

IEEE P2600 Meeting #11
May 19-20, 2005
Holiday Inn on King, Toronto, ON, Canada

Attendees

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

Carmen Aubry, Océ
Nancy Chen, Okidata
Peter Cybuck, Sharp
Nick Del Re, Canon
Tom Haapanen, Equitrac
Takanori Masui, Fuji-Xerox
Ron Nevo, Sharp
Yusuke Ohta, Ricoh
Sameer Yami, Toshiba America Business Solutions

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 9:20 AM 5/19/2005 ***

Administrivia [Wright]

The following administrative items were reviewed:

Introductions

(see Attendees, above)

Agenda review

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2005.ppt>

- Mark Tillinghast was going to provide an Excel sheet with all email comments in an organized table, but had not done so by the beginning of the meeting. Don copied all emails into a word document, which we will use for review.

- Is the DAPS issue on the agenda? [Nevo]
 - Yes [Wright]
- Is Enterprise vs. High Security definitions on the agenda? [Nevo]
 - Yes [Wright]

Meeting fees

Don collected US\$70 from each attendee to cover meeting fees for the hotel, as previously announced and agreed. Don will email receipts to each person during the week following the meeting for their expense reports.

Minutes and Agenda approvals

April's minutes and May's agenda were approved without changes.

IEEE patent policy

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2005.ppt>

No response to question about patent disclosures.

Inappropriate topics review

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2005.ppt>

Officers

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary / Lead Editor: Brian Smithson, Ricoh.

Editors: Jerry Thrasher, Lexmark; Ron Bergman, Ricoh; Yusuke Ohta, Ricoh (High Security PP); Ron Nevo, Sharp (Enterprise PP); **Carmen Aubry, Océ (SOHO PP) ← new**

Meeting schedule update

July's meeting will be held on July 11 and 12 at Apple's R&D Campus, 1 Infinite Loop, Cupertino CA, in conjunction with the PWG. . The P2600 meeting will be held on Monday and Tuesday, and PWG meetings will be held on Wednesday through Friday. Details are available on the P2600 web site at <http://grouper.ieee.org/groups/2600/meetings.html>. Note that the Cupertino Inn is within reasonable walking distance of the Apple Campus, others not so sure.

Sep 15-16 West Caldwell, New Jersey, at Ricoh Corporation headquarters. Details will be published in June on the P2600 web site.

Oct 24-25 New Orleans - w/PWG

Dec 13-14 San Diego - considering HP site, but open to suggestions

The most up to date schedule for meetings in 2005 is listed on the slides
<http://grouper.ieee.org/groups/2600/presentations/P2600-May2005.ppt>

TCG update [Wright]

- Brian Volkoff did not attend this meeting.
- Next meeting is June 21-24 in Amsterdam
- There have been no HCWG meetings since last report
- Volkoff wants to schedule an evening HCWG meeting to enable teleconferencing for US people who can't attend

Action items from previous meeting [Wright]

Refer to slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-May2005.ppt>

See slides for completed items

Sec 1 (Smithson)

- graphics updated
- other items still open

Sec 2

- section 2 cross-check
 - complete, one item needs attention (unlocked operator panel)
- sec 4 team to look at environments in sec 2
 - in progress -- threat analysis
- decide whether to include security environments in final standard
 - still open

Sec 3

- missing sections
 - largely complete
- move asset section to section 1
 - remains open
- actual recommendations for each threat, aligned with section 2 threats
 - is aligned, but (as above) some recommendations not complete

Sec 4

- HS [Ohta]
 - updates done
 - need to do some more work on rationale section
- Enterprise [Nevo]
 - multiple drafts circulated
- SOHO [Aubry]
 - 1st draft
- no work on Public yet
- threat analysis [Smithson]
 - need to be on the agenda for this meeting, before PP
- the name of HS may need to change [Nevo]
 - was based on NIST doc, definitions taken almost verbatim including the name HS [Wright]
 - issue is about confidence, EAL2 not enough [Aubry]
 - good idea to get something out there even at a lower confidence level, get experience, then if needed do an EAL4 or something [Wright]
- another issue in consistency manual, not just confidence but also functional requirements [Ohta]
 - if DAPS requires medium or high robustness, then we need more functional requirements
 - even in basic robustness, there are some different requirements that we don't currently have

