

# IEEE P2600 Meeting #37

## August 11-12, 2008

### Sharp Labs, Camas WA

#### Attendees

Chair: Don Wright, Lexmark  
 Vice Chair: Lee Farrell, Canon  
 Secretary / Lead Editor (2600.n): Brian Smithson, Ricoh

Carmen Aubry, Océ  
 Nancy Chen, Oki Data  
 Peter Cybuck, Sharp  
 Nick Del Re, Canon  
 Helmut Kurth, atsec (by phone)  
 Harry Lewis, InfoPrint  
 Ron Nevo, Sharp  
 Glen Petrie, Epson  
 Hyun Woong Shin, Samsung  
 Alan Sukert, Xerox  
 Jerry Thrasher, Lexmark  
 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 comments may appear in these minutes, indicated by {braces}, inserted by the Secretary for clarity.

Attendees.....	1
Administrivia [Wright] .....	2
Review and Approve June Minutes [Wright] .....	2
Review IEEE Patent Policy [Wright].....	3
Call for Potentially Essential Patents [Wright] .....	3
IEEE Meeting Guidelines [Wright].....	4
2008 Meeting Schedule [Wright].....	4
Update on Trusted Computing Group (TCG) Hardcopy Working Group (HCWG) [Volkoff].....	4
Update on INCITS CS1 Working Group [Thrasher] .....	4
Update of CC Vendor's Forum [Sukert].....	5
Review of Action Items from Previous Meeting [Wright] .....	5
PP Evaluation ad hoc Committee Status [Nevo].....	5
Guide to P2600 PPs <i>ad hoc</i> Status [Sukert] .....	6
Production Printing Protection Profile [Lewis] .....	7

Protection Profiles Review – Comment Resolution [Wright] .....	7
Protection Profiles Review – Comment Resolution continued [Smithson] .....	7
Schedule review [Smithson].....	12
Next meeting details [Wright] .....	13
Closing [Wright].....	13

**\* Called to order at around 9:00 AM PDT 8/11/2008 \***

***{Many thanks to Lee Farrell who captured the minutes during the first half of day one}***

## **Administrivia [Wright]**

Don Wright led the meeting and provided the planned agenda topics:

- Welcome & Introductions
- Update and Approve Agenda
- Review and approve June Minutes
- IEEE Patent Policy Review
- 2008 Meeting Schedule
- Update on TCG (Volkoff)
- Update on INCITS CS1 Working Group (Thrasher)
- Update of CC Vendor's Forum (Sukert)
- Review of Action Items from June Meeting
- PP Evaluation ad hoc status (Nevo)
- Protection Profiles Review and Comments
  - \* PP-A (36c proto)
  - \* PP-B (36c proto)
  - \* PP-C (36c proto)
  - \* PP-D (36c proto)
  - \* Comments
- Issues raised on e-mail
  - \* Function Access Control Policy
- Guide to P2600 PPs ad hoc status (Sukert)
  - \* PP Guide Outline
- Production Printing Profile (Sukert)
  - \* Draft (36c proto)
- Schedule Review
- Other items
- Posting and Comment deadlines for the September Meeting
- Next meeting details

## **Review and Approve June Minutes [Wright]**

There were no objections to the Minutes.

## Review IEEE Patent Policy [Wright]

Don presented the “Participants, Patents, and Duty to Inform” slide:

- All participants in this meeting have certain obligations under the IEEE-SA Patent Policy. Participants:
  - \* “Shall inform the IEEE (or cause the IEEE to be informed)” of the identity of each “holder of any potential Essential Patent Claims of which they are personally aware” if the claims are owned or controlled by the participant or the entity the participant is from, employed by, or otherwise represents
    - “Personal awareness” means that the participant “is personally aware that the holder may have a potential Essential Patent Claim,” even if the participant is not personally aware of the specific patents or patent claims
  - \* “Should inform the IEEE (or cause the IEEE to be informed)” of the identity of “any other holders of such potential Essential Patent Claims” (that is, third parties that are not affiliated with the participant, with the participant’s employer, or with anyone else that the participant is from or otherwise represents)
  - \* The above does not apply if the patent claim is already the subject of an Accepted Letter of Assurance that applies to the proposed standard(s) under consideration by this group  
(Quoted text excerpted from IEEE-SA Standards Board Bylaws subclause 6.2)
- Early identification of holders of potential Essential Patent Claims is strongly encouraged
- No duty to perform a patent search

