

IEEE P2600 Meeting #22
September 6-7, 2006
Equitrac, Waterloo, ON, CA

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
Satoshi Fujitani, Ricoh
Tom Haapanen, Equitrac
Harry Lewis, IBM
Ron Nevo, Sharp
Ken Ota, KonicaMinolta
Alan Sukert, Xerox
Brian Volkoff, HP
Bill Wagner, KonicaMinolta

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 09/05/2006 ***

Administrivia [Wright]

The following administrative items were reviewed:

Agenda review

Refer to meeting slides for detail
<http://grouper.ieee.org/groups/2600/presentations/P2600-Sept2006.ppt>

Minutes and Agenda approvals

The July 2006 minutes, as updated on 8/31/06, were approved without
additional changes.

The September 2006 agenda was approved with a few additions.

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-Sept2006.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

October conference call? We may 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. It will be primarily for PP authors, but the call will be announced on the mailing list and all will be welcome to join.

Oct 23-24 with PWG, FSG, OSDL, at Lexmark, Lexington, KY – ***expect two full days of meetings***. There will be a TCG HCWG meeting on October 25. For reference, FSG will meet October 23-25, and PWG will meet October 26-27.

Dec 11-12, at Peerless, El Segundo, CA – ***expect two full days of meetings***. There will be a TCG meeting on Dec. 13 at a nearby HP facility.

Feb 21-22, 2007 with PWG, on Maui or other Hawaiian island. TCG HCWG meeting is also likely.

- Finish draft if it hasn't been completed in December

Apr 24-25, location open (looking for East Coast, USA)

- Handle comments from sponsor ballot

May 30-31, location open

- Handle comments from 1st re-circulation

Jul 11-12, location open

- Handle comments from 2nd re-circulation, if needed
- Cut-off for draft to RevCom is August 17th

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>

TCG update [Volkoff]

- KonicaMinolta joining the HCWG this month
 - has not yet elevated membership
- looking for additional members
- looking at whether to require TPM or allow other methods

INCITS CS1 update [Thrasher]

- 1831 project "minimum security guidelines for ..."
 - first draft reviewed
 - generally looks like a mirror of the VISA PCI
 - concern about copyright issues about that
 - concern that PCI is somewhat dated
- a bunch of new projects in the works, ISO frameworks and such

Action items from previous meeting [Wright]

Main action items were updated on presentation slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Sept2006.ppt>

One item generated some additional discussion:

- ideas for benefits of funding evals
 - (see slides for some ideas already considered)
- other ideas?
 - contributors get a vote on choosing the lab [Thrasher]
 - contributors get a vote on choosing which PPs and which order [Smithson]
- need to look at what kind of acknowledgement can be put on an IEEE std
- copyright license means what? [Farrell]
 - would allow you to use portions of the std without paying a fee
 - need to look into what that means for published PPs
- schedule? [Wagner]
 - need to get this settled out by first of the year

Action item spreadsheet was reviewed and updated:

- Pre-meeting:
 - <http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20060831.xls>

- Post-meeting:
<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20060913.xls>

CCVF update [Thrasher]

- CCVF wants to add a new assurance class for secure methodologies into CC.
- CCVF plans to meet t ICC'06 and has also scheduled a meeting between CCVF and the CC Development Board at ICC
 - Thrasher and Smithson plan to attend the meetings at ICC

JBMIA activities [Smithson]

