

IEEE P2600 Meeting #25

February 22-23, 2007

Marriott Wailea, Kihei, Maui HI

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, Okidata
Peter Cybuck, Sharp
Satoshi Fujitani, Ricoh
Tom Haapanen, Equitrac
Takeshi Nakamura, Kyocera-Mita
Ron Nevo, Sharp
Ken Ota, Konica-Minolta
Glen Petrie, Epson
Ole Skov, MPI Tech
Alan Sukert, Xerox
Hiroki Uchiyam, Ricoh
Shigeru Ueda, Canon
Brian Volkoff, HP
Craig Whittle, Sharp

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.

Attendees.....	1
Administrivia [Wright]	2
Agenda review.....	2
Minutes and Agenda approvals	2
IEEE patent policy	2
Inappropriate topics review	3
Officers and Editors.....	3
Meeting schedule updates [Wright]	3
TCG update [Volkoff]	4
INCITS CS1 update [Thrasher].....	4
CCVF update [Sukert].....	4
New PARs [Wright]	5
Action items from previous meeting [Wright].....	5

PP structure discussion [Smithson].....	6
Email issues.....	16
Family of PP emails [Smithson].....	16
External Environment as an asset [Wright, on behalf of Aubry]	16
Sameer Yami's email [Wright, on behalf of Yami]	17
Compliance clause [Nevo]	18
Comments database review [Wright]	18
PIN codes are user data or tsf data? [from Aubry]	18
Management data needs a clear definition [from Aubry]	18
PP-C does not normally need user I&A? [from Aubry]	19
We can't always e-shred management data, especially if it is being handled in the OS or by a third party [from Aubry].....	19
P2600 25a main body review [Thrasher]	19
PP-A 25d review [Smithson]	20
DoS/DDoS discussion [Ueda]	22
Schedule [Wright].....	24
Action Items review [Wright]	24
Next meeting [Wright]	24
Closing [Wright].....	24

*** Commenced at 9:10 AM 2/22/2007 ***

Administrivia [Wright]

The following administrative items were reviewed:

Agenda review

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Feb007.ppt>

Minutes and Agenda approvals

The December 2006 minutes were approved without additional changes.
{It was later noted that Peter Cybuck should have been listed as an attendee at the December meeting, and so an updated version of the December minutes have been posted}

The December 2006 agenda was presented, and Smithson asked that the overall project schedule update be added to the agenda. The agenda, with that addition, was approved.

IEEE patent policy

Patent policy was reviewed. There were no patent disclosures made by attendees.

Note: A new patent policy will be instituted in April 2007.

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-Feb007.ppt>

Officers and Editors

No changes.

Officers:

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary: Brian Smithson, Ricoh.

Lead editors:

Editor (clauses): Jerry Thrahser, Lexmark.

Editor (PPs): Brian Smithson, Ricoh.

Meeting schedule updates [Wright]

Apr 24-25, with PWG, IEEE Headquarters, Piscataway NJ

- A TCG HCWG meeting will be held on Apr 23.

May 30-31, tentatively IEEE-USA in Washington DC

- IEEE USA offices are available, but someone will need to arrange snacks/etc
 - need a volunteer
 - room size will accommodate around 18-20 around the table
 - others can fit in the room, but not at the table
- could host somewhere else
 - I could host in Waterloo [Haapanen]
 - I could host in Toronto at HP [Volkoff]
 - BAH might come in to talk about doing evals (in Canada) [Cybuck]
 - could also have NIAP visit
 - Cybuck will confirm

Jul 11-12, location remains open, possibly HP in Roseville CA (nearest major airport is SMF Sacramento), or Redmond/Bellevue WA

- planned for Roseville
- PWG is scheduled for the same week [Farrell]
 - they were thinking Seattle or SF Bay Area [Farrell]
 - Microsoft has not been contacted about it [Farrell]
- another option is to have MS host PWG in Redmond, and HP host P2600 and TCG in Bellevue [Thrasher]

- Lee will check on MS hosting PWG in Redmond, then Volkoff could host P2600 and TCG at HP in nearby Bellevue

The following are tentative dates/locations, for which discussion began at this meeting:

Aug 22-23, location open, possibly Waterloo or Toronto ON

Oct 24-25, location open

- Could shift to Oct 23-24
- I could probably host at Ricoh in Cupertino CA, will confirm [Smithson]

Dec 10-11, with PWG, Austin TX

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]

(TCG web site: <http://www.trustedcomputinggroup.org/>)

- Sharp is now full member
- We had a full meeting at Atlanta member meeting
- Toshiba has also joined but could not attend
- we have been working on the FAQ for the TCG web site presence
- we are reformatting the use case document
- both should be posted soon

INCITS CS1 update [Thrasher]

(INCITS CS1 web site: <http://cs1.incits.org/>)

- CS1 has a meeting at HP in Palo Alto in two weeks
- they work on a broad range of items, ranging from ISMS metrics to crypto standards
- most interesting to this group is the PII standard
 - still dealing with lawyers about how much they can use the PCI standard
- CC v3.1 parts 2 and 3 have gone to "final committee draft"
- update to 15446 guide to PPs and STs is just starting

CCVF update [Sukert]

