

**IEEE P2600 Meeting #16**  
**January 16-17, 2006**  
**Imperial Palace Hotel, Las Vegas, NV**

**Attendees**

Chair: Don Wright / Lexmark  
Vice Chair: Lee Farrell / Canon  
Secretary/Lead Editor: Brian Smithson / Ricoh

Carmen, Aubry, Océ  
Peter Cybuck, Sharp  
Nick Del Re, Canon  
Tom Haapanen, Equitrac  
Harry Lewis, IBM  
Glen Petrie, Epson \*  
Ole Skov, MPI Tech \*  
Alan Sukert, Xerox  
Jerry Thrasher, Lexmark  
Brian Volkoff, HP  
Bill Wagner, independent  
Sameer Yami, Toshiba

\* first-time attendee

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 9:04 AM 01/16/2006 \***

**Administrivia [Wright]**

The following administrative items were reviewed:

***Agenda review***

Refer to meeting slides for detail  
<http://grouper.ieee.org/groups/2600/presentations/P2600-Jan2006.ppt>

***Minutes and Agenda approvals***

December's minutes and January's agenda were approved without  
changes.

## ***IEEE patent policy***

There is some new text in the IEEE patent policy statement. Essentially, the new text encourages disclosure of patent issues early in the standards process. Refer to meeting slides for detail:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Jan2006.ppt>

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-Jan2006.ppt>

## ***Officers and Editors***

No changes in Officers since December:

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary: Brian Smithson, Ricoh.

Editors:

Lead Editor (Smithson)

Clause 1: Overview (Wright)

Clause 2: Normative References (Wright)

Clause 3: Definitions (Sukert)

Clause 4: Introduction to Hardcopy Devices (Wright)

Clause 5: Security Environments (Cybuck)

Clause 6: Hardcopy Device Assets (Volkoff)

Clause 7: Hardcopy Device Threats (Thrasher)

\* Clause 8: Best Practices and Threat Mitigation (Haapanen)

Annex A. High Security PP (Smithson)

Annex B. Enterprise PP (Nevo)

Annex C. SOHO PP (Aubry)

Annex D. Public PP (Chen, Sukert)

Annex E. Password/PIN generation (clause 8, Haapanen)

Card authentication (clause 8, Haapanen)

Biometric authentication (clause 8, Haapanen)

Remote authentication (clause 8, Haapanen)

Algorithms and key sizes (clause 8, Haapanen)

Disk overwrite (clause 8, Haapanen)

Secure development processes (clause 8, Sukert)

Annex F. Informative References (clause 2, Wright)

Annex G. Bibliography (clause 2, Wright)

Annex H. Additional definitions (clause 3, Sukert)

\* Clause 8 was divided into two clauses during this meeting.

## ***Meeting schedule update***

**Mar 2-3**, Washington DC at IEEE USA Headquarters

L Street, between 18<sup>th</sup> and 19<sup>th</sup>

There is no hotel setup, you're on your own

TCG HCWG will meet on the previous day, Mar 1, at 9am

**Apr 2-3** with PWG, Mount Laurel NJ (near Philadelphia) at Okidata

**Note: the date for this meeting was incorrect in December's minutes**

Harry Lewis inquired about moving this meeting to one week later. He will follow up about that. At present, the current schedule stands.

**May 17-18**, Paris, France (arrangements being made by Océ)

**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

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

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

Aside from the April 2-3 meeting, no schedule conflicts or issues were identified during this meeting.

## **TCG update [Volkoff]**

- At the most recent conference call, we decided to co-locate at some upcoming P2600 meetings
  - DC
  - Camas
- Member meeting in Hawaii is coming up at the end of March
- Status: not much changed since last P2600 meeting

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

- There is an INCITS CS1 meeting on 2/1/2006 in San Jose
- They are revisiting the minimum security reqts for info stored on networked computer
  - getting some opposition from NIST and NSA
  - the objection is that these requirements aren't based on risk assessment, they're just a bunch of "yea, verily" statements
- They are also doing something with dynamic access control, an extension of RBAC

## Action items from previous meeting [Wright]

Refer to slides for detail:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Jan2006.ppt>  
and to pre-meeting action items file:

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20060113.xls>

- General items
  - updated techdocs page
  - jan and march meetings finalized
- Spreadsheet items
  - some of the older PP action items may be obsolete or different -- I'll review before next meeting
  - see post-meeting sheet for others
  - AI #81 invite NIAP to some part of March meeting
  - AI#108 changed to "sections", is that what it should be in a PP? IEEE wants "clause"
  - how to get styles straightened out?
    - Thrasher will do 1-4, 6, and 7, and repost them
    - Cybuck will do 5, tom will do 8
    - Smithson will do PPs
  - Smithson to post DOC files for 12a annexes, jerry will update
- Aubry identified some problems with old content that has crept back into pp-h-15a