- Japanese Business Machine Industry Association has become interested in P2600, and in particular, PP-B.
 - They represent all of the Japanese vendors of MFPs
 - Just began talking about it. Initial companies in this activity are Canon, Fuji-Xerox, Ricoh, and Sharp.
 - They were considering writing a new PP-B, which I have discouraged in favor of providing individual individual comments.
 - Their first meeting as a working group will be in late September or early October, which is good because we should have resolved some of the CCv3.1 issues with the PPs.
- It would be good if someone from JBMIA can attend a P2600 meeting to present their input. [Wright]
 - Ricoh was suggesting that we have liaisons from both groups attending some of each other's meetings.
- It would also be good to find out what the JBMIA issues are before the JBMIA invests its time and effort in a formal proposal. We may be able to address JBMIA concerns directly or through liaison persons. [Farrell]
- They will need to move quickly because we are trying to wrap this up around the end of the year / January at the latest. [Wright]
- Any idea of what they are concerned about? [Farrell]
 - Practical implementation issues. It is good to get feedback from implementors, but I wish we also had more feedback from customers as well.
- It is possible that Don Wright could meet with JBMIA on November 27 (he will be in Tokyo that day, and available for a meeting). Perhaps we (with Smithson) could arrange to meet with JBMIA. [Wright]
- This may be an opportunity for us to find a way to leverage their support of P2600.

- We have talked about the benefits of individual companies contributing to PP evaluation funding. What would happen if JBMIA provided funding? Would the benefits flow down to their members? [Wagner]
 - Not clear, we haven't really thought about that. [Wright]

Korean CC Scheme [Wright]

- There was a proposal that for any evaluated product, not just EAL 4+, that Korea would require source code to be supplied.
- This was not well received by many companies, and was worked on by the ITI Standardization Policy Committee.
- (Don) received an email from Helen Lee Wong, Counselor for Consumer Affairs, American Embassy in Seoul, that said their new proposed policy:
 - Applies to all EAL 1-4 products purchased by Korean government agencies (including education and health care)
 - Requires three documents: a CC certificate, ST documentation, and the evaluation report translated into Korean language.
- It seems like a country manager could arrange to get reports translated. [Smithson]
- This was put on the table of a free trade agreement, so it was raised to a very high level.

Commenting Tool [Wright]

- It's a filemaker application
- It generates tilde-separated file (so don't use tildes in your comment data)
- It creates a single CSV file to e-mail to Don
- Don has a tool to aggregate comments into a single file
- There is a comment resolution tool that can be used during meetings
- There is also a comment report generator that can be used to report results

Command injection issue [Sukert]

- (background was given about the Xerox vulnerability disclosure at 2006 Black Hat Briefings)
- this kind of attack not adequately covered by ccv3.1 SFRs or current threats
 - could be covered under t.tsf.sw.applet
 - doesn't quite fit the definition, but could be modified
- at first I thought it could deserve its own new threat, something between t.tsf.sw and t.ud.acc.hack [Smithson]

- Ohta-san (of Ricoh Japan) pointed out that it's an implementation issue and should be covered under SARs, not SFRs [Smithson]
- Did the Xerox product pass CC certification? [Volkoff]
 - Yes this one was
- This should be covered under SARs and depends on the EAL level [Aubry]
- Security architecture SARs should have picked up the authentication bypass problem [Smithson]
- at what level do we require that? [Chen]
 - it is automatic based on the EAL [Aubry]
- agreed, this is a design or coding problem, but a lot of the threats that we have are also design or coding problems
 - I disagree, I don't think the bulk of our threats are design or coding problems, they protect against unintended uses like sniffing or overloading with packets, or other cases like salvaging data in which a product may be perfectly well designed and implemented but not to delete data and therefore salvaging can occur [Smithson]
- At HP we have a design objective to protect against command injection [Volkoff]
- would this difficulty be caught by evaluators? [Wagner]
 - depends on the EAL [Aubry]
 - when you certify, you certify functionality and then the CC process assures implementation [Volkoff]
 - do we have confidence that this kind of thing would be caught? Otherwise it would reflect poorly on the standard if a product was certified but had a problem like this [Wagner]
 - CC eval at increasing levels increases assurance of implementation, but not perfect security or no vulnerabilities [Aubry]
- What could you do to prevent this kind of thing? [Wright]
 - Should be caught by vulnerability testing [Aubry]
 - Cross-site scripting is part of a standard test [Del Re]
 - what O'Connor was doing was a vulnerability assessment on this MFP [Smithson]
- this should have been in the design constraints [Del Re]
 - should have been in the design and the test was also flawed [Wright]
- some of these things were pretty obvious [Wright]
 - at least, what led to the bypass should have been obvious [Smithson]
- this is a reminder that we should do good design practice
 - good design, or good practice? Design is SFRs, practice is SARs. They had authentication, and they had functions for controlling network traffic, both are good design. But they