(No CCVF web site)

- No activity except for some informal meetings at RSA

New PARs [Wright]

Refer to these files:

<http://standards.ieee.org/board/nes/projects/2600-1.pdf>
<http://standards.ieee.org/board/nes/projects/2600-2.pdf>
<http://standards.ieee.org/board/nes/projects/2600-3.pdf>
<http://standards.ieee.org/board/nes/projects/2600-4.pdf>
<http://standards.ieee.org/board/nes/projects/2600rev.pdf>

- standalone PARs for PPs
- modified PAR for main body
 - removed mention of PPs
- reviewed on Tuesday {2/20/07}
 - so far, votes have been for approval
 - will be officially in the system in a week or two
- can we do one for production printing? [Sukert]
 - we can easily add one for that, we are not locked into just these ones
- do the PARs mention environments? [Thrasher]
 - yes, the text is taken from our existing documents
- 2600 PAR was also modified
 - removed the third item in "Purpose" which was to form the basis for CC eval

Action items from previous meeting [Wright]

Main action items were updated on presentation slides:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Feb007.ppt>

Action item spreadsheet was reviewed and updated:

- Pre-meeting:
 - <http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20070216.xls>
- During meeting:
 - <http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20070222.xls>
- Post-meeting:
 - <http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20070228.xls>
- PP eval issues
 - We could get some labs to visit us in April [Smithson]
 - CSC not working on anything less than EAL4 in US [Sukert]
 - SAIC works with Canadian scheme [Cybuck]
- Smithson to send individual AI reminders for next meeting [Wright]
- applet issue -- Volkoff to look into

- PP family issue
 - Peter to confirm with NIAP
 - Ueda-san to post minutes from IPA meeting
- Unspecified audit means unspecified, but the ST must rationalize whatever choice it makes (if it doesn't choose min, basic, detailed...)

PP structure discussion [Smithson]

Refer to:

<http://grouper.ieee.org/groups/2600/email/msg00738.html>

<http://grouper.ieee.org/groups/2600/email/msg00745.html>

<http://grouper.ieee.org/groups/2600/email/msg00747.html>

<http://grouper.ieee.org/groups/2600/email/msg00749.html>

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.1-25d.pdf>

<http://grouper.ieee.org/groups/2600/presentations/Maui2007/objects-25g.xls>

- Goals
 - Write PPs that support a wide variety of HCDs, a wider variety of products than have ever been represented in PPs before, so we are breaking some new ground
 - On top of that, we have four environments (or more)
 - We want to be accepted by at least two major schemes, Japan and US or Canada
 - Defining a security problem definition that is meaningful and relevant to customer communities
 - We have not had as much input as we might like, but DAPS has been helpful and each of us have some customer view
 - Supported by vendors
 - A worst case scenario is that we complete our PPs and it isn't required by customers, or supported by vendors, or accepted by schemes
- Practical goals
 - Customers understand it so they can choose environments
 - Vendors understand it so they can design products, write STs, and get products certified
 - Evaluators need to understand it so they can evaluate
 - We want to get the project done
- Most important goals are: quality and acceptability of the standard, and then usability to all audiences, and the least important goal is how much work and time it takes for us to get there
- Goals are OK, but how we achieve is the issue [Nevo]
 - If we have 10 PPs for one environment, it is difficult for customers to understand

- I thought we agreed at the last meeting to come up with language that said you don't need to apply threats if your product does not have that functionality, and then we would have tables that show what applies
- Also, a vendor could pick and choose PPs and still claim compliance with P2600, and it would be confusing for the customer to understand what the vendor actually complies with
- I would like to simplify it and make it easier
- If we do 10 PPs, and four environments, there's 40 PPs to do, I don't know how long it would take to synchronize all of those, it took us 2 years to do four PPs, and we would need to change the main document also, so I am concerned about how long it would take to do
- We are dealing with multifunctional devices, and if we write these PPs, then we are writing for single functional devices [Cybuck]
 - For the customer point of view, it will be difficult to mix and match all of these PPs to write an RFP
 - From the vendor point of view, there is the cost and timeline for certifying against all of these PPs
 - NIAP talked about using the family of PP structure, but they also said that it might be possible to work a little outside of the established rules, so it may be worth the time to negotiate with them about that
 - It is worth at least having those meetings with schemes and evaluators to see if there is some language we can use in the existing PPs to make it work
- In response to those comments... [Smithson]
 - It is still four documents, four families of PPs, one for each environment, not 40 documents, and so a product would comply with one of the four
 - In fact, it will be fewer PPs because some environments will have no threats in some PPs, so it may be only 20 or 30 PPs and not 40, but still that is a lot of PPs
 - There are rules in the family PPs that disallow a vendor from picking and choosing PPs
 - An ST would need to conform to at least one of the four main functional PPs (print, scan, fax, copy)
 - An ST would also need to conform to all PPs that represent functions that are present in their product
- You would need to validate your product against all of those PPs [Cybuck]
 - But it is still a single ST, and IPA confirmed that it would work that way, you would have one ST that conforms to several PPs [Smithson]