## Email issues [Smithson]

- We need to decide if we adopt NIAP's threat/assumption/policy names
  - they have better names (they are in verb form)
  - ours have structure and we'd need to make lots of changes
- New CIM information is similar to v2 CIM, some name changes and a few other changes [Aubry]
  - Yes, there are many similarities, and this list seems to include basic and medium robustness items [Smithson]
- "Customer engineer" is not in Enterprise PP
  - Add it [Wright]
- There is a note about maintenance ports in Pub PP which isn't in the others
  - Add it to HVA, SOHO, and Ent [Wright]
- NIST vs P2600 Clause 5 references in introductory sections of PPs
  - Strike " Those environments are defined within the Protection Profile documents, and their definitions are based on guidelines established by NIST." from PP forwards

## Clause 2 review [Wright]

Refer to:

<http://grouper.ieee.org/groups/2600/drafts/Clause2/clause2-15a.pdf>

- need help on normative and informative references
  - clause and PP editors: review and suggest if any belong in the other category
- need to look at annexes
- clause editors: going forward, if you add a reference you should send it to Don Wright
- bibliographic citation style needs to be looked at in IEEE style manual

## Clause 3 review [Sukert]

- Edits were made in place
  - Refer to original document:  
<http://grouper.ieee.org/groups/2600/drafts/Clause3/clause3-14a.pdf>
  - Refer to edited document:  
<http://grouper.ieee.org/groups/2600/drafts/Clause3/clause3-14a.doc>
- firmware definition
  - Persistent computer instructions and data embedded in the HCD that can control ... (see clause 3 update)
  - update also in PPs
- media definition
  - should refer to paper, transparencies, etc
  - change other uses of the word to something else, like storage device or (what for drums/belts?)
- kilobits per second
  - should be Kb/s not Kbps in clause 8
- other minor changes made in place
- terms and definitions need to be formatted in IEEE style

## Clause 8 review [Haapanen]

- Edits were made in place
  - Refer to original document:  
<http://grouper.ieee.org/groups/2600/drafts/Clause8/clause8-15a.pdf>
  - Refer to edited document:  
<http://grouper.ieee.org/groups/2600/drafts/Clause8/clause8-16a.doc>
- Request to split out Best Practices part of clause 8 into a new clause 9
  - No objections [Wright]

## Clause 5 review [Cybuck]

Refer to:

<http://grouper.ieee.org/groups/2600/drafts/Clause5/clause5-15b.pdf>

- noted that not all HVA environments are large enterprises
  - some are islands, some are small standalone businesses
  - need another description and graphic
- reviewed / accepted changes
- should capitalize environment names: High Value Asset, Enterprise, etc.
- change "Profile" to "Environment" or "Protection Profile", as appropriate

## Public PP review [Sukert]

- changes include both Alan/Nancy and Brian, from meeting 15
- Edits were made in place
  - Refer to original document:  
<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-p-15b.pdf>
  - Refer to edited document:  
<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-p-16a.pdf>
- do the terms/defs need to be in IEEE style?
  - table styles were from IEEE, but term/def table isn't right [Smithson]
  - is there a format for PPs? [Wright]
  - no, they seem to be variable [Smithson]
  - so an evaluator wouldn't have a problem with IEEE style [Wright]
- how to deal with scope in the case where the HCD boots over the network? [Aubry]
  - would need to certify the network parts also as part of the TOE [Wright]
  - would be difficult to certify [Cybuck]
  - it's outside of the HCD, so it couldn't use this PP [Wright]
  - it would be like a firmware update or maybe applet load as long as the image is the same every time [Thrasher]
  - that brings up an issue, if you update the firmware then it is no longer the same [Wagner]
  - then you are no longer certified, unless you have certified that version [Wright]
  - you'd use a "continuity certification" to get the upgrade certified [Smithson]
- section 2 text got scrambled in Pub PP
  - 2.4 needs to also refer to other PPs and we had some text describing what Demonstrable meant