DAPS Issues [Wright]

- Are there deficiencies in our profiles based on consistency manuals for basic and medium robustness?
 - basic is EAL2, we could achieve with some additional requirements [Aubry]
 - basic we can do, but medium or high robustness is probably not reasonable for us to do [Ohta]
 - these manuals are US-centric, evaluation in other countries may be a problem [Ohta]
 - it may be possible in other countries, but there might be difficulties because they don't know this manual
 - on the other hand, we need to use the manuals in order to use NIAP to evaluate our PP
- If we use the manuals and develop our PPs accordingly, would it cause evaluation in another country to fail or otherwise not be possible?
 - no, nothing like that [Ohta]
- Can we create a list of what changes we need to make in order to follow the NIAP document, has anyone made such a list?

- I've seen some that they have and we don't, and some we have they don't [Chen]
- Is it OK to exceed their guidelines?
 - you should specify in your ST that either you have only what is in the PP or that you have all of what is in the PP plus more [Aubry]
 - there are some requirements in the manual that seem brand-specific, like alarms [Chen]
- page 54 (basic robustness) lists three options for compliance: exact, strict, or demonstrable [Aubry]
 - demonstrable may allow us to show that we meet their requirements without using their exact specifications
- in conversation with David Freas, DAPS might certify our HS and Enterprise PPs without charging us because it fills their need [Wright]
 - maybe just do HS compliance with NIAP and leave Enterprise alone [Nevo]
 - need to look at how much work is involved [Wright]
- How do we go about making this assessment? [Wright]
 - there is a list of 26 instructions
- Should we go through it as a group, or do it for next meeting?
 - we have more time than usual before July meeting
 - first thing we should discuss is whether how difficult it would be to comply before doing a detailed assessment [Ohta]
- getting evaluated without funding would be a significant benefit
 - it is possible, just a lot of editing
 - Are there other profiles we can look at? [Yami]
 - there is another international group, can't remember the name, working on protection profiles [Chen]
 - INCITS [Wright]
 - it will be the US TAG for JTC-1 SC 27
 - there would be other groups advising on JTC-1 from other countries
- Can we divide up the work?
 - may not be possible because some in the group have more or less familiarity with PPs
 - could do as a group, but off-line anything that takes too long [Smithson]
 - agreed, do as a group [Wright]

NIAP basic robustness assessment [Wright]

- Instruction 1: Characterize Robustness
 - Any conflicts in the blue text for Appendix D?
 - reference to DoD is an example, could be made more generic by calling it "United States Department of Defense"

- should look at their definitions and descriptions of authorization, access, and entities to make sure they are consistent with ours [Smithson]
- Instruction 2: Accommodating Software Only TOEs
 - Do we have any software only TOEs?
 - we can have, see 1.2 in the PPs [Nevo]
- Instruction 3: Uses of Basic Robustness
 - their text seems to be lighter weight than our HS environment, it's more like a good description of what our Enterprise PP should be [Smithson]
 - the instruction doesn't mandate this text, we could modify it to fit our environment; it only suggests that you have a discussion [Wright]
 - we could use the suggested text from the Medium Robustness manual [Nevo]
 - as long as that doesn't have other implications [Wright]
- Instruction 4: Assurance Requirements for Basic Robustness
 - EAL2 +
 - flaw remediation
 - examination of guidance
 - is reasonable [Ohta]
 - we have ASE, they don't [Nevo]
 - Did they omit it deliberately? [Wright]
 - it is always required, at any EAL [Ohta]
- Instruction 5: Content and outline of a Protection Profile
 - we have pp application notes as section 6
 - CC doesn't specify a strict structure [Ohta]
 - we could move it then [Wright]
 - 6.2 (if it is the same as in the medium robustness manual) would be new [Smithson]
- Instruction 6: Format for the title page of a Protection Profile
 - Required title is "US Gov't Protection Profile for...", is that a problem? [Smithson]
 - we could use that on the cover page for NIAP, but not have the cover page in the IEEE spec [Wright]
- Instruction 7: Assumptions
 - some name changes
 - we may need to modify some assumptions [Ohta]
 - we don't have A.NO_GENERAL_PURPOSE [Wright]
 - is for server PPs, see footnote [Ohta]
 - we could safely include it though [Wright]
- Instruction 8: Describing Threats
 - what does it mean "threats the TOE cannot recognize"
 - recognize is probably not a good word to have used
 - we may need to remove some threats from PP [Ohta]
 - it is common sense, don't put something in the PP that you can't address [Aubry]