He provided a few IEEE Patent Policy related links, saying that all participants should be familiar with their obligations under the IEEE-SA Policies & Procedures for standards development:

- Patent Policy is stated in these sources:
  - \* IEEE-SA Standards Boards Bylaws  
<http://standards.ieee.org/guides/bylaws/sect6-7.html#6>
  - \* IEEE-SA Standards Board Operations Manual  
<http://standards.ieee.org/guides/opman/sect6.html#6.3>
  - \* Material about the patent policy is available at  
<http://standards.ieee.org/board/pat/pat-material.html>

## Call for Potentially Essential Patents [Wright]

Don provided an opportunity for WG members to identify or disclose patents that any WG member believes may be essential for the use of the P2600 standard. No one responded.

## IEEE Meeting Guidelines [Wright]

The list of Other Guidelines for IEEE WG Meetings was presented and reviewed with the group:

- All IEEE-SA standards meetings shall be conducted in compliance with all applicable laws, including antitrust and competition laws
- Don't discuss the interpretation, validity, or essentiality of patents/patent claims
- Don't discuss specific license rates, terms, or conditions
  - \* Relative costs, including licensing costs of essential patent claims, of different technical approaches may be discussed in standards development meetings
    - Technical considerations remain primary focus
- Don't discuss or engage in the fixing of product prices, allocation of customers, or division of sales markets
- Don't discuss the status or substance of ongoing or threatened litigation
- Don't be silent if inappropriate topics are discussed ... do formally object

## 2008 Meeting Schedule [Wright]

Don listed the remaining dates for P2600 meetings this year:

- Sep 9-10                      Arlington, VA [Sharp]
- Oct 24                         Lexington, KY [Lexmark]
- Dec 11-12                    Plantation, Florida [Equitrac]

Don explained that the August, September, and October meetings are definite. The December meeting is planned as a contingency.

## Update on Trusted Computing Group (TCG) Hardcopy Working Group (HCWG) [Volkoff]

Brian Volkoff said that there was no July/August meeting held. There is still no TCG HCWG activity to report.

## Update on INCITS CS1 Working Group [Thrasher]

Jerry Thrasher referenced some of the CS1 topics that might be of interest to P2600:

- CS1 Project – Small Organization Baseline Information Security Handbook (approved in CS1 and forwarded to INCITS EB)
  - ➔ this is an alternative approach to the previous PCI-related activity that was stalled because of copyright issues.
- Presentation of the NIST proposal for a new project in CS1 – The Policy Machine (no definitive decision, created ad-hoc to further discuss)
  - ➔ a policy that prevents copying and possibly printing of document data. Expected to be a significant effort, possibly resulting in multiple standards.

- ISO/IEC 3rd FCD 15408-1 – Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model (approved without comment)

...and some of the CS1 topics at the September meeting that might be of interest to P2600:

- ISO/IEC 1st CD 27033-1, Information technology – Security techniques – Network security – Part 1: Guidelines for network security
- ISO/IEC 3rd WD 27033-2 (18028-2) – Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security
- ISO/IEC 2nd WD 27033-3 – Information technology – Security techniques - Network security Part 3: Reference network scenarios Risks, design techniques and control issues

## **Update of CC Vendor's Forum [Sukert]**

Alan Sukert reported that the e-mail discussions have been limited to logistical items relating to the upcoming ICCC conference. He said there was nothing of interest.

The US Army has updated their Letter to Industry regarding their latest policy. It is unclear whether it applies to printers or not.

