

IEEE P2600 Meeting #21
July 26-27, 2006
Xerox, Rochester NY

(updated 8/22/06)

Attendees

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

Nancy Chen, Oki Data
Peter Cybuck, Sharp
Satoshi Fujitani, Ricoh
Tom Haapanen, Equitrac
Takanori Masui, Fuji Xerox
Ron Nevo, Sharp
Glen Petrie, Epson
Alan Sukert, Xerox
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 9:15 AM 07/26/2006 ***

Administrivia [Wright]

The following administrative items were reviewed:

Agenda review

Refer to meeting slides for detail
<http://grouper.ieee.org/groups/2600/presentations/P2600-July2006.ppt>

Minutes and Agenda approvals

The June 2006 minutes were approved without changes.
The July 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-July2006.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.

Meeting schedule updates

Sep 6-7, at Equitrac, Waterloo, ON, Canada

There will be a TCG HCWG meeting (for TCG members) on Sep 8, location TBD.

October conference call? We may wish to schedule a conference call after the International Common Criteria Conference (Sep. 19-21) and before the October P2600 meeting in order to discuss announcements about CCv3.

Oct 23-24 with PWG, (and other printer-related groups) at Lexmark, Lexington, KY – ***expect two full days of meetings***

Dec 11-12, at Peerless, El Segundo, CA – ***expect two full days of meetings***

No 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>

Project schedule update [Wright]

- Clauses 1-9
 - merged
 - continue to review; consider a new compliance clause
- PPs

- CCv3.1 announcement is currently scheduled for Sep. 19-21 at ICC. It was previously supposed to have been in July.
 - NIAP CIM for CCv3.1 should be available at or soon after ICC
- 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

2007 Meeting Schedule formulation [Wright]

- January-February
 - Finish draft if it hasn't been completed in December
 - Week of Jan 8 (too close to holidays) or Feb 19 (more likely)
- April
 - Handle comments from sponsor ballot
 - April 16-17, or week 23rd
- May
 - Handle comments from 1st re-circulation
 - Week of May 21st or 28th
- July
 - Handle comments from 2nd re-circulation, if needed
 - Week of July 23rd
 - Cut-off for draft to RevCom is August 17th

TCG update [Thrasher]

- use cases done
- now working on how this applies to implementing HCDs
 - do we need a real TPM?
 - mobileWG (for example) as their own specs
 - behavioral reqts
 - technical reqts
- also considering how to claim compliance [Smithson]

INCITS CS1 update [Thrasher]

- 30-day agenda published

- proposal approved for guidelines (see agenda)
- list of gotta-dos without regard to risk management
- target is an ANSI tech report
- protection profile registration process up for 5-year review
- anything about p2600 in CS1? [Smithson]
 - no
 - I presented p2600 to W1 in May [Wright]
 - WRT p2600, once it is a US national standard we could fast-track it through SC27 (not CS1)

Common Criteria Vendors Forum (CCVF) [Thrasher]

- formed by Wesley Higaki (Symantec) and others
- premise is that CC is not being developed with enough industry input
- wants to stop or influence CCv3
 - mainly part 3
- looking at modifying part 3 to incorporate secure methodologies, based on Microsoft SDL
- counter argument is that it's inherent in SAR part of CC
- CCVF maintains that CC focuses on less important things like paperwork and not on whether a vendor has good secure development methodology
- how long in existence? [Farrell]
 - about six months
- some association with ITAA
- there is no public web site or mailing list access
 - to join, send mail to Wesley Higaki <whigaki@symantec.com> and ask to be added to the CCVF mailing list

Action items from previous meeting [Wright]

Main action items were updated on presentation slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-July2006.ppt>

Action item spreadsheet was reviewed and updated:

- Pre-meeting:
 - <http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20060719.xls>
- Post-meeting:
 - <http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20060801.xls>

Email issues [Wright]

Refer to slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-July2006.ppt>

T.UD.PHY.OUTPUT issues [Smithson]

- Choices are:
 - Do not require any technical solution for T.UD.PHY.OUTPUT
 - Require O.ACCESS for PP-A
 - Require O.ACCESS for both PP-A and PP-B
 - Require O.ACCESS for PP-B, and O.ACCESS and O.I&A for PP-A
- Seiko/Epson: use O.ACCESS for B, O.ACCESS and O.I&A for A [Petrie]
- Ricoh: [Smithson]
 - limited interfaces on some devices makes it difficult to implement O.I&A
 - shouldn't need to require O.ACCESS for walk-up copy jobs
 - would need to provide this functionality for every device in the chosen environment
 - should not do PP-B
 - maybe do PP-A
- threat description would need to be modified [Thrasher]
- can we write the PP to allow O.ACCESS *_instead_* of OE.LOCATION? [Smithson]
- Lexmark: should not disallow products to be certified if they don't have a robust operator panel interface [Thrasher]
- Toshiba: should still have technical solution in environment A [Yami]
- how many people here use O.ACCESS printing at their own office? [Smithson]
 - <<insert the sound of crickets...>>
- resolved
 - O.ACCESS for A, not for others
 - OE.LOCATION, OE.TRAIN for B
 - OE.TRAIN for C
 - No requirement for D

T.DOS.FAX issues [Smithson]

- Proposal is to add T.DOS.FAX into PPs with the same objectives as T.DOS.PRT and T.DOS.NET (i.e. resilience, recovery)
- Resolved: Accepted without objection
- Resolved: Include an application note that recovery may not be fully automatic if such attacks result in exhausted consummables

Subjects, objects, etc [Smithson]