- Instruction 9: Threats, Policies, Objectives and Requirements
 - this will take some work to go through the whole instruction
- Instruction 10: Specifying Requirements on the IT Environment
 - don't see any issues here, since we don't have any IT environment requirements
 - I'm wondering if we should have some IT requirements [Farrell]
 - there were some issues, such as using LDAP [Wright]
 - it seems like the instruction is cautioning us against doing that [Farrell]
 - if we have dependencies, we should include them [Farrell]
 - if we have assumptions that depend on the IT environment, we should say that they can be met by using certified components at the EAL [Wright]
 - sec 6.3 of HS PP talks about that [Ohta]
 - if an ST can use local authentication or LDAP, in one case there would be no IT requirements and in the other there would be IT requirements; how can one ST address both? [Wright]
 - we will need to make a question and ask NIAP about it [Wright]
 - other evaluators may have different answers [Ohta]
- Instruction 11: Scheme Interpretations
 - probably OK unless different evaluating agencies (e.g. different countries) have different interpretations
- Instruction 12: Rationale Section
 - need to go through this offline
- Instruction 13: Conventions
 - some formatting work to do in SFRs
 - What about NIAP refinements, which are noted by NIAP in the SFR name? [Chen]
 - refinements are acceptable in CC2.2 [Ohta]
 - however, other countries may not be able to interpret a NIAP refinement [Ohta]
 - need to look at which, if any, NIAP refinements are required and whether they'll cause problem outside of NIAP [Wright]
- Instruction 14: Glossary
 - we don't just have a "user", we have various flavors
- Instruction 15: Degree of Compliance
 - we are using "demonstrable"
 - need put that in the intro
 - also the definition of "demonstrable" [Smithson]
- Instruction 16: FAU_GEN.1-NIAP-0407 Audit data generation
 - is an explicit SFR, not just a refinement [Ohta]
 - however, it is acceptable outside of the US [Ohta]

- the difference between Basic and Medium for this is the addition of 16-2 which states that a user identity must be associated with audit events [Smithson]
- we should ask whether this would be acceptable outside of the US, otherwise we are guessing [Aubry]
- most influence is from US, CA, AU, and UK, so we can ask them [Cybuck]
 - NIAP will of course be OK
 - I can ask in Canada
- Instruction 17: FAU_SEL.1-NIAP-0407 Audit event selection
 - just a refinement
- Instruction 18: FAU_STG.1-NIAP-0429 Audit event storage
 - just a refinement
- Instruction 19: FAU_STG.3 Action in case of possible audit data loss
 - is not in our PP [Ohta]
 - is OK not to have it, NIAP is just specifying how it should be used if you use it [Wright]
- Instruction 20: FAU_STG.NIAP-0414 Audit event storage
 - we have STG.1 and STG.4
 - they are recommending we specify audit protection, which we do, and they say it is "desirable" to have it administrator-settable [Smithson]
 - keep as is, leave it up to the ST-writer to add if they want [Wright]
- Instruction 21: FIPS 140-2 (Security Requirements for Cryptographic Modules)
 - FIPS works in Canada too [Cybuck]
 - Is there another country that mandates its own validation? [Wright]
 - in other words, passing FIPS means that you fail somewhere else
 - problem is that there is nobody in Japan to validate FIPS [Ohta]
 - FIPS isn't just about the algorithm, it also looks at key management and other things [Cybuck]
 - from a user point of view, it is acceptable [Ohta]
 - it's a requirement for many sales to US gov't [Cybuck]
 - Would anyone design a product with this kind of security that had no intention to sell to the US gov't? [Wright]
 - looking at the FIPS compliant list, it is done down to the firmware revision level and operating mode [Smithson]
 - some lab may need to see your validation certificate before passing you on CC [Wright]
 - I thought FIPS wasn't required until EAL4 [Ohta]
 - but if we specify it in the PP, it doesn't matter that it is EAL2 [Cybuck]
 - Peter will talk to DAPS and/or NIAP [Wright]