## **Review of Action Items from Previous Meeting [Wright]**

Don Wright led a review of the 2008-08-10 Action Item spreadsheet, which was updated in the meeting to reflect the latest status.

Item 246 was the only Action Item that remains [partially] open: “Find out what copyright license terms could be offered on an IEEE std and what that means for a published Protection Profile.”

Item 246 remains partially open.

## **PP Evaluation ad hoc Committee Status [Nevo]**

{refer to <http://grouper.ieee.org/groups/2600/presentations/Camas2008/IEEE-PP-Validation-8-2008.ppt>}

Ron provided the latest information on the progress with the IEEE. He explained that the IEEE has provided a license agreement for the 14 sponsors that have contributed to the payment for the evaluation fees:

- |                   |            |
|-------------------|------------|
| • Canon           | • Océ      |
| • Fuji-Xerox      | • Oki Data |
| • Hewlett Packard | • Ricoh    |
| • InfoPrint       | • Samsung  |

- Konica Minolta
- Sharp
- Kyocera
- Toshiba
- Lexmark
- Xerox

According to Ron, the IEEE has sent out (or will send out) the license agreement for 10 copies of the P2600 standard documents.

The list of completed activities for PP evaluation includes the following:

- IEEE provided Contract – 4/1/08
- Start formal evaluation (with family of PPs) – 4/14/2008
- P2600 Backgrounder – finished 4/20/08
- IEEE Press Release: selecting atsec – 4/29/2008
- New style of PP (SFR packages/options) (based on atsec review) – 5/2008
- PPs are ready for the vote process – 8/2008

Ron identified several items that still need to be addressed:

- Do we need to buy the PP rights from IEEE?
- Are we submitting a Production PP?
- Complete PP (“packages” approach) documents (almost complete)
- Incorporate latest comments and resolutions
- Officially submit the revised PP to atsec – 8/2008
- Atsec will Submit:
  - \* PP-A to NIAP – US Scheme – 9/2008
  - \* PP-A,B,C,D to BSI – German Scheme – 9/2008 (tentative)
- Approved PP version for IEEE (approved by RevCom) – 12/2008
- IEEE Press Release of PPs – 3/2009?

## **Guide to P2600 PPs *ad hoc* Status [Sukert]**

Alan Sukert reported that PP Guide Version 37a has been posted. It contains an expanded outline for all sections plus the first draft of sections 1-3. Atsec has commented that they believe the Guide content outline looks good, and seems to address the appropriate sections.

The remaining plan is as follows:

- Post PP Guide Version 38a for Sep 08 P2600 Meeting by Aug 26th
  - \* Will incorporate Chapter 5.2.1 plus as many additional sections as are available
- Have initial text for all sections for posting and review at Oct P2600 Meeting available by Oct 10th
  - \* Will try to have as much as we can by then
- Approve initial PP Guide at Dec P2600 Meeting

Carmen suggested that it would be good to get confirmation from atsec that what we write is accurate and consistent.

## Production Printing Protection Profile [Lewis]

Harry Lewis reported that the latest draft of the Production Printing Protection Profile is 36c proto.

He said that the AFP consortium is meeting on October 6-8. It already has a full agenda. He had hoped to coordinate a group to meet on the morning of Oct 9 to discuss PP-E. However, Alan Sukert noted that Oct 9 is Yom Kippur—and he cannot attend.

Harry said that he will re-consider the agenda, possibly coordinating an hour or so into the existing activities.

## Protection Profiles Review – Comment Resolution [Wright]

Don Wright led the review of comments submitted on the Protection Profile documents. There were many comments requiring changes for consistency of text, clarification, or correcting cut/paste errors—and did not cause notable discussion and were accepted for modification as proposed. These and the withdrawn or rejected comments are not included in the list below.

All Suggested Remedies were recorded by Don for subsequent publication.

