieee.org/groups/2600/presentations/P2600-June2006.ppt>

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

No changes in Officers:

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary: Brian Smithson, Ricoh.

Editor (clauses): Jerry Thrahser, Lexmark.

Editor (PPs): Brian Smithson, Ricoh.

### ***Document Management***

As we merge documents into a single standard, older documents will be moved to a new "historical" section.

A private area on the P2600 web site has been established. When we have a complete standard composed of all documents, it will be put in the private area. The private area is password-protected for web access.

Those who can access the web site using SFTP will be able to access it as before.

The password for the private area was announced at the meeting, but it will not be published in these minutes nor sent to the email list (for obvious reasons).

***If you need to know this password, contact Don Wright or Brian Smithson by private email.***

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

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

*Note that the airport code is ROC*

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

At present, it appears that there will be NO Internet access for attendees at this meeting.

There had been a potential change for this meeting, to September 19-20. Smithson noted that this would conflict with ICCS 2006. This change is no longer necessary, and so we will meet as previously scheduled, September 6-7 in Boulder CO.

**Oct 23-24** with PWG, (and other printer-related groups) Lexington KY at Lexmark

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

No schedule conflicts or issues were identified during this meeting.

A schedule for 2007 has not yet been proposed. It is expected that we will not need to meet as often in 2007 as in previous years.

### **Schedule update [Wright]**

- Clauses 1-9
  - merged
  - review in May and June
- PPs
  - Waiting for July draft of CCv3.1
  - Into the PPs by September?
  - PPs reviewed and iterate 1-2 times
- Complete draft in December meeting
- January 2007
  - Form IEEE ballot body
  - Engage CC eval lab(s)
- February
  - Start balloting
  - Start evaluation of PPs
- April (will require a meeting)
  - Reconcile comments from IEEE and eval labs
- May – June – July
  - Recirculations
- September
  - RevCom / Standards Board Approval

### **TCG update [Volkoff]**

- use cases done
- still soliciting participation
- no significant changes since last update
- are use cases public? [Wright]
  - are private to TCG but can be made available on a case-by-case basis

- when marketing puts HCWG on front page, then will likely be published
- can use cases be released to P2600? [Wright]
  - may be able to get approval for that
  - some have been distributed individually
- will HCWG be on web page soon? [Farrell]
  - yes, probably in a month
- HCWG is meeting this week? [Wright]
  - yes, at HP site

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

- Nothing significant since last P2600 meeting
- Next CS1 meeting is in August

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

Refer to slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-June2006.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-20060616.xls>

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20060630.xls>

- PP evaluation funding
  - Sharp still wondering about the benefits of funding
  - general action item was assigned, not to anyone specific
  - HP was wondering why to pay for PP-C and PP-D?
- CCV3 update from NIAP?
  - No
- Should P2600 be a Standard or a Recommended Practice?
  - The issue is that standards predominate "shall", recommended practice "should"
  - can it be both? [Smithson]
    - needs to be one of standard, recommended practice, or guide
  - as currently written, reviewers may say that there are not enough compliance items to be a standard
  - can there be a standard part and a recommended practices part? [Nevo]
    - if you have compliance reqts and recommendations, it would typically be a standard
  - if we say an HCD shall be compliant with PP-A,B,C, or D, that would have a lot of requirements
  - what if we said that mfr shall do one of the recommended practices? [Thrasher]

- practices are not all inclusive to address a threat [Smithson]
- can't we just use the SFRs in the PPs?
- if we use PPs for compliance reqts, how would one claim compliance? specific to op env? or could you say you are compliant with P2600 but only comply with PP-D? are there other standards that have different levels of compliance? [Smithson]
- we wouldn't require actual certification by a lab [Smithson]
  - yes, we would not require CC certification and IEEE doesn't police compliance
- we resolved to create a Clause 10 to be prototyped for discussion at the July meeting
- AI #198
  - I proposed something about that, but not as a PP team effort, in a document I posted on Friday [Smithson]
    - it is on the agenda for review
- Action item spreadsheet was reviewed and updated {see files}