- had bad design practice, the authentication could be bypassed and the functions could be subverted [Smithson]
- Looking at the description of what happened, this is like EA.PROXY, using the web form service to open up the telnet server [Thrasher]
 - But how do you find such things in the real world? [Aubry]
 - It can require exhaustive testing [Thrasher]
 - I think this was an indirect way to get to EA.PROXY [Smithson]
 - If you agree with EA.PROXY, then in PP-C we need to make sure that this threat is included
 - I don't think PROXY is the one. That's intended to handle open relays or ftp bounce attacks, not to handle injecting commands that overwrite a password file and an inetd file which then allows you to connect to telnet with the password of your choice. I don't know how the threat description would inform you to design against command injection [Smithson]
- Resolved: Sukert to propose threat/SFR language [Wright]

PP-A vs PP-B threats [Aubry]

- T.TSF.AUD.ACCESS / ALTER
 - As written, it doesn't make sense
 - agreed to leave T.TSF.AUD.ACCESS in PP-B
- T.UD.SNIFF.NET
 - There were no objections to removing this from PP-B
 - Resolved: remove T.TUD.SNIFF.NET from PP-B [Wright]

Top-down SFR generation [Smithson]

Refer to these files::

<http://grouper.ieee.org/groups/2600/presentations/SFRworksheet22a.xls>

<http://grouper.ieee.org/groups/2600/presentations/SFRSamples22a.doc>

- Purpose was to
 - understand why/how each SFR/SAR related to threats
 - ensure that NIAP CIM was included
 - ensure that we are applying these requirements consistently
 - be able to more easily manage changes from ccv3.1 draft to ccv3.1 final and CIM v3 (based on ccv2.3) and whatever new CIM comes from NIAP for ccv3.1
 - possibly generate SFR/SARs for all four environments from one data source
- it is a trial run based on the subject/object/etc work that was started two meetings ago
- Looking at SFRworksheet:
 - Threats/objectives table is taken from PP-A
 - List of SFRs is all possible ccv3.1 SFRs

- SFRs are selected for each objective based on the most recent ccv2.3-based PP (which was PP-H-11b)
 - For each SFR, see if there are any entities (subjects, objects, users, etc) that should be specified
 - If not, use the SFR unchanged
 - If yes, insert the entities that may be appropriate
 - In the worksheet, O.I&A and O.ACCESS were completed
- Looking at SFRsamples:
 - These are the SFRs either written out unchanged or written with entities specified
 - In some cases it was better to refer to a table than to put the entities in-line in the SFR assertion
- This level of detail seems appropriate for the ST, but not for the PP [Wright]
 - I was concerned about that, but if we leave it open, then the PP is meaningless, you could allow read-write to everything for everybody and still comply with the PP
 - Wouldn't the evaluator see that? [Wright]
- You force all of the STs to have all of those roles [Aubry]
 - They must define them in order to fulfill the various requirements
 - What if the ST does not have those roles? [Aubry]
 - They wouldn't comply with the PP.
- Doing this trial run, we can see how the SFRs come out and if they are too specific, we can easily adjust them back to be more general. The tradeoff is between being too restrictive to ST writers versus relying too heavily on evaluators.
- A compromise may be to leave the SFR text fairly general but then put a statement in a PP application note that gives the intention and an example, and then the evaluator could look at that in the ST and see if the ST fulfills the intention of the SFR
- It would be good to get some advice from a lab on this, but we don't have one under contract
- To the extent that I looked at each of these SFRs it took only a few hours to complete the first two columns, so it seems like an efficient way to work
- I like the PP application note idea [Wright]
 - We could have a consistent model that we use as an example in those app notes, but the ST author would not need to use the same attribute names or even the same organization of attributes
- Write access for an auditor is not usual, it should be a security administrator who writes and the auditor who reads [Aubry]
 - It is easier to see such errors by generating SFRs in this way
- I had some problem understanding the SFPs that are shown in square brackets in the SFR text. They could refer to P.policy

statements where specific policies (like MAC or DAC) must be followed, or they could refer to a collection of SFRs that form a policy. The latter makes the SFRs self-referential and we could make a mess of them if we write SFRs in fully formed text without some kind of rigorous approach.