- Instruction 22: FDP_ACF Access control functions
 - only difference is in ACF.1.3 and ACF.1.4 which allow "no other rules" as a selection [Wright]
 - same problem instruction 16 [Ohta]
 - ccv2.1 + international interpretations -> ccv2.2
 - NIAP local interpretations may not be accepted by other countries
 - it is an explicit requirement
 - If one country certifies a PP or product, don't the other countries have to accept it? [Wright]
 - they may post it with comments or qualifications [Cybuck]
 - what this one does is that it allows you to claim 1.3 and 1.4 without actually doing anything [Smithson]
 - defer as with instruction 16 [Wright]
- Instruction 23: FDP_IFF.1 and .2 Information flow control functions
 - difference is in the second assignment statement [Wright]
 - Is there a comma missing between "attributes" and "list"? [Smithson]
- Instruction 24: FIA_AFL.1 Authentication failures
 - we can do this one easily, it is not an interpretation [Ohta]
- Instruction 25: FIA_USB.1 User-subject binding
 - Is a mistake? it refers to medium robustness [Wright]
 - the reference is to a table, and that table in the basic robustness includes FIA_USB.1 [Smithson]
 - we don't invoke FIA_USB, and it is only recommended [Wright]
 - rationale: we don't support users acting on behalf of other users
- Instruction 26: FPT_TST_EXP.1.1 TSF self test
 - it requires all three modes, not allowing selection of one or more [Nevo]
 - difficult to do the "on request" part for low-end products [Smithson]
 - And why is "at request of administrator" in square brackets?
 - since it is recommended not required, leave as is to support low-end products [Cybuck]
- Conclusion?
 - there are more SFRs in table 7 that need to be discussed [Aubry]
 - this is in Instruction 9 [Wright]
 - We would need to put, in section 1 of the PP, that it is based on CCv2.2 plus NIAP interpretation. Currently it says just CCv2.2 [Ohta]
- "US Gov't PP" requires also PP development process (another document)
 - some of the principles we could or do follow

Document reorganization proposal [Smithson]

- {Smithson presented overview of proposal that was presented via email; see email for original proposal}
 - Identify organization of the document in the intro
 - Bring in material from Section 3 about HCDs and put it into intro
 - More description of threats
 - PPs and Section 2 are organized by asset
 - Section 3 is organized by access
 - Both are useful, perhaps with a cross-reference
 - Overview of threats, then specific threats, and then “best practices” (split up between manufacturers and end-users)
 - Jerry recommended that the “best practices” should come before the specific threats
 - Then the PPs, with their fixed format
 - Some of the material in Section 3 that is lengthy or detailed could be put in annexes
- Where to put the definitions and acronyms? [Wright]
 - I don't know, where do they usually go? [Smithson]
 - right after the intro [Wright]
- This could reorganize the teams [Smithson]
 - Not so bad, the sections just move around {see designations of source sections on slides} [Wright]
- An outsider viewing the document might find it useful if there was a graphic (like in the CC document) that you could click on to go to different sections. [Cybuck]
 - Would work if it was online. Would it still be useful for a paper copy? [Wright]
 - That would be useful [Cybuck]
 - Which diagram? [Smithson]
 - {Like figure 11 or figure 12 in CC v2.2 part 1}
- Where should the PP intro go? [Wright]
 - At the end of the Threats section since the PP has information about mitigating threats that isn't covered in that section [Smithson]
- Can PP's be separate? [Ohta]
 - It will be for CC evaluation; we may be able to do something for the P2600 spec, we will need to talk with the IEEE Editors about that [Wright]
- {See slides for accepted proposal and designation of source sections of current document}