## Email issues [Wright]

Refer to slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-June2006.ppt>

- T.UD.PHY.OUTPUT [Smithson]
  - Issue was why are O.I&A, O.ACCESS, and O.MONITOR objectives to mitigate removing a document from the output tray. If we don't require mechanical mailboxes or an access-controlled print mechanism, then the objectives should be only training users and putting the device in a visible location.
  - Why don't we require solutions like that? Most of the manufacturers have them available. I think it's a big security hole. [Haapanen]
    - Are the kinds of things you're suggesting things that manufacturers can do? Or are they IT requirements? [Wright]
    - Manufacturers offer them and we could test compliance [Haapanen]
    - For example, send a job and receive a PIN code that must be entered to release the job [Nevo]
  - One of the issues is that T.UD.PHY.OUTPUT is included in all PPs, and I don't think we'd want to require this kind of solution in all environments.
    - Certainly not in SOHO. [Haapanen]
    - I don't think even in Public. There's no implied guarantee of privacy in that environment. [Smithson]
  - Which ones would be appropriate objectives? [Wright]
  - O.ACCESS [Nevo]
  - Not O.I&A or O.MONITOR? [Wright]

- No, it's not the same kind of authentication, it's just a simple PIN [Nevo]
- Do we want to force this capability to be in every product? Or should you leave it up to the manufacturer to add it to their ST? [Thrasher]
  - I think it's a requirement for OpEnv A. [Wright]
  - Maybe for B it has O.ACCESS, and A has O.I&A also [Nevo]
- But if you have, for example, a simple printer in an A environment. Maybe it's in the HR director's office, so it needs to be in the A environment, and yet it is sitting next to their desk and their office is locked when unattended. Do they really need locked print? [Smithson]
  - Wouldn't SOHO be OK? [Haapanen]
  - Then it wouldn't have the network protection, [Thrasher]
- If you require that files are stored on the device waiting for release, that's a problem in some environments. They don't want documents hanging around on the device. [Cybuck]
  - That's not the requirement. It could be stored on a server. Or some other method, but it requires some identification to release. [Wright]
- There is no way that the PP can have a strong recommendation. It is just in or out. [Thrasher]
- Can we agree that OE.LOCATION is sufficient for B, C, and D? [Thrasher]
- I think O.ACCESS is required for B. [Nevo]
- So that would apply to all kinds of devices, simple printers, FAX machines, even copiers even though we know that the person is standing there making the copy. How are we going to describe that? [Smithson]
- It should just be printing or fax receive. [Nevo]
- The threat is written as "output tray", so we'd need to rework the threat. [Smithson]
- For fax, you'd put all incoming faxes into the secure box? [Thrasher]
- How would you know who it is to? [Smithson]
- Someone could turn it off if they want. Or else, you could turn off fax by default and require they turn it on [Haapanen]
- We'll need to think about that in relation to the Policy #13 discussion about TOE rules [Thrasher]
- Can we say that these are tentative decisions? O.ACCESS required for A and B, O.I&A also for A, OE.LOCATION and OE.TRAIN also needed for all? [Wright]
- I think they need to be tentative. I'm not comfortable agreeing to these until I've talked to our marketing and development people. [Smithson]

- If we use some kind of access control device for releasing print jobs, do we still need OE.LOCATION? Does the device fulfill that objective? [Haapanen]
- OE.LOCATION is up to the environment, not the TOE. [Thrasher]
- So would you still need it? [Thrasher]
- I guess not, we could remove OE.LOCATION in cases where we have O.ACCESS. I also propose that we have OE.TRAIN along with OE.LOCATION. [Smithson]
- I'm not sure OE.LOCATION belongs in C. By definition, you can't require OE.LOCATION. [Sukert]
- It's monitored. [Thrasher]
- But not for that. So maybe only OE.TRAIN belongs in C. [Smithson]
- Summary of tentative decision, to be discussed at July meeting:
  - A. O.ACCESS and O.I&A
  - B. O.ACCESS
  - C. OE.TRAIN
  - D. OE.TRAIN and OE.LOCATION
- Secure fax [Yami]
  - We don't secure fax in any PP. Is that OK, or should we:
    - require some kind of encryption/authentication
    - require disabled fax?
  - we can't require secure fax, because there is no interoperable standard that is implemented within the TOE [Cybuck]
  - so we could require turning it off by default or not installing it [Thrasher]
    - that's a major function of an MFP [Yami]
    - some customers require no fax installed [Wright]
    - some require that there be no INTERFACE even [Cybuck]
    - our customers are concerned about FAX-network connections and are usually satisfied if the FAX modem cannot bridge to the network [Freas]
    - another issue is how strong is the administrator authentication required to turn it on or off? [Cybuck]
  - there was discussion about secure fax over Internet, is that something we can consider? [Wright]
    - it's not really fax, it's just a tiff file [Thrasher]
    - there are third-party services that offer it, it's almost like scan-to-email [Smithson]
  - there is no way to write the threat to say that does not apply to a particular interface? [Thrasher]
    - We already did it, we have T.UD.SNIFF.NET for network traffic but no T.UD.SNIFF.FAX [Smithson]
  - We haven't included any fax threats, but we agree that fax is inherently insecure, yet you can certify a device with a fax installed [Haapanen]
    - That's the way it is currently written [Smithson]