Sample SFRs for PP-C and CCv3.1 [Sukert]

Refer to this file:

<http://grouper.ieee.org/groups/2600/presentations/Sample%20SFRs%20for%20PP-C%20for%20CCv3.1%20v2a.doc>

- first attempt at applying CCv3.1 to PP-C
 - mapped SFRs between 2.3 and 3.0 to 3.1
 - take draft 3.0 version of PP-C and use map to create a 3.1 version
- first part of document is PP-C as currently defined (22a1)
- second part of document is translated using map
 - didn't opt to go back to a 2.3-based PP-C because that might introduce old problems
- (walkthrough of document)
- These don't always line up, and they are in alphabetical order and so some of the relationships are disjoint in the document
- Does this work effect the main document, or just the PPs?
[Wagner]
 - I think just the PPs

Comment on clauses 1-9 [Wright]

Refer to comment tool output:

<http://grouper.ieee.org/groups/2600/comment-tracking/sept2006-disposition.pdf>

PP-A review [Smithson]

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-a-22a.pdf>

- Accepted all changes to this rev level
- Some changes were made in place during review
 - Temporary Data definition
 - need to update PP-B,C,D
 - Stored Data definition
 - need to update PP-B,C,D
 - Management Data definition
 - need to update PP-B,C,D
 - O.NETWORK change
 - need to update PP-D
 - turn on line numbers, whole document!

- need to update PP-B,C,D
- change table 11 to 10pt typeface
 - need to update PP-B,C,D
- "section 0" in 4.4, change to section 1.2.1
 - need to update PP-C,D

Refer to updated file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-a-22b.doc>

PP-B review [Nevo]

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-b-22a.pdf>

- Accepted all changes to this rev level
- Some changes were made in place during review
 - reference to NIST EAL should be Common Criteria EAL
 - check PP-C
 - "section 0" in 4.4, change to section 4
 - check PP-C,d
 - check for headers/footers throughout
 - section breaks

Refer to updated file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-b-22b.pdf>

PP-C review [Chen/Sukert]

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-c-22a.pdf>

- Accepted all changes to this rev level
- Some changes were made in place during review

Refer to updated file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-c-22b.pdf>

PP-D review [Aubry]

Refer to original file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-d-22a.pdf>

- Accepted all changes to this rev level
- Some changes were made in place during review
 - some assumptions need review/rewording/deletion?
 - like A.ADMIN, A.USER
 - add objectives and rationale back in (with a PP app note)

Refer to updated file:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/pp-d-22b.pdf>

Production Printing issue [Lewis]

- Would it be appropriate for me to write some modifications to PP-B or a new profile for production printing?

- Nothing in the description of operational environment B would indicate production printing [Wright]
- We talked about it being somewhere between C and D [Aubry]
- I think it's OK to say that it's a lightweight PP because security is provided in a physical way for production shops.
 - Is that really true? It seems like if you're printing credit reports or bank statements, the stream of data going to the printer could be quite valuable [Smithson]
- Isn't it more an issue of what you're printing than that it is a production environment? [Wagner]
 - It's a controlled environment, not like an MFP that you can walk up to in an open environment.
 - Maybe if they're printing bank statements, then it's an OpEnv in an A environment, or if they're printing menus for the local take-out then it's a C or D environment. [Smithson]
- Seems like a production environment is a B environment [Wright]
- Why then is it that no production printing systems are CC certified? [Aubry]
 - Perhaps same reason that SCADA systems are not secured. It's a big hole. [Smithson]
 - For years, production printing systems were connected in non-network environments [Wright]
 - Some requirements like data overwrite would significantly slow down production [Aubry]
 - There are other controls that handle things like rolls of paper that print negotiable financial instruments.
 - We haven't indicated timing on overwrite, it could be an end-of-day thing [Thrasher]
 - It could be specified in the ST [Smithson]
- Do any customers ask for CC certification? [Smithson]
 - Not to any large degree. That's why I think PP-D would make sense.
 - DAPS does production printing. Maybe they're just considering the fleets of MFPs that they support and not their internal production machines. [Smithson]
- We can't go back at this time and create a new environment. [Wright]
- Perhaps it could be a custom PP that a company develops and evaluates, based on one of the P2600 PPs. A benefit for funding the PP evaluations and getting that copyright release. [Smithson]