*{... end of Farrell's minutes, beginning of Smithson's minutes ...}*

## Protection Profiles Review – Comment Resolution continued [Smithson]

Refer to comments with resolutions:

[http://grouper.ieee.org/groups/2600/comment-tracking/P2600A\\_2008\\_08\\_v05.pdf](http://grouper.ieee.org/groups/2600/comment-tracking/P2600A_2008_08_v05.pdf)

[http://grouper.ieee.org/groups/2600/comment-tracking/P2600B\\_2008\\_08\\_v03.pdf](http://grouper.ieee.org/groups/2600/comment-tracking/P2600B_2008_08_v03.pdf)

[http://grouper.ieee.org/groups/2600/comment-tracking/P2600C\\_2008\\_08\\_v03.pdf](http://grouper.ieee.org/groups/2600/comment-tracking/P2600C_2008_08_v03.pdf)

[http://grouper.ieee.org/groups/2600/comment-tracking/P2600D\\_2008\\_08\\_v03.pdf](http://grouper.ieee.org/groups/2600/comment-tracking/P2600D_2008_08_v03.pdf)

And to the PPs:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.1-37a.pdf>

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.2-37a.pdf>

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.3-37a.pdf>

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.4-37a.pdf>

- {most comments were not controversial, see the resolution documents for details; for others, see below}
- {refer to comment #51} There is some concern that IPA will interpret access control rules that allow, for example, an administrator to read documents to mean that the TOE must provide that functionality.
  - That is true, if the ACR expresses permission then the function must exist [Kurth]

- It was proposed that we rewrite most or all of the ACRs in terms of what is denied, rather than what is allowed. Would that solve the problem?
- It better expresses what you really want. You also want some flexibility for the ST author to add an allowance if their product supports such a function. [Kurth]
- How do we ensure that the ST author cannot allow access that we do not want to allow?
- An app note saying that the ST author can allow certain kinds of access like a user can modify their own documents but not another's. If a product allows something which contradicts that, it would require an explicit action by the owner or an administrator.[Kurth]
- If we have an ACR that allows a user to read their own document, and an ST author wants to also allow an administrator to read documents, is that not more restrictive? [Aubry]
- We currently have a policy of allowed actions. You can add further rules that do not contradict the default rules. If we use a deny approach and say that a normal user is not allowed to access documents that are not owned by them, the ST author could add that an administrator can also access documents and that would not contradict the default ACR. [Kurth]
- I will prototype the rules and we can discuss with the PP editors in email.
- {refer to comment #40} We have gone back and forth between FPT\_TST and FPT\_TEE to require at least simple power-on integrity self-tests of HCD operating software. Since such a test would likely be performed by the target of the test, is it even a valid requirement?
  - That depends on the threat that you are trying to mitigate. If it is the threat that some non-deliberate problem modifies the software, then the evaluator would need to calculate the likelihood that the test would pass even if the software was modified. Although usually, the whole thing just hangs. But if someone deliberately changes the software, it is a simple alteration to reverse or remove the instruction that branches if the software check fails, so there is no way for software to do a self-test against a deliberate attack. [Kurth]
  - Is it worth putting into a PP? It doesn't seem to be worth much as a security test, but everyone does something like that.
  - Yes, as long as you allow the ST author to add additional tests if their product performs them [Kurth]