Email comments

- {Email originator's name is indicated in the [square brackets] at this bullet level}
- The current figure indicates that some components of an HCD, especially the Operating Panel and Local Interfaces, are outside of the TOE. [Sukert]
 - Figure has been updated but didn't make it into the PPs. Will be inserted into PPs. [Smithson]
- The entry for T.TSF.CRED indicates that the security objective O.MONITOR applies to this threat. However, the corresponding discussion for the T.TSF.CRED threat in Section 7.1.2, Correctness, Table 11 Additional justification for Security Objectives, page 51, does not include a discussion of the O.MONITOR security objective. [Sukert]
 - Make Table 10 and Table 11 consistent in terms of what security objectives apply to the threat T.TSF.CRED. [Wright]
- Each of these four threat discussions references security objective 'O.PROTECTED'. To be consistent with Table 10 and Section 4.1.4 this should be 'O.PROTECT'.
 - O.PROTECTED changed to O.PROTECT throughout. [Wright]
- Table 12. Correspondence between security objectives and security functional requirements indicates that SFR FTA_SSL.3 helps achieve security objective O.I&A, but this paragraph that provides the rationale for O.I&A doesn't discuss SFR FTA_SSL.3. [Sukert]
 - This section is currently under development. Recommendation: Add to this paragraph how FTA_SSL.3 helps achieve O.I&A. Justification: Completeness and consistency between Table 12 and corresponding text. [Wright]
- When a printer starts to work, the power consumption goes way up. If this were a trigger for RF eavesdropping, it would be a good one. Typical Idle Versus Busy values are 20 Watts Idle to as much as 1.2 kWatts for laser printers.
(http://www.macalester.edu/cit/faq/power_usage.html) [Tillinghast]
 - Rejected. In a high security environment, critical infrastructure including electrical circuits would be inaccessible to unauthorized people and therefore the monitoring thereof would not be likely. [Wright]
- Since DAPS has proposed to an NMCI workgroup the use of the High Security PP as a reference document it would be useful to inform that group that our profile was not intended to address the high level requirements of a government classified network. While it can provide very useful guidance a modified version would very likely be required for that unique environment. [Nevo]
 - Change the definition of the HS environment in section 1 to exclude government classified environments. We could consider Adding "Commercial" in front of "High Security." [Wright]