- In that sense, it is not very different from having a single PP that has tables which show which threats apply to which functions. In the family PP case, you would have very clear division of TOE boundaries depending on what functions are present in the ST's TOE [Smithson]
- One area that will require work is that the current list of threats don't divide up very neatly by function, but I think that will be a lot of work whether we use the family PP structure or come up with some language that permits us to write a single PP with optional functions; I don't think it's as easy as coming up with some clever language and adding some columns to some tables
 - That issue is completely separate from the issue of which structure to use? [Farrell]
 - It has been brought up as an issue that we will have much more work to do if we choose the family structure, and I don't think that has been determined; I suspect that the amount of work required will be equivalent in either case [Smithson]
- There was a meeting earlier this week at IPA and my understanding (I wasn't there) is that they would not accept a single PP with options language
- I am open to proposals for alternatives on this that will simplify matters, but not on a philosophical basis. The proposer needs to go to evaluators or schemes or the JBMIA and work out the details. The current proposal went through many direction changes along the way as a result of just such discussions, and I encourage anyone who wants to propose an alternative to go through a similar process
- What if we have a single PP that has sections, one for a printer, one for a fax, etc., so if you have an MFP then you need to do all of them unless you can prove that you don't have that option; it is easier for customers because a product is certified against a single PP, and it is simpler for vendors [Nevo]
 - A complete section for each function, which has interfaces and hard disks and other options for printing, and the same for scanning, etc? Or would you have 10 sections, like the 10 PPs in the family structure? [Smithson]
 - 10 sections, but some things that are the same could be put in an introduction [Nevo]
 - If your device has those functions, they would need to use that section [Petrie]
 - Yes [Nevo]
- How many vendors would want to certify their low end products anyway? [Cybuck]
 - Probably the only things that would fall out are do you have a hard disk and do you have a fax, most everything else you would have [Wright]

- There would be some others, like software update [Nevo]
 - Our original task was to be flexible enough to accommodate any kind of HCD [Smithson]
 - So you could have an ST for a standalone scanner [Wright]
 - If it is properly constructed, then that should work [Smithson]
 - Do we need to have that level of complexity to accommodate standalone products? [Wright]
 - There is a PP in existence now for a standalone copier, so somebody wants one [Smithson]
- If you want to redesign it so we have a PP for an MFP, MFP minus fax, MFP minus hard disk, whatever, you need to write it up, work out how it would be structured, work through some of the details and use cases, get feedback from labs or schemes or whoever, and make a concrete proposal. I tried working through some of these approaches and couldn't get it to work, but that's not to say it can't be done. But I don't want to leave this meeting with action items to change the family structure to something else, find out that I can't make it work, and show up in April with no forward progress since February. If you want to try something else, then by all means try it, and I'll share my own experience if that will help, but I think I should continue on this approach in parallel and we'll see in April.
 - If we can reach consensus now, then we won't have to try it different ways [Nevo]
 - But if the consensus is that we should try to stick with four PPs with options, and then I can't get it to work, we haven't made progress. I tried some of what you are proposing, and I couldn't get it to work. Perhaps you or someone else can. [Smithson]
- What didn't work? [Farrell]
 - IPA rejected it, for one [Smithson]
 - So we have a difference in opinion between NIAP and IPA? [Farrell]
 - At one time, NIAP said that we should look at two PPs and they were both in the family structure, but Cybuck said that they have also indicated there is some room for negotiation. [Smithson]
- But was the options language proposed to IPA, or just the concept? [Cybuck]
 - Just the concept [Smithson]
 - So maybe if a concrete proposal was made, they would accept it. [Cybuck]
 - Yes, please make such a proposal. I think I need to continue working on a direction that I think will work. But perhaps the other approach will be much better and IPA and NIAP will accept it. Some of the PPs in the family will be trivially small, with just a few threats, and maybe the overhead of a PP

structure for just a few threats will make a single PP with options look much more attractive even to the schemes [Smithson]

- I think that when they see the complexity that results from the family PP, and compare it to a relatively straightforward single PP in which some threats fall away in the absence of functions [Wright]
 - It could be, but it may not be so simple. Some of the threats will fall away, but some threats will remain but change depending on the context of functionality. Same goes for objectives and SFRs. [Smithson]
 -
- What are other's thoughts on this? [Cybuck]
 - The JBMIA study group presented the single PP idea to IPA, and they rejected it in favor of the family PP structure. Even the Sharp representative in JBMIA agreed with this. [Fujitani]
 - The customer issue is important. If it's possible for one ST to conform to several PPs, that may make it better for the vendor, but I am not sure how the evaluators will deal with it. I think we need to draft up at least one section of an alternative and get feedback on that before making this change to a family PP structure [Cybuck]
 - A customer may be confused in some cases about what PP to choose, but at least in the PP-A and PP-B environment, we could provide some guidance in another document that helps the customer. This is something we discussed at IPA [Ueda]
 - I think that the guide document, suggested by Petrie, is a good idea and now that IPA and DAPS have brought it up also, there may be two audiences for such guidance: customers and vendors. [Smithson]
- Another way to do it may be to say that we limit the scope to MFPs, so you have an MFP with a fax and an MFP with a hard disk, but otherwise it is out of scope, which would simplify everything [Nevo]
 - That is a major change of scope [Smithson]
 - An option for fax? [Sukert]
 - Basic profile would have copy, scan, and print. Fax would be an option, and hard disk would be an option [Nevo]
 - I don't have the numbers, but I think the majority of MFPs have fax. So would we have eight profiles, four with fax and four without fax? [Sukert]
 - No, instead of nine options, we'd have two options: fax and disk [Nevo]
 - So you would still have a family, but a smaller one: an MFP PP and an option for fax, and an option for disk. [Nevo]
 - What about doc server, software update, system management, etc.? You are really only eliminating print,

scan, and copy, and replacing those three with one
[Smithson]