Refer to

<http://grouper.ieee.org/groups/2600/presentations/Rochester/SubjectsObjectsAndBeyond.pdf>

- Subjects/objects/etc may be thrown out of CCv3 part 2, but they are part of the overall model and were in CCv2.3

- Purpose of this work was to clarify my own effort to work on CCv3 SFRs
- Idea was to define the entities, test them in some use cases, and then write some SFRs using them
 - Entities were defined
 - Some use cases were written
 - SFRs are the next step
- I am presenting this now to get feedback on the approach and on any specifics
- (feedback was positive – awaiting a presentation with SFRs at next meeting)
- Each company should bounce this proposal off of their implementation teams [Wright]

Availability as an asset [Chen]

- Availability is not a traditional asset in the risk analysis sense
- availability is a special term in the security field and it may be confused with the term as used in confidentiality/integrity/availability
- (discussion)
- Resolved to leave it as an asset
 - call it HCD Availability in the clauses
 - call it TOE Availability in the PPs

Software vs Firmware vs Applet assets [Chen]

- Clauses refer to Software which includes both firmware and applets
- PPs have only Firmware in the asset table (but Applets are used elsewhere)
- Resolution:
 - add Applet to PP asset table
 - add “Firmware” and “Applet” subsections under Software in the P2600 clause

External Environment as an asset in PPs [Chen]

- it's not in table 1
- by “assets”, we refer to TOE assets; is it OK to include EA even if it's not inside the TOE? [Smithson]
- there are threats against the EA [Thrasher]
- should be included also in figure 1 [Smithson]
- Resolved
 - add EA to table 1
 - add EA cloud to figure 1

T.UD.ACC.NORMAL definition [Chen]

- There was much discussion, resolving in a new full description (in the clauses) and adding RIP to acronyms

PP-A review [Smithson]

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-a-21a.pdf>

- Accepted all changes to this rev level
- Some changes were made in place during review
 - Many of these will need to be reflected in other PPs
- Regarding David Freas' emails of 7/16/06:
 - Adding FIA_QAD to PP-A and PP-B, proposed:
 - Add one-factor authentication (password), at least 4 numeric characters for PP-B and at least 8 alphanumerics for PP-A
 - Two- and three-factor auth quality are not specified
 - FPT_RIP.1 vs FPT_RIP.2
 - On hold awaiting CCv3.1

Refer to updated file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-a-21b.doc>

PP-B review [Nevo]

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-b-21a.pdf>

- Accepted all changes to this rev level

PP-C review [Chen/Sukert]

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-c-21a.pdf>

- Accepted all changes to this rev level

PP Appendix A, B, C review [Smithson]

Refer to original files:

http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp_Appendix_A_References-21a.pdf

http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp_Appendix_B_Glossary-21a.pdf

http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp_Appendix_C_Acronyms-21a.pdf

- Accepted all changes to this rev level
- The only requested change was to add (duplicate) PP definitions for Assets, etc. into Appendix A Glossary so that there is one place to look for definitions.

Power-on/power-off nonvolatile storage proposals [Smithson]

Refer to proposal:

<http://grouper.ieee.org/groups/2600/presentations/Rochester/Proposal2%20to%20P2600.pdf>

- This is a refinement of a proposal made at the previous meeting (Camas, June 2006)
- Proposal 1, *accepted*
 - Rename T.TSF.CRED.DISK as T.TSF.SALVAGE and expand its scope to include both Management Data and User Function Data. The new name takes it out of the T.TSF.CRED family and helps make it clearer that we mitigate this threat using the same approaches that we use for T.UD.SALVAGE. The expanded scope gives coverage to User Function Data and the rest of the Management Data types.
 - Change the objective of O.PROTECT to prevent unauthorized access to data on non-volatile storage devices when disconnected from the TOE.
 - Remove O.PROTECT from the list of objectives for all threats except T.UD.SALVAGE and T.TSF.SALVAGE.
 - O.MONITOR could be used to detect an unauthorized or unscheduled powerdown [Chen]
 - Apply O.DELETE to T.UD.SALVAGE and T.TSF.SALVAGE.
 - Rely on O.I&A and O.ACCESS to mitigate T.UD.ACC.*, T.TSF.AUD.*, and T.TSF.CONF.*.
 - In PP-A, require O.DELETE and O.PROTECT for both UD and TSF data.
 - In PP-B, require O.DELETE and O.PROTECT for TSF data, but only require O.DELETE for UD data.
- Proposal 2, *rejected*:
 - Distinguish between removable nonvolatile storage (like disk drives) and nonremovable nonvolatile storage (like NVRAM soldered into the controller)
 - Prohibit persistent document storage in PP-A
 - This would be more of a site policy matter, some PP-A environments allow document storage [Cybuck]
- Proposal 3, *accepted*:
 - Remove T.UD.SNIFF.NET from PP-B. This would mean that you don't need to encrypt document data over the network in B environments. You would still need to encrypt TSF data.
- Proposal 4, *accepted*:
 - Remove T.TSF.AUD.ACCESS from PP-B (leaving T.TSF.AUD.ALTER). This is more consistent with the definitions of PP-A and PP-B and may make it easier to implement PP-B devices.

Clause 8 review [Thrasher]

Refer to original file:

http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v20a_ncb.pdf

- Accepted all changes to this rev level
- (We also looked at which “recommended” mitigation approaches that we might want to require which are not already required by one or more Protection Profiles. We did have time to complete this review of Clause 8, but did not find any recommendations that we thought should become compliance requirements outside of the PPs.)

Closing [Wright]

See you in Waterloo, ON, Canada

**** Adjourned at 1:20 PM, 07/27/2006 ****