- Is it our intent to provide reference documents for the DAPS/NMCI workgroup? If yes, the threat list and target environment descriptions will have to be re-evaluated. [Nevo]
 - No. If anything we'll wait until we get specific feedback from DAPS. [Wright]
- We need to resolve the inconsistency of definition between T.UD.IMP.* (man-in-the-middle attack) in Section 2 and T.UD.IMP in the PP, and also need to discuss countermeasures against it (by I&A? or by configuration protection and well-managed network?). [Ohta]
 - Change the names of the threats to T.UD.ALTER.FAX, T.UD.ALTER.PRINT, T.UD.ALTER.SCAN and these include both altering the USER DOCUMENT as well as deleting it in transit. [Wright]
- 1.3.5 security in public environments [Yami]
 - someone could print confidential documents that could be compromised [Yami]
 - Would someone want to print confidential documents at such a location? [Wright]
 - maybe there could be an obligation to use a more secure environment, for example, at a hotel that might host meetings that have confidential information [Cybuck]
 - given the litigious nature of the US, a terms of use would probably be so full of disclaimers that it wouldn't matter [Wright]
 - How about something like PIN-accessed print? [Wright]
 - a lot of hotels are offering printing services, and you don't want your docs laying around in the business center waiting for you to pick them up [Cybuck]
- table of recommended algorithms and key sizes [Yami]
 - Sameer Yami to do first draft
- 4.2.1 item 3 use "authentication information" instead of "password" [Yami]
 - use "authentication data" instead, more consistent with CC terminology [Ohta]
 - OK, use "authentication data" [Wright]
 - should also look for other discussion of passwords in mgmt data elsewhere and make consistent [Smithson]
- 4.2.1 table 98 add role for auditor [Yami]
 - Proposing to add this to add a new "actor"? [Wright]
 - Wouldn't this be the administrator? [Nevo]
 - It may be a separate person [Smithson]
 - Auditor may be checking on the Administrator [Aubry]
 - May make sense for auditor to have change permissions and administrator have read-only [?]
 - We discussed before and decided not to have a separate role. [Ohta]

- What are the implications for the device? Would each device need to have an interface for auditors? Another login? [Cybuck]
- Would this be only necessary for HS environment? [Wright]
 - enterprise should have separate role too [Chen]
- If we define it, does everyone need to implement it? [Wright]
 - you're either compliant or not [Cybuck]
 - we don't require anyone to implement each role [Smithson]
- OK to add the role to HS and Enterprise [Wright]
 - should also look through PP for places where that role should be used, otherwise it makes no sense to define it [Smithson]
 - there are many places to consider [Ohta]
- 4.5.1.1 #3 add auditor to FAU_SAR.1 [Yami]
 - {ssue is that if we specify "auditor", we are requiring an auditor role to be implemented in every device}
 - suggestion: put auditor outside of the selection, then the auditor always has access and the mfr can decide if to give others access [Wright]
 - CC doesn't specify hierarchy in FAU_SAR area [Cybuck]
 - best way is to have "auditor and [assignment: other roles]" [Ohta]
 - we should add selection around assignment to allow "no one" [Chen]
 - assignment can specify null set [Ohta]
 - OK [Wright]
- 4.5.1.2 add appendix with list of crypto standards etc [Yami]
 - we decided this elsewhere [Wright]
 - it won't be referenced in the PP because the PP stands alone without the P2600 annexes [Smithson]
- 4.5.1.3 2689-90 need more elaboration [Yami]
 - this is the CC predefined text [Ohta]
 - could have a PP application note about it
 - needed also in Enterprise PP
- 4.7.2.5 p147 other SFRs for crypto keys needed [Yami]
 - key management and key destruction are not included because not all devices have capability to generate and destroy keys [Ohta]
 - it is important to generate and destroy keys, but if we have this requirement for all TOEs then all HCDs must have capability of those functions
 - more likely many HCDs have their keys generated in development process and use them until end of life
 - for HS environment, static keys are not secure enough, they do need to generate and destroy keys [Chen]
 - to meet some standards, they may have software-generated keys or special hardware, but rarely will a static key suffice [Cybuck]
 - some of these are required by NIAP BRP instruction 21
 - OK to add to HS only [Wright]