- Need to apply to other PPs [Smithson]
- T.TSF.CONF needs a note that it doesn't include .AB
  - in other PPs we didn't list exclusions. [Smithson]
  - for T.???.\* threats, list the included ones in the description field -- see Pub PP T.TSF.CONF for example
- get more from audio
- OE.NET\_MANAGE doesn't have a parenthetical description
  - use "Network management"
  - apply to all PPs
- subjects, objects, and operations
  - need to reconcile naming conventions
  - need to use D.\* for subjects (see section 6)
- what is FDP\_ISA used for? in real life?
  - Find out from NIAP
- need to deal with NETWORK\_INBOUND(/OUTBOUND)\_POLICY
  - is a subject? object?
  - which objects need access control?
    - AI124
    - apply to other PPs
- EAL2 extended -- ALC\_FLR.2 needs to go in all PPs
- ADV\_ARC subheadings should be H4's
  - apply to other PPs?
- same for ADV\_TDS, PRE, etc.
- rationale section still has app notes in the first three paragraphs -- need to move them

## Environment Definitions Proposal [Smithson]

Refer to:

[http://grouper.ieee.org/groups/2600/presentations/LasVegas/Environment\\_Definition\\_Proposal\\_2.ppt](http://grouper.ieee.org/groups/2600/presentations/LasVegas/Environment_Definition_Proposal_2.ppt)

- Basis for discussion is NIAP's issue with our definition of operational environment
  - High Security meant something special to NIAP
    - "High Security" means EAL 6-7 [Cybuck]
  - High Value Asset was a problem because it's a relative term. Everyone thinks their assets are highly valuable.
- What we seem to really be distinguishing in our current environments is the level of accountability provided by the TOE.
  - In a SOHO environment, there is little accountability. If you're on the network, you can use the resources. Often no logins. No accounting records. There are basic security protections, but if you're in the door, you can do anything.
  - In the Public environment, you're dealing with temporary or transient users, so you don't need to specifically identify them, but

- you need to authorize them (such as if they've paid) and you need to keep track of activities for billing/account purposes.
- In Enterprise, you have people log in individually, and you track exceptions and unsuccessful activities – security events.
  - In what I'm calling the Auditable operational environment, you do all of that and you're logging everything – successful events included – so that someone can perform any kind of audit. You also have an individual role for an auditor.
  - How do you define “accountability”? [Farrell]
    - Assigning responsibility for actions to an individual or entity.
    - How do you measure that? This person is more accountable than that person? [Farrell]
      - Not so much the person, but the device provides the mechanism for accountability.
  - If you substitute “accessibility” for “accountability”, does it still work? [Cybuck]
    - Accessibility is often associated with section 508 things [Wright]
    - Accessibility is one aspect of it, but by itself it doesn't cover logging. You could have very good access controls but no records, and you wouldn't be auditable.
  - How about “managed”, or “controlled”? [Wright]
    - I thought about those, and also “regulated”.
    - But nobody would want the “unmanaged” or “uncontrolled” one [Wright]
    - Maybe we should have color codes or numbers or something, instead of names. [Wright]
  - Aside from the names, do you think this is the right way of describing things? There is some impact, in clause 5 and elsewhere.
    - There may be confusion between auditing and accounting. [Wright]
  - This fixes some things, but may create new problems [Wright]
  - It's multi-axis and you're trying to collapse it into one axis [Petrie]
  - Impact: there would be some changes where these environments are defined, primarily in clause 5 and the PPs
  - I think there may be a marketing value if these definitions more closely match actual market segments.
    - I think the marketing point of view is important, but I don't know that this is substantially better than what we have [Farrell]
  - We went through a whole analysis with DREAD and STRIDE, and every risk analysis has asset value as its basis, and this approach seems to go away from that. [Thrasher]
  - Maybe we could call it the “regulated asset” environment, but that does limit it to regulations. [Wright]
  - I think we can say that because of the value of the assets, their use needs to be accounted for. And the higher the value of the asset, the more effort and time can be spent by an attacker [Wright]

- That's not entirely true. My medical records aren't inherently valuable, nobody's going to mount a sophisticated attack to get them, but the cost of disclosure to a HIPAA regulated enterprise would be high.
- With no consensus to accept this proposal, I'll let it go but ask that we incorporate some of these ideas into our descriptions of the existing environment as currently named.
  - Could we call it a "special asset" environment? [Wright]
  - What we're trying to get at is the cost of compromise, and I can't think of a word for that [Wagner]
  - If we use a general word, it forces them to read the text at least [Wright]
  - I think SOHO and Public are very descriptive, Enterprise is somewhat descriptive, so it would good to have another name that was at least somewhat obvious.
- How important is this problem that we're trying to solve? [Petrie]
  - They are mostly not happy with our names, especially High Security
  - Do we need to pay attention to it, or can we let it slide? [Petrie]
    - I think we can let it slide, but I also think NIAP has a point.
- OK, so we leave it alone for now.