- If we had a requirement in profile A, then you couldn't certify with the fax installed. Most devices, the fax is optional I think [Haapenen]
- Threats map to objectives and SFRs. Once it gets to that stage, is the evaluator going to care? [Thrasher]
- A good evaluator may look at the whole device, including fax, or flag that there is a piece of functionality in that class of device that isn't accounted for in the threats. So our options are: [Smithson]
  - leave as is
  - require FAX disabled by default but can be turned on
  - require FAX not installed at all
  - require no FAX interface at all
- we shouldn't tell companies that they can't do something (like offer FAX) in a certified product. We can set some minimum requirements and let manufacturers add to that, but we shouldn't preclude certifying a product that includes fax [Sukert]
- documents are protected once they are on the TOE [Yami]
- is an evaluator going to flag the inconsistency that we protect data over network but not over phone line? [Thrasher]
  - we can claim whatever we want [Nevo]
  - when the evaluate the profile, won't they see that hole? [Wright]
  - especially in light of policy #13 [Thrasher]
  - one of the bigger objections to fax is that something executable could be transmitted [Cybuck]
- we also threw out T.DOS.FAX, and we could put that back in to the same extent that we support T.DOS. everything else [Smithson]
- I think we could rationalize the inconsistency of network versus phone lines because there are established interoperable standards to handle that, but it would be more difficult to rationalize the DOS thing [Smithson]
- does anyone now have certified product with FAX? [Wright]
  - Yes [group]
- does anyone claim protection of data on phone lines? [Wright]
  - No [group]
- does anyone claim protection of data on network, but they have a fax and do not claim protection of data over the phone line? [Thrasher]
  - Yes [group]
- we need the fax bridge threat and T.DOS.FAX [Nevo]
  - used to be in T.EA.PROXY [Thrasher]
  - not in current definition [Sukert]
  - it was meant to be covered by T.EA.PROXY [Wright]
  - that's how it is written in the PP [Nevo]
  - but not in clause 7 [Sukert]

- we could expand T.EA.PROXY again [Sukert]
  - it should be its own threat, different vector, different mitigation [Smithson]
  - there is an Air Force policy, I will get a reference and send to the list [Cybuck]
- action is to add T.EA.FAXBRIDGE [Wright]
- NIAP policy letter 13 [Sukert]
  - See <http://niap.nist.gov/cc-scheme/policy/ccevs/policy-ltr-13.pdf>
  - regarding acceptable TOE
  - email of 6/12/06 included proposed text
  - would it be better to say that only the software that the manufacturer provides with the product being certified, not everything that's available? [Cybuck]
    - that's the intention of the policy [Smithson]
  - I added "and software"
    - The definition should imply inclusion of software [Wright]
  - What does the "or" clause mean? [Wright]
    - They have specific examples of how it comes into play for some specific products, like firewalls [Smithson]
    - How does that apply to hardcopy devices? [Wright]
    - I don't think it does [Sukert]
    -
  - Could we use the term "compliant configuration"? [Wright]
    - That's self-referential. How about "the entire hardcopy device as delivered to end customers"? [Smithson]
  - starts in file0094 at 1:00
- Elevation of DoS threats [Smithson]
 

Refer to <http://grouper.ieee.org/groups/2600/presentations/Camas-20/ThreatAnalysis-20a.xls> and <http://grouper.ieee.org/groups/2600/presentations/Camas-20/ThreatsAnalysisWorksheet-DOSchange.pdf>

  - DoS threats are listed in clause 7 as low importance in environment A and moderate importance in environment B. DoS threats are included in both PP-A and PP-B, but it looks inconsistent in clause 7. The action item was to look at the threat analysis worksheets to see whether there are unintended effects of elevating the base importance to moderate in environment B. There were no bad effects.
  - Is there anything that needs to be changed? [Wright]
    - I already sent the changes to Jerry [Smithson]
    - They have been incorporated [Thrasher]
- New PP-A section 3.1 [Smithson]
  - We agreed some time ago to put the CIM instruction #3 text somewhere in the PPs. However, the PP structure has changed and so we needed to decide where to put it in the PPs. I think it fits best in a new section 3.1 and placed it there in PP-A as an example.