- Custom and legacy is not needed? just use public [Smithson]
 - custom was used to be consistent with NIST, and NIST gave legacy as an example, we added public [Wright]
 - then it is OK to refer to custom and even legacy, but at least note that we don't deal with legacy and it is provided as just an example [Smithson]
- inconsistencies between threat tables in section 2 and section 3 [Sukert]
 - this is to be addressed by risk assessment work [Aubry]
 - also the criteria for HML in section 3 is different from the criteria used to determine applicability of threats in section 2, so we should state the criteria and make it consistent [Smithson]
- inconsistencies in wording of threat descriptions [Sukert]
 - yes, need to go through that [Wright]
- name problem T.UD.SALVAGE vs. T.UD.SALVAGE.DISK [Sukert]
 - T.UD.SALVAGE is correct [Smithson]
- 4.3.2.1 T.UD.SNIFF remove example text [Ohta]
 - Should we add something else to include ME sniffing? [Wright]
 - I don't think it's necessary [Ohta]
 - but if we're considering DAPS/NMCI, the NMCI web site talks about tempest [Cybuck]
 - we could put it in a "threats not addressed" section [Nevo]
 - Is this a threat that the device doesn't have "awareness" (per NIAP document)? [Wright]
 - T.UD.SNIFF.EM is only for sniffing network traffic. T.UD.PHY.EM is for sniffing the device that would be protected by tempest or Faraday cages [Nevo]
 - sniffing network ME isn't just on the cable, it could also be 802.11 [Nevo]
 - "interfaces" refers to more than just network, it also includes USB, 1394, etc [Smithson]
 - we shouldn't require encryption of local interfaces [Aubry]
 - I think we consider Bluetooth as a local interface [Smithson]
 - threat description in 2.5 is incorrect [Nevo]
 - T.UD.PHY.EM is not given a detailed description in section 2 [Smithson]
 - break into two threats in PP, .SNIFF.EM and .SNIFF.NET [Wright]
- 4.3.2.3 remove "during" [Ohta]
 - Is there no threat during the attack? [Masui]
 - there is no way to countermeasure during the attack [Ohta]
 - Shouldn't you be able to copy even if the network is being attacked? [Wright]
 - O.RESILIENT also protected assets and other interfaces/functions during an attack on one interface/function [Smithson]
 - requires a good multitasking OS [Cybuck]
 - or separate processor [Wright]

- if we address "during" it should be a separate threat [Ohta]
 - O.RESILIENT has several objectives with different importance: protecting assets during is more important than protecting availability of other functions [Smithson]
- How do you know that a DOS has occurred? [Cybuck]
 - you don't need to do something active to protect assets during a DOS, you just need to protect assets always [Smithson]
 - Is it a security-related event that needs to be logged? [Wright]
 - Yes [?]
- so the "during" threats are against availability of other functions and confidentiality of assets [Ohta]
 - that implies that you need to detect a DOS [Del Re]
 - no, it could be architecturally separate functions [Wright]
- NIAP document requires "partial_self_protection", separate domain for TSF execution [Aubry]
- DOS attacks in HS are not so likely [Ohta]
- agreed to remove "during" threats and modify O.RESILIENT [Wright]
- 4.3.2.3 add "flood" into description [Ohta]
- 4.3.2.3 remove FAX entirely [Ohta]
 - only HOOK was high risk, and its recovery is a natural function [Ohta]
 - Which risk assessment? [Wright]
 - the threat analysis worksheet, need to defer until discussion of that [Ohta]
- 4.3.2.4 add SB springboard [Ohta]
 - we had the phone-to-network vulnerability before [Wright]
 - sending data from FAX modem to remote system
 - bridging phone to network
 - could be included in T.EA.PROXY with a different description therein [Ohta]
 - resolved [Ohta]
 - SB -> T.EA.PROXY
 - T.EA.PROXY and T.EA.DOS -> T.EA.DOS
 - accessing documents through phone line or maintenance port is already in T.UD.ACC.HACK
- 4.3.2.5 remove redundant text in T.TSF.CRED [Ohta]
 - with some changes
- 4.3.2.5 better text for T.TSF.AUD [Ohta]
- 4.7.1.1 add X for O.I&A at T,TSF,SW and provide justification later [Ohta]
- Inconsistency of definition of T.UD.IMP.* in sec 2 and PP, and also countermeasures (I&A? or configuration and well managed network?) [Ohta]