- What was the structure of the PPs that you mentioned in a previous meeting? Weren't they single PPs with optional language? [Wright]
 - No, they were family PPs. One had four security levels, and you could choose one of the four. The other had something like sixteen functional areas and two EALs, and you could pick any combination of functions and one EAL and generate any of thousands of resulting PPs. [Smithson]
- So you have which basic functions? [Thrasher]
 - Print, scan, copy, and fax. [Smithson]
 - Fax is a top level? Wouldn't that require printing also? [Thrasher]
 - It is separate from printing and scanning because the access control rules can be different for incoming faxes than for incoming print jobs over a network [Smithson]
- Does the proposal to limit scope to MFPs disallow single-function devices, like a standalone printer? [Sukert]
 - Yes [Nevo]
- In production printing, there are some things that are unique to that environment. What do we do about those unique things, like the threat of counterfeiting? [Sukert]
 - You would have another family PP for that environment, and it could have unique threats. It should work OK in the family PP structure or most alternative structures. The only thing that might be a problem is that we had a hierarchical structure of environments A, B, C, and D, and the production print system environment may not fit into that hierarchy. [Smithson]
- In the PP, the TOE description says multifunction. [Nevo]
 - That's the generic architectural description. Right below that, it says that it is only an example. But we could change the scope to MFPs if we want to do that and it better fits the market demand. [Smithson]
- What would someone do if they want a certified printer? [Farrell]
 - I think that everyone who is under HIPAA regulations should have a certified printer, even at the nurse's stations [Smithson]
- Some are hearing this as nine PPs and some are hearing it as four PPs. [Farrell]
 - My proposal is four families of PPs, each containing several PPs (nine in PP-A).
 - So you can refer to one of those families as a single entity [Farrell]
 - The way it would work is that each PP has its own PP name which can be referenced by that name, and which can only

- be used according to the family rules. The ST would refer to each individual PP but must confirm to the family rules.
- Describe an MFP or a printer that doesn't have system management. Why not just include it in each of them? [Wright]
 - You could include it in each of print, scan, fax, and copy, but then each redundant requirement would need to be evaluated. But anyway, there are devices with no management. I have a laserjet 4L at home which has no management, just one button to print a test page. [Smithson]
 - Do we need to include such devices? [Nevo]
 - I was really wondering if the system management threats would be different depending on other functions. [Thrahsler]
 - I don't think that it would for management. For some functions, like access control, there are differences between print and scan and copy and fax, and that's why there are PPs for those functions. So far, I think management is abstract enough that it would apply to all functions. The JBMIA worked on this, and then I worked on it further with Ohta-san and tried combining things to make the smallest set of PPs, and we came up with nine of them for the PP-A environment. [Smithson]
 - How many legitimate combinations would there be? [Wright]
 - Any combination should work, but I don't know how many would represent real products. For example, if we treat an operator panel as an interface, then I can't imagine a product that wouldn't have either a data interface or an operator panel. I am not yet sure that we'll be able to treat operator panel as an interface. But assuming that we can, then every ST would include the INT PP. [Smithson]
 - So it is not optional? [Nevo]
 - It's an option, but if all products have that function, then all STs would reference that PP [Smithson]
 - Why not make it required? [Nevo]
 - It doesn't seem to have a benefit to making some required and some optional, as long as you require that all functions of the product be considered in the ST. Except for the four basic PPs that define a hardcopy device [Smithson]
 - Why not put it in the four basic PPs? [Wright]
 - Then you'd have redundant requirements in cases where you have more than one of the basic PPs. [Smithson]
 - There is a tradeoff between treating things equivalently, like interfaces, and treating them uniquely. If you treat things too generically, then the security problem definition isn't meaningful. But if you treat them too uniquely, you start implying architectural and implementation requirements. For example, I have audit logs and accounting logs as separate objects, but I think we may need

to collapse them into one object “system logs” because otherwise we’re implying that all products in this environment will have auditing and accounting functions. [Smithson]