- It is driven by a policy, so we should modify it to say that we are trying to detect non-deliberate changes.
- Yes, because otherwise you would need something like a TPM [Kurth]
- So which one is better for this purpose? TST or TEE?
- It is TST. FPT\_TST.2 has that specific requirement. TEE is for test of external entities, such as underlying hardware or testing of network services. [Kurth]
- What if you want to test something like a time source? [Nevo]
- Then you would use TEE. You would at least make sure that the clock is ticking [Kurth]
- We have some cases, such as reliable timestamps, where the ST can either use an internal source or an external network source. Would we use TEE for the external source?
- You would trust that the external source is reliable, because you don't have any control over it. [Kurth]
- Would you at least test to see if the time source is available, because some of your SFRs depend on that time source?
- You might check to make sure that no one is spoofing the time source, but that is not a TEE function, it is more an authentication function. [Kurth]
- We should add an app note to clarify this [Nevo]
- {refer to comments #8, 9, 49, 55} There is confusion about the wording of FTP\_ITP\_EXP and its title.
  - What you're trying to express is that a very specific kind of vulnerability does not happen. This is usually covered in vulnerability analysis, not in an explicit SFR. But in the CC, SFRs generally express something that the TSF should do, not something that the TSF should not do. This may be address in the next version of the CC. [Kurth]
  - We'll work on rewording this offline.
- {refer to comment #9} There is an app note that says if trusted path is provided by the environment, then the SMI package can't be claimed. What does that mean? Does it mean that the SMI package does not need to be used? I thought that the TOE and the environment needed were required to provide a trusted path. [Aubry]
  - A trusted path is required, but it might be provided by the environment, for example, if an intelligent network card does all of the IPsec encryption and that network card is a third-party device and can't easily be evaluated as part of the TOE. [Kurth]

- So if the TOE does not implement the trusted path, can I still claim compliance with the PP? [Aubry]
- The intention is that a trusted path must be used, but if it is handled by a network card that is not part of the evaluation, what do we do?
- The ST author could clearly explain how the trusted path is provided in the overall product but not in the evaluated TOE. Or you could convince the third party to participate in the evaluation and provide the necessary documentation. [Kurth]
- The other part of the SMI package requires network flow mediation, so it would be thrown out with the trusted path part. [Aubry]
- I think that if you use a third party product for trusted path, you would either need to include it in the evaluation or use a certified product or compose the TOE.
- You might need to unbundle those two parts into separate packages [Kurth]
- If we left the SMI package as is, but removed the app note, then could we leave it up to the ST author to deal with the situation with their evaluation lab?
- Yes, they could not claim full compliance but they could claim the other SFRs in the package. They would need to claim that the trusted path is provided by the environment. [Kurth]
- What prevents an ST author from not claiming either part of the SMI package? [Aubry]
- They can't, because there is a conformance rule that says if they have a network interface in their product then they must conform to the SMI package.
- In that case, then the only choices would be to evaluate the third party product or use a certified product and do a composite evaluation. [Kurth]
- We need to put something in the PP guide for this situation [Aubry]
- {refer to comment #73, and to document <http://grouper.ieee.org/groups/2600/presentations/Camas2008/Function%20access%20control%20policy.doc>} Currently, each package has an access control rule to allow users to use the function of that package. This results in many redundant SFRs, and NIAP had commented earlier that they did not like to see administrative functions distributed among packages. The proposal is to consolidate them the common PP.
  - The principle of access control is independent of the packages, but we can't identify the packages in the common PP because that would force the ST author to

- include all HCD functions in their product. Instead, we want to specify the access control policy and require the ST author to include it as needed for whatever packages their product requires. It allows the flexibility for authorizing use of functions of the user is authorized to use the TOE, or authorization for specific functions can be administrator-controlled. [Kurth]
- Where is the actual TOE access control policy stated? [Sukert]
    - It is not stated in a table, like the user data access control SFRs, the policy is formed by the collection of SFRs with partial specifications.
    - The table approach is one way to do it, but the more typical way to specify an access control policy is to specify the rules in the SFRs [Kurth]
  - Is there something that ensures that a user must be authorized to use TOE?
    - An unauthenticated user is not permitted to permit any operation by the SFRs. [Kurth]
  - {refer to comment #6} There were some questions about what is meant by “plaintext”.
    - I thought it meant text, like ASCII [Chen]
    - Plaintext is the unencrypted text, versus ciphertext which is encrypted [Kurth]
    - So we could use “unencrypted data”.
  - There is some general discussion about the NVS package, especially because we received information from NIAP after the last meeting about it. At the last meeting, we had assumed that the US government wanted the NVS package, but NIAP said that they thought it made sense to remove that package because the CC doesn’t deal with mitigating threats when the TSF is not operating and also because they questioned the mitigation techniques. Also, NIAP is more concerned about protecting data in NVS devices that have been decommissioned, and we were dealing with protecting data in NVS devices that are part of an operating HCD.
    - There are specific crypto techniques that the US government requires through FIPS-140, but there is no accepted encryption or overwrite technique for dealing with decommissioned devices [Kurth]
    - So if we stated that the scope of protection is for devices that are designed to be removed by end-users, so we don’t contradict the assumption about physical security, do you think NIAP would object if we left the package in?
      - You would protect data that is leaving the protection of the TOE, like you do with network traffic. Another way would be to extend the scope of the TSF to