## Clause 9 review [Haapanen]

Refer to:

<http://grouper.ieee.org/groups/2600/drafts/Clause9/clause9-16b.pdf>

- change Security Environment to Operational Environment (all docs)
- how many best practices are also in clause 8 mitigations?
  - quite a bit of overlap
- are there unique items in clause 9 that aren't in clause 8? [Wright]
  - yes, some -- like design and architecture [Smithson]
  - suggestion: bring the annexes back into clause 9 to give it more unique value [Wright]
  - another suggestion: remove the redundant material in clause 8 and make references to clause 9 [Smithson]
  - another suggestion: make the whole clause 9 into an annex [Thrasher]
    - or an informative clause [Wright]
  - Wright will look at merging the annexes (including secure development) into clause 9 [Wright]

## SOHO PP review [Wright]

- Edits were made in place
  - Refer to original document:  
<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-s-15a.pdf>
  - Refer to edited document:  
<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-s-16a.pdf>
- need to apply changes made to SOHO in 16a to other PPs
- O.NETWORK needs a parenthetical description (4.1.3) [Smithson]
- There is an issue with inbound/outbound filtering because it requires user authentication, which isn't required in SOHO [Aubry]
  - For SOHO devices, I agree [Wright]
  - How we mapped threats in SOHO, we didn't consider either credentials or user data needing protection. [Thrasher]
  - O.NETWORK has two parts, one related to protecting data in transit and the other having to do with inbound/outbound traffic. [Aubry]
  - T.UD.ACC.HACK was about using non-standard interfaces, which I don't think translates into port filtering. That's about turning physical connections off. If port filtering is just a matter of saying that I only accept connections on port 443, that's not so unreasonable for a SOHO device. [Thrasher]
    - Are people going to actually configure such things? [Smithson]
    - Depends on how are you going to ship it? [Wright]
    - Wide open, but I could see how you'd pop a CD in the drive and a wizard would walk you through which interfaces you're going to use and it would turn off the rest [Smithson]
    - That would be more user friendly for SOHO to have such a wizard. [Wright]
    - A web utility might have a secure mode and an open mode. Maybe not port-by-port. [Thrasher]
    - What threats does this mitigate? [Smithson]
    - T.UD.ACC.HACK. [Thrasher]
    - Someone needs to come back with a proposal for SOHO with everything complete. Maybe not correct, but complete and consistent [Wright]
    - If this is a forward-looking standard, a wireless device at home may have a large range and that may become the attack point for your network [Cybuck]
- What about t.ud.phy.output where you need to protect against reprints? If you don't identify users, how do you know if it is an unauthorized reprint? [Wright]

- Did we keep T.UD.ACC.NORMAL just to have something in SOHO? [Thrasher]
- It's a print-and-hold thing.
  - So if you don't have print-and-hold, you've mitigated the problem. [Smithson]
  - FAX might be received to memory [Cybuck]
  - Having to authenticate users over the network is different, and how you do one without the other I don't know [Thrasher]
  - Not so difficult: you let everyone print, but if you want to print and hold, you send a PIN and then use it to unlock the job [Smithson]
  - How do you put that in the PP? [Thrasher]
  - I don't know how you include that and not restrict other things [Aubry]
- Can we get rid of O.NETWORK in this profile?
- Work on this and report in the next meeting [Wright]
- It's not the normal SOHO device, it's the secure one [Cybuck]
- Would it work to have nothing more than an IP address range? I don't want user accounts. [Thrasher]
  - That's how I envisioned it, you want to only allow people on your network in. It gets more complex with wireless. We don't need to specify how – it might be that they need to physically acknowledge something on the HCD the first time they print. We're already saying that SOHO security consists mainly of locked doors and people recognizing strangers. [Smithson]
- T.TSF.CONF.AB is included in SOHO but we took it out of Public, that breaks the hierarchy. Should we take it out of SOHO, or should we put it back into Public? [Smithson]
  - Did we really decide that these need to be hierarchical? Is that a rule? [Wright]
  - So far, we've held it as a strong preference. [Smithson]
  - SOHO is likely to have an address book. [Wright]
  - Would you ever want to take a SOHO-class HCD into a Public environment? [Thrasher]
  - Yes, maybe for a small Internet café. [Smithson]
  - Does it really matter? [Wright]
  - When we made them hierarchical and it sometimes required artificiality, we did so by adding requirements and not by taking them away.
  - Putting it back in to Public would be easier to justify [Thrasher]
  - OK [Wright]

## Clause 5 review [Cybuck]

Refer to:

<http://grouper.ieee.org/groups/2600/drafts/Clause5/clause5-15b.pdf>

- noted that not all HVA environments are large enterprises
  - some are islands, some are small standalone businesses
  - need another description and graphic

## Closing [Wright]

See you in DC \* ***Adjourned at 3:30 PM, 01/17/2006*** \*