- One thing I tried was to take the list of objects that were defined in the nine TOE models and see how they corresponded with the existing threats list. I found that some of the objects in the nine models weren’t covered in our existing threats list, and some of the existing threats didn’t have equivalent objects in the nine models, so there is some work to do whichever approach we take. {see objects-25g.xls – missing objects and threats are highlighted}
- Is Device Data a TSF object or a User object? [Thrasher]
 - At first I thought it was a User object, but then it occurred to me that something like tray settings would be a security item in the case of printing checks. [Smithson]
- So the next steps to this approach would be to
- I think that an alternative to this approach should be given a fair trial, and that means it needs to be worked through: language, document structure, dividing up threats/objectives/etc by function, showing the results to evaluators or schemes or JBMIA.
- How would we tell evaluators how to evaluate this? [Wright]
 - Any combination according to the rules should be OK. But each PP should be evaluatable by itself. [Smithson]
 - Would there be any combinations that don’t work? [Wright]
 - I suppose that there might be, but that could be the case in a single PP with options. [Smithson]
 - Is there a naming convention? How do you know what the ST conforms to? [Wright]
 - Each PP has its own name and would be referenced in the ST by that name. {For example P2600.1-PRT is the print function PP for environment A.}
- Any other opinions? [Wright]
 - When we visited IPA, they said that this structure is complex and would benefit from a guide [Uchiyama]
 - That would be a guide for evaluators, and we’d need one for security target writers and for end users [Wright]
 - That might be the case no matter how we structure these PPs. What we are trying to do is accommodate many kinds of TOEs, hundreds of possible products from dozens of vendors, in one PP or family of PPs. It is always going to be complex and would benefit from a guide [Smithson]
- I don’t understand IPA’s position. Why wouldn’t it be easier to simply have a single PP and some language that says if you don’t have this option, then you don’t have this threat? What are they basing their decision on? [Wright]
 - Part of it might be a pedantical adherence to the Common Criteria rules, but to be fair, I don’t think it is nearly as easy

- to make a single PP with options as putting some language in the existing work. Try to write one. Threats will need to be rewritten depending on which functions are present, and break out the SFRs accordingly.
- It's not just threats, it's also the objectives, and the SFRs, and it ripples through the document. The way the current document is written is that there's no clean tie between the function and the threats and objectives and SFRs. That's one thing this proposal does, it forces a. [Thrasher]
 - I don't think the evaluators are going to want to make interpretations like "I know the objective says that you need to protect fax data, but since you don't have a fax, we'll ignore that". I don't think they'll go for that, and this proposal will make it easier for everyone in the end. [Smithson]
 - The SFRs should end up being the same, no matter which approach is taken. [Chen]
 - Yes, if we've done it correctly, the SFRs should be the same.
 - Once you've broken it out this way, wouldn't you now have the information necessary to say that "if you have this function, you need these SFRs"? You've built it up from nothing, and I'm proposing that we tear it down from everything. [Wright]
 - If we had developed these threats around functions to begin with, then it would work that way. [Smithson]
 - Our threat model was based around an asset being threatened over some access method. [Thrasher]
 - Really, we started with a brainstorming session and then later organized it by asset and access. I'm taking more of a security analysis approach [Smithson]
 - I am hoping that you can collapse some of these objects together. I think of object = asset, and for example, is there a necessary difference between accounting and audit logs? [Thrasher]
 - Good example. I think that accounting and audit logs are different from job logs. The only reason they are separate now is that accounting logs deal with functions like printing and scanning, but audit logs deal with all events. Eventually, I hope that they can be combined into "system logs" for purposes of the PP. But when you write an ST, you would consider breaking them out depending on how your actual product works, so if accounting logs are special because you lease the equipment based on usage, you would want to treat them specially in your ST [Smithson]
 - Am I going to get in trouble if I don't have system logs? [Thrasher]
 - You don't require system logs, so I don't have to verify anything [Nevo]
 - No, if you have the object, then it implies that you need to have them in your product in order to use this PP. [Smithson]

- So if I have a printing function, then I need to have accounting and auditing logs? [Wright]
- Yes, or at least system logs if they are combined. That's why it is important to look carefully at these TOE models. Also keep in mind that this is profile A, but B, C, and D would not have so many objects. [Smithson]
- That's why we should genericize the terminology [Thrasher]
- It's a balance between implying requirements on the product, like "you must have audit logs and accounting logs" when really you don't want to make that requirement, versus treating logs too generically, like "logs are logs" but that allows users to look at audit data that they shouldn't be able to look at. [Smithson]
- I think this restructuring involves re-doing all of the threats, which tears up the entire base document, correct? [Wright]
 - I think it is advisable to re-do the threats, and it would involve a lot of work. The only reason I think we should do that is that I believe that the current threats aren't going to stand up to evaluation by function. But if another approach will work, I suspect that it will also require quite a bit of re-work of the base document anyway. [Smithson]
- Has any official body said that our current approach is wrong? [Farrell]
 - Not officially, not in writing, IPA made comments [Cybuck]
 - They haven't seen any document that shows a functional division approach [Wright]
 - No, they saw this document {P2600.1-25d.pdf} and a previous version of it also. They saw this one three days ago. [Smithson]
 - But they haven't seen any other methodology [Wright]
 - They saw the older PP that didn't have a functional breakout. [Smithson]
 - So they can't make a fair comparison. They haven't seen an equivalent outline of an alternative approach. [Wright]
 - Yes, and someone should write that approach. I've heard claims that it is simple and better and therefore it shouldn't be that difficult of a task. Let's make a comparison. [Smithson]
 - Yes, I think we should show IPA another approach. [Nevo]
- Would it be valuable to have an evaluation lab look at it first? [Wright]
 - Yes, the evaluation labs work as consultants and would be a good first step before going to NIAP [Cybuck]
- The two approaches we're talking about assume that the original approach won't fly. [Sukert]