include the media itself, like they do for smartcards, but that is a very different and difficult evaluation. The problem with decommissioning is that the NVS device or the whole TOE may not be operating correctly when it is decommissioned, so a solution like overwrite could not be used. [Kurth]

- What is the threat implied by the objective of protecting integrity of NVS data? [Farrell]
  - We are concerned that someone might remove the device, modify it, and reinsert it. Even if it is random data. It should be detected. [Kurth]

## Schedule review [Smithson]

Refer to document:

<http://grouper.ieee.org/groups/2600/presentations/Comas2008/schedule37c.pdf>

- Can you describe the PP evaluation process? When can you start? What do you need from us?
  - It can start when the PPs are stable enough. There will likely be some small changes during the evaluation. We will apply to NIAP to evaluate PP-A, and to BSI for the others. [Kurth]
- So we can't do another draft until after the sponsor ballot period ends.
  - August 27. I suggest that at the end of the next meeting, early in September, we will have reviewed all of the comments and a new draft can be produced after that. We would use that draft for PP evaluation. We could hold off on starting a recirculation until after atsec has had some time to review it. [Wright]
- If we don't get many comments from the sponsor ballot body other than ones we've discussed in the WG, we could have a draft to review at the September meeting and then just put some finishing touches on it after the meeting.
  - There have not been any comments submitted so far. [Wright]
- How long does it take after we apply for evaluation before we can start evaluation? [Sukert]
  - We can start evaluation right away. [Kurth]
- How long do you think it will take from start of evaluation to certificate? [Sukert]
  - If everything goes smoothly, six to eight weeks for evaluation. It depends on how fast you respond to respond to issues. For the scheme part, it should not take long because it is a PP and not an ST, assume it might be another four weeks. [Kurth]

- {Revised schedule was proposed, discussed, and approved. The major change is that PP validation cannot begin until a new draft is issued, and a new draft cannot be issued until the end of the first ballot period (8/27/08). This means that PPs will not be certified until around the beginning of December 2008. It also means that the final drafts cannot be submitted to RevCom for review in their December 2008 meeting, and instead will be submitted for their March 2009 meeting for IEEE standards approval.}

## Next meeting details [Wright]

Refer to meeting slides for

detail: <http://grouper.ieee.org/groups/2600/presentations/P2600-August2008.ppt>

and to the meeting web page for most current status of upcoming meetings:

<http://grouper.ieee.org/groups/2600/meetings.html>

- P2600.1/2/3/4 PPs are under change control
- Deadline for posting documents: August 26, 2008
- Deadline for posting comments: September 2, 2008
- Next meeting will be September 9-10, 2008:
  - Sharp  
1300 Wilson Blvd., Suite 800  
Arlington VA 22209
  - No hotel block
  - Rosslyn Metro station is diagonally across the street. This area is close to the Key Bridge across the Potomac from Georgetown.
  - Parking in bldg -- \$12 per day (\$8 if you arrive before 8 AM). Use the garage entrance on the Fort Meyer Drive side of the building. Take the elevator to the 8th floor..

## Closing [Wright]

*\* Adjourned at 3:05 PM PDT, 8/12/2008 \**