- No problem with that [Wright]
  - It will need to be put in the other PPs, but they will need to use the basic robustness text.
- Unmodified? [Wright]
  - Yes, no modifications are needed.
- PP-A/PP-B proposals [Smithson]
 

Refer to <http://grouper.ieee.org/groups/2600/presentations/Camas-20/Proposal%20to%20P2600.pdf> and [http://grouper.ieee.org/groups/2600/presentations/Camas-20/camas\\_proposal.xls](http://grouper.ieee.org/groups/2600/presentations/Camas-20/camas_proposal.xls)

  - Started looking at how we deal with data that is stored on HCD (document and TSF) to see if the objectives really match up with the threats and if there are any holes or inconsistencies. I found a number of issues:
    1. O.DELETE is an implementation-specific objective. There are many ways to mitigate T.UD.SALVAGE besides deletion, such as encryption. We require O.PROTECT and O.DELETE, which seems redundant.
    2. O.PROTECT is for documents stored intentionally, and O.DELETE is for residual [Nevo]
    3. It's not quite written up that way
    4. T.TSF.CRED.DISK was recently re-integrated into T.TSF.CRED, but it is a very different threat vector and mitigation approach than the other T.TSF.CREDS. Also, we don't require O.DELETE even though we specifically refer to residual data. Also, it only refers to management data and not to user function data, which is a hole.
    5. We have mixed together threats that occur in the powered-on state and the powered-off state, but they are very different threat vectors. Powered-off threats can't make use of O.I&A, O.ACCESS, or O.MONITOR, for example.
    6. For powered-on threats, we require O.PROTECT but we also require O.I&A and O.ACCESS. If we really need O.PROTECT in the powered-on state, that means that we are assuming that O.I&A and O.ACCESS can be bypassed, and I think we should not make such an assumption.
    7. We still have some issues distinguishing PP-A and PP-B. The only threat differences are T.UD.SNIFF.EM and T.TSF.CRED.EM and T.UD.IMP.\*.
  - Proposed:
    1. Separate powered-off and powered-on threats. Change T.TSF.CRED.DISK to T.TSF.SALVAGE and expand its scope to include user function data.  
Limit O.PROTECT to be used only for powered-off threats, and eliminate O.DELETE as redundant.  
Rely on O.I&A and O.ACCESS for powered-on threats.

2. Remove T.UD.SALVAGE from PP-B. It was rated as having the same risk factor in PP-B and PP-C, and yet we don't include it in PP-C. However, T.TSF.SALVAGE would remain in PP-B.
  3. Remove T.TSF.AUD.ACCESS from PP-B, but leave T.TSF.AUD.ALTER. Rationale: we shouldn't care if the audit logs get read in PP-B, but in the more regulated environment of PP-A we would care.
  4. Remove T.UD.SNIFF.NET from PP-B. Its score was the same in PP-B and PP-C, but we chose to put it in PP-B and not PP-C. We'd leave T.TSF.CRED.NET in PP-B, which is consistent with the other changes.
- There are some implementation effects of these proposals, especially having to do with the need for document encryption. Refer to the documents for details.
  - This also smoothes out the difference number of threats between each environment.
  - Does this still maintain the hierarchical relationship of the PPs? [Farrell]
    - Yes
  - We haven't yet seen the results of making PP-A a medium robustness EAL3 PP. Would that be enough without these changes? [Thrasher]
    - Don't know yet
  - SALVAGE is an issue for me, because some DoD customers require deletion of data. Encryption doesn't fulfill their requirement [Freas]
    - Do they care about TSF data on the disks?
    - The regulations may be old and don't account for that. [Freas]
  - Since this was presented on short notice, let's discuss this between now and July's meeting.

## **P2600 clauses 1-6 review [Thrasher]**

Refer to original file:

[http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\\_P2600\\_v20a.pdf](http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v20a.pdf)

- Changes were made in place during review
- Some asset descriptions were changed that need to be incorporated into the PP asset descriptions

Refer to updated file:

[http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\\_P2600\\_v20b.pdf](http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v20b.pdf)

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

Refer to original file:

[http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\\_P2600\\_v20a.pdf](http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v20a.pdf)

- Changes were made in place during review.
- Several short descriptions of threats were altered (T.DOS.FAX.HOOK and .LOOP) which need to be incorporated into PPs.
- Also some long threat descriptions were altered.
- A new threat T.EA.FAXBRIDGE was added, but not all detail has been included yet.
- Should we add a reference to the ISO TR 15446? This would also be in the PPs.
- We considered adding T.DOS.FAX back into the PPs
- Changes were made in place and after review
- We ended at 8.1.1 because of time constraints.

Refer to updated file:

[http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE\\_P2600\\_v20b.pdf](http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v20b.pdf)

## **Closing [Wright]**

See you in Rochester, NY \* ***Adjourned at around 1:00 PM, 06/20/2006*** \*