- We had an assumption that we could write what we wanted for everything, and then put in the escape valves for options. [Wright]
- IPA said that wouldn't fly [Sukert]
- No, they didn't see a document that had the escape valves [Nevo]
- They did say that it wouldn't work, conceptually [Smithson]
- They didn't see a fully formed proposal [Cybuck]
- The alternative proposal is to have some language in the document and some tables that say what can be eliminated if you don't have certain functions [Nevo]
- You have some threats that apply to multiple functions [Thrasher]
- You may not need to go to the SFR level, if a threat is eliminated because the function isn't there, then the SFR would be eliminated also [Nevo]
- Some SFRs satisfy multiple objectives, some objectives mitigate multiple threats, so it won't always be easy. [Smithson]
- We need something at a similar level of detail to the current proposal [Cybuck]
- Who will work on this? [Wright]
 - {Nevo and Cybuck will prepare initial draft}
 - Who else will help review?
 - {Farrell , Chen,and Sukert}

Email issues

Family of PP emails [Smithson]

Refer to

<http://grouper.ieee.org/groups/2600/email/msg00714.html>

<http://grouper.ieee.org/groups/2600/email/msg00718.html>

<http://grouper.ieee.org/groups/2600/email/msg00720.html>

- These have been made obsolete by additional information, except for the email by Chen which was inadvertently neglected. I will review and respond. [Smithson]

External Environment as an asset [Wright, on behalf of Aubry]

Refer to

<http://grouper.ieee.org/groups/2600/email/msg00715.html>

- Ms. Aubry provided examples of firewall and VPN PPs which addressed protection of external assets.

- These products are intended to pass information through from one network to another. Our MFPs are not intended for that purpose. [Ueda]
- I don't think the intent was that we would provide full firewall functionality, but these were the closest examples that Ms. Aubry could find. [Wright]
- There was some opinion that we should not try to protect assets that are outside of the TOE, but others contended that we need to provide some protection because it is so important to customers. [Thrasher]
- There are two cases, one is where an attack is propagated through interfaces on the HCD, and the other is where the HCD is attacked and used to directly attack external devices. [Smithson]
- Filtering is probably not the right approach for this. Instead, we should use access control and prevention of pass-through. [Wright]
- Filtering can help with denial of service. [Nevo]
 - But if we prevent passthrough, then the DoS stops at the HCD. [Wright]
 - Except that it can force the HCD to reply [Nevo]
 - We will talk about DoS issues in general later [Smithson]

Sameer Yami's email [Wright, on behalf of Yami]

Refer to

<http://grouper.ieee.org/groups/2600/email/msg00727.html> {and many responses}

- Regarding t.ud.phy.output, yes, it is not in PP-A v24 and should have been there based on a decision made in July 2006 [Smithson]
- Regarding the TOE and operating system issue:
 - The question is: do TOE threats apply to temporary and other files created by the underlying operating system?
 - Yes, the operating system is inside the TOE, so it can apply to the underlying operating system files
 - The question doesn't really ask about specific threats, but it could be relevant to salvage threats [Smithson]
 - Swap files and cache files can contain all sorts of useful information [Thrasher]
 - t.tsf.salvage generally covers TSF data, and applies to PP-A and PP-B; t.ud.salvage applies to PP-A only [Smithson]
 - so if you use encryption to protect disk data, you'd need to encrypt cache files too? [Nevo]
 - if you don't want to modify the underlying operating system, there are some disks that encrypt in the controller [Wright]
 - we could specify t.tsf.salvage more specifically and limit the data that is protected [Smithson]

- so we are saying that need to encrypt everything for all products that we want to certify? [Farrell]
- you could create a virtual ramdisk and use that instead [Volkoff]
- Brian Volkoff will write up a response

Compliance clause [Nevo]

Refer to

<http://grouper.ieee.org/groups/2600/drafts/compliance/MFD%20Compliance%20Clause-25a.pdf>

- includes comments from last time
- also added B environment
- parenthetical stuff like "O.I&A from PP-A" should be removed, because this goes in the main body of the standard and doesn't refer to PPs [Thrasher]
- changes in the objectives in this document should also be made in the appropriate PP also, since that is where they came from [Smithson]
 - 1.2.1.1 objective change needs to be reflected in PPs
 - 1.2.1.4 "the Management"
 - 2.2.2 "assets of the HCD"
- DOS mitigation objective (1.1.1.6) should not be to protect all assets [Sukert]
- environment B section is mostly the same

Comments database review [Wright]

PIN codes are user data or tsf data? [from Aubry]

- I think they are TSF data because they affect the operation of the TSF, but on the other hand, they are created by the user and for the user which also fits the definition of User Data. In any case, it would not be User Document Data. [Smithson]
- the same applies to other user credentials [Smithson]
- Smithson will look at other PPs/STs to see how they handle credentials [Smithson]

Management data needs a clear definition [from Aubry]

- should it be one definition that is tweaked for each profile? or each profile writes its own? [Wright]
 - I think it should be one definition that is subsetted down for b, c, d [Smithson]
- management data is not an official CC term, but we have been using it for a long time [Smithson]