Which PPs to evaluate, and when? [Wright]

- What is the benefit of evaluated PPs? [Volkoff]
 - ST eval would only require that the ST follows the PP, product matches the ST, and assurance reqts are met
- what if you want to eval a PP for your own use? [Volkoff]
 - I would think that we could allow a single company to fund the eval of a PP that as a group we decided not to eval [Smithson]

- it would be more expensive to eval a PP and an ST, but perhaps would be less expensive to eval a PP for multiple STs
- PP-A and PP-B most likely to be evaluated
- PP-C under consideration
- PP-D LAL least likely
 - why? [Wagner]
 - presumed lack of market demand
- we should get Freas comments on likelihood/value of getting PP-A and/or B adopted in some form as a US govt PP

Compliance clause [Wright]

- Came up two meetings ago.
- The issue was that clauses 1-9 are full of “shoulds” and makes it look like a recommended practice and not a standard [Smithson]
 - We started going through clause 8 to see if there was anything that could be turned into a “shall”, and although we didn’t completely go through clause 8, we came up with none [Smithson]
 - A problem with this approach is that when we have recommendations for manufacturers, do we list all possible mitigation techniques? Would we require that they follow all of them, or one or more of them, or some selection of them? It becomes more complex also if you consider different requirements for different operational environments. [Smithson]
- If we stepped up a level, for example, saying that devices using wireless communication shall use 802.11i. Would that be appropriate?
 - Only for those that use 802.11 [Thrasher]
 - Specifying that would date the standard. Things change. Also, it would be difficult to find references for mitigating all of the threats. [Wagner]
 - This wouldn’t be attached to threats; it would be something that devices should do independent of specific threats. Another example, “device configuration using the operator panel shall require a password”.
- I think it’s the right idea, but is it something we can do in the timeframe of completing P2600? [Sukert]
 - If we can get someone to draft it.
 - I think we should have any compliance requirements stated early in the document, and should start with compliance with one or more of the PPs. If we have more requirements, we could state them there.
- The way clause 8 is written, it is mitigation threat-by-threat. This is a problem because not all threats apply to all environments [Threat]
 - We could have four compliance sections, one for each environment, starting with compliance with that environment’s PP.
- These requirements would need to be aligned with the PPs [Nevo]
 - We certainly wouldn’t want them to be contradictory

- I think we should only have requirements outside of the PP that cannot be addressed by a PP, such as if they are beyond the TOEs ability to detect or control. [Smithson]
- That would be part of the IT environment, beyond the manufacturer's ability to control. But we have recommendations for IT professionals.
- But there isn't such a thing as P2600 compliance for an IT environment. We decided that previously. IT environments comply with other standards, like ISMS.
- I will make a draft compliance clause for next meeting [Nevo]

Next meeting [Wright]

- October 23-24 in Lexington at Lexmark, so we have a long break except for those who are attending ICCO.
- Racing season is open, and there are other meetings going on, so make your reservations early.
- (much discussion about Marriott properties and Starbucks)
- Expect two full days to meet in Lexington, and also two full days at the following meeting in El Segundo.

Closing [Wright]

See you in Lexington

** Adjourned at 12:15 PM, 09/7/2006 **