- it seems like it ought to be related to CC management (as in FMT SFRs), but I am sure it isn't and instead is more related to system administration type of management [Smithson]
- if we list the types of data, even in a "such as..." form, does that imply that we must have that kind of data in every implementation? [Thrasher]
 - I hope not, but if that appears to be the case, we might make a more general definition and then put the examples in an app note [Smithson]
 - I am also concerned that if we have a list of examples, but a particular TOE does not have any of those kinds of data, will that be a problem for ST evaluation? [Smithson]

PP-C does not normally need user I&A? [from Aubry]

- maybe not unique user ID, but it will often have some kind of authorization process (such as, did you pay?) before allowing operations [Smithson]
- I thought we were handling this through the use of an anonymous or guest user, which should be OK as long as we don't require a unique ID and don't require a particular strength of password [Smithson]

We can't always e-shred management data, especially if it is being handled in the OS or by a third party [from Aubry]

- this is like the OS issue that Sameer brought up [Thrasher]
- does this imply that if encryption is used, e-shred is not needed? [Volkoff]
 - they provide different kinds of security [Smithson]
 - DoD people require e-shredding even if the data is encrypted [Thrasher]
 - encryption is not a substitute for e-shred [Volkoff]
- even with the current requirement, there is a window of time during which data hasn't yet been e-shredded (such as if there is a power fail) [Thrasher]
 - but the TOE has no control over that [Volkoff]
 - we don't specify the timeliness of deletion, it could be every hour [Thrasher]

P2600 25a main body review [Thrasher]

Refer to

http://grouper.ieee.org/groups/2600/drafts/FullSpec/IEEE_P2600_v25a.pdf

- compliance clause description shouldn't say that it defines security mechanisms [Sukert]

- so you just say that you are compliant with clause 10? [Nevo]
 - you say that you are compliant with the whole standard, for a particular environment [Wright]
- is it normal to have a statement in the standard about how you state your compliance, such as "this product is compliant with IEEE Std 2600 for Operational Environment A" [Smithson]
 - we can put that in clause 10 [Wright]

PP-A 25d review [Smithson]

Refer to

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.1-25d.pdf>

- {this was intended only as a walkthrough to familiarize people with the content of this partial draft of a Family of PPs}
- The document contains some real content and also some descriptions of the structure of content that will be inserted later. Descriptions are in square brackets.
- If we have one PP and not a family of PPs, would we use the same format? [Nevo]
 - I used the new IEEE template and wrapped it around the common criteria recommended outline from part 1 of CC v3.1 [Smithson]
- Rules for use:
 - At least one of the basic four HCD PPs must be used (print, scan, fax, or print)
 - Any and all of the nine PPs must be used if the ST's TOE contains functions that are represented by the PP's TOE
- Demonstrable or Strict conformance? [Nevo]
 - I thought that we had agreed to use Demonstrable [Smithson]
 - What is the benefit of Demonstrable? [Farrell]?
 - Demonstrable allows an ST author the flexibility to demonstrate that the same or different solution is described for the same problem definition
- I included ALC_FLR.2, but I don't think we have resolved this
- Document Server may not be the best name, but it is a document storage and retrieval function. The distinction is that a document is stored during one job and can be retrieved during another job, possibly by a different user, possibly multiple times.
- Management refers to any kind of HCD management, which we will need to be careful to specify broadly enough so as not to imply specific functional requirements
- Nonvolatile Storage refers to storage of data on devices that can be "practicably removed" by unauthorized persons for analysis and

recovery. The idea is that NVRAM or Flash that is surface-mounted on a controller wouldn't qualify, but a hard disk that can be unbolted would qualify. It would be left to the evaluator to make a determination for devices that are in the grey area.

- Software Installation still has an issue about whether or not to include downloadable applets. The issue is that if a normal user can invoke downloading applets, then it is a vulnerability (unless it is limited to specific applets and they have been included in the TOE)
- Interface includes any kind of data interface, but I am also trying to include operator panels and other physical controls. I am not sure this will work.
 - Many operations can be performed either over a data interface, such as on a TWAIN client, or on an operator panel, which is why I am trying to treat them equivalently
 - I think we need to treat web servers specially because they have a lot of vulnerabilities and they are a common target for attackers [Sukert]
 - Maybe web servers and operator panels would fit in a new PP that deals with user interface issues? [Smithson]
- Some of these PPs would probably apply to just about every conceivable HCD that one would want to certify. For example, they will probably all have interfaces and management. But it didn't seem to add any value to make the rule more complex by requiring those. I also wasn't sure that those could be combined together because then if you had some of the combined functions, you would require all of them.
- The part of a PP which normally provides a "TOE Overview" is a little more difficult in a family structure. I needed to start out with a family overview and then proceed to give individual TOE overviews.
 - One of the example family PPs that we've been looking at (public key-enabled applications) has guidance for the evaluator; maybe we can use some of that [Wright]
- The previous PPs had a lengthy description of MFP architecture. I tossed that out because I didn't want to imply that all MFP functions were required, and I think that such information could be contained either in the main body or in the Guide document.
- In the family overview, I define the different kinds of entities and describe the diagram notation that is used for each TOE. I think that these diagrams should be re-done in a standard notation like UML.
- I used the term "channels" to include interfaces and input/output trays. The reason I needed to have a term that included both is that some operations can use either one, and I didn't want to imply a requirement for one or the other or both.
- I am not sure if the distinction between "normal" and "privileged" subjects will turn out to be important. I included it because it was

how Helmut Kurth did it in his Modeling Security Functional Requirements presentation, and I was using some of his techniques. This distinction may go away.

- In the security problem definition, the threats and objectives can probably be listed in total with some indication of which PPs they apply to. However, the rationale tables will need to be created for each PP in order to show completeness of each PP.
- SFRs can probably be listed in total also, but the SFR rationale tables will need to be done for each PP.
- SARs will be listed in total and will apply equally to all PPs because they are all at the same EAL.

DoS/DDoS discussion [Ueda]

- {Ueda-san presented some slides that provided a DOS/DDOS description from Japanese National Police}
 - about 3 years old but conceptually still applies
- "there is no fundamental defense for DDOS attacks"
- according to CC
 - SFRs must trace back to at least one objective
 - each objective must be fulfilled by at least one SFR
- O.RESILIENT and FPT_RCV.2
 - needs to be able to determine that an attack is happening
 - will need to judge whether to go into maintenance mode or not
 - it is too much to implement
- where does it say that you need to identify the attack? [Nevo]
 - FPT_RCV.2 requires it [Ueda]
 - It only says recovery [Nevo]
 - It says that maintenance mode is required for "certain kinds" [Smithson]
 - You need to at least recognize that it is an attack [Farrell]
 - We were talking about recovering in the sense of having robust software implementation that could withstand an overload condition, whether it's an attack or not [Smithson]
 - How would you validate it? [Nevo]
 - That's the point. At EAL2 or EAL3, there's no requirement to validate robustness of software (not robustness in the NIAP definition) [Smithson]
- We are thinking that something like a watchdog timer that would detect a hang-up and reboot, but FPT_RCV requires more than that [Ueda]
- In the description of FP_RCV, the SFR requires a list of failures or service discontinuities

- If the machine hangs up, you can identify that you are stuck but you don't need to identify the kind of attack [Nevo]
 - But in some cases it would need to go to maintenance mode [Ueda]
 - If it tried to automatically recover and got stuck again, it could detect that and then go to maintenance mode [Wright]
- List of failures and discontinuities could be “network interface failure” [Thrasher]
- The whole purpose of trusted recover isn't for that. If you look at appendix J.8 in CC part 2, it talks about crashes caused by various failures and unexpected or erroneous discontinuities, not DoS attacks. It's purpose is to ensure that if those kinds of failures occur, the device doesn't come back in an insecure state. [Smithson]
 - “Communications failure” could be a denial of service attack [Wright]
- O.RESILIENT requires automated recovery, not human intervention [Ueda]
 - If automated recovery didn't work, then human intervention wouldn't be unreasonable [Wright]
- The kind of automatic recovery that O.RESILIENT talks about is to sit and wait for the attack to go away. That isn't the kind of thing that one can test for. [Smithson]
- In many cases, you won't need to do anything to recover, it's more of a robustness issue [Wright]
- My suggestion is to leave T.DOS threats in P2600, but not in the PPs because it is one of the problems in CC world that is solved by vulnerability assessment test. [Ueda]
 - What does that mean? [Wright]
 - It means that tests are run during the AVA part of the evaluator's testing. We don't need to specify the tests. The evaluator is expected to test for common vulnerabilities for this class of device. It's a normal part of evaluation. [Smithson]
 - If it's not specified, then it's not likely to be tested [Cybuck]
 - Increasingly, I think evaluators are required to perform AVA tests. [Smithson]
 - Threats of this kind change [Volkoff]
 - There was a presentation at ICCV about it, which said that AVA should take place throughout the evaluation and not just at one point. Also, NIAP wrote a policy that stated that vulnerability assessment would be part of their requirements. It's an assurance requirement, built-in, we don't need to specify. [Smithson]
- Can we have security objectives in the main document and not have them in the PP? [Nevo]
 - No, I don't think so [Smithson]

- We could have objectives for compliance with the standard that are not checked in the PP because it is not possible to check for them in the common criteria world [Wright]
- I thought we agreed that we would not do that, because otherwise you would have problems when someone gets certified but cannot claim compliance with the standard or vice versa. [Smithson]
- One thing that we might be able to put in the main document is to mimic the evaluator's instructions from the CEM (aka CC part 4) because that it does state that the evaluator will perform vulnerability assessment. [Smithson]
- Let's post these slides to the mailing list and discuss and decide at the next meeting [Wright]

Schedule [Wright]

Refer to meeting slides for the new schedule

<http://grouper.ieee.org/groups/2600/presentations/P2600-Feb007.ppt>

Action Items review [Wright]

Refer to meeting slides for general action items

<http://grouper.ieee.org/groups/2600/presentations/P2600-Feb007.ppt>

- Other action items will be added to the action items database during creation of the meeting minutes

Next meeting [Wright]

- **Two full days** in Piscataway. For more information, refer to: <http://grouper.ieee.org/groups/2600/meetings.html>.

Closing [Wright]

See you in New Jersey!

** Adjourned at 12:25 PM, 2/23/2007 **