- three threats in section 2 [Wright]
 - FAX
 - PRT
 - SCAN
- Impersonating TOE interface means what? [Ohta]
 - refers to, for example, stealing the address of the TOE and having a print job printed on a different device, maybe out of scope [Smithson]
 - should be a network management issue [Aubry]
- could change IMP to MIM [Chen]
- sec 2 says alter, PP says access and/or alter [Wright]
 - I think PP was correct [Smithson]
 - but access without altering is a SNIFF [Wright]
 - then there is another, DOS: [Smithson]
 - t.ud.sniff -- access
 - t.ud.alter -- alter
 - t.ud.dos -- delete or not forward
- How about IMP meaning alter or delete? [Wright]
- resolved [Wright]
 - Change T.UD.IMP.* to T.UD.ALTER.*
 - change throughout document
 - ALTER is to include deletion or failure to forward
 - this may be a problem that needs a different threat, let's see how it goes [Smithson]

Distinguishing Enterprise vs. High Security PP [Nevo]

- In table 1
 - value of assets H+ vs. H, not big difference
 - physical security doesn't help much
 - network protections similar
 - legislative mandates: none in HS, H in enterprise
 - HS example of pharma lab would have CFR 21 (?) along with possibly HIPAA and SOX [Smithson]
- another difference is that security takes precedence over usability [Cybuck]
- propose that Enterprise have value of asset = M [Nevo]
 - Example of enterprise? [Wright]
 - companies like Sharp, Ricoh, Lexmark [Nevo]
 - may have some HS environments for such things as HR data
 - islands of HS within enterprise [Wright]
 - this is consistent with the NIST descriptions [Cybuck]
- What about legislative mandates? [Smithson]
 - they would be in the HS island [Nevo]

- so a company like Ricoh would have most of its operation in Enterprise level, but finance, HR, R&D labs, and some other functions would be HS islands [Smithson]
- would be good to have definitions for H/M/L value assets [Smithson]
- need to change examples [Nevo]
 - HS
 - pharma
 - military research lab
 - financial/stock broker
 - social security office
 - Enterprise
 - cable TV company
 - large ad agency
 - big box retailer
 - SOHO
 - As current
 - Public
 - As current

Threat analysis [Smithson]

- {Smithson described process}
 - Took threat list from section 2
 - Group (Nevo, Aubry, Smithson, Haapanen) individually assigned numbers (high/medium/low) for each environment:
 - Likelihood of threat
 - Impact of threat
 - Tried to do cost, but this didn't work out as well
 - Likelihood multiplied by impact equals risk
 - Very subjective because we don't know the specifics of the target environment like you would in a specific business impact analysis
- What is the range of these numbers? [Wright]
 - 1-3 for likelihood and impact, 1-9 for risk [Haapanen]
- What is the color coding? [Wright]
 - Above 3 is yellow, above 4.5 is red [Haapanen]
 - Colors do not indicate which items should be in the PPs [Haapanen]
- Since we redefined Enterprise, we have possibly invalidated the results [Smithson]
- The idea was to compare these results with Jerry's H/M/L assessments in Section 3 and the big table in Section 2, and also to look at whether there were widely varying results between individuals in the group [Smithson]
- We should re-do this with the new definition of Enterprise and perhaps open it up to a larger group. I have another sheet that can be used optionally that calculates values for each threat based on other factors:

- Impact: duration of attack, persistence of outcome, scope of impact, importance of asset, stealthiness of attack, discontinuity caused, discredit caused
- Likelihood: means, opportunity, motive
- One problem with this assessment was that these factors probably should have been unequally weighted
- What are we going to do with these results?
 - Looking at risk alone, you might include one versus the other, but cost of mitigation should be considered also [Smithson]
- Are we going to have a section in the PP that says “the following threats are not addressed because of low impact / low likelihood”? [Wright]
 - We could, based on that NIAP document [Smithson]
- What if one is 4.99, another is 5.00, and another is 5.01, and you’ve drawn the line at 5.00?
 - The line can be moved, maybe based on clustering. [Smithson]
- T.UD.SNIFF.EM has a high rating, but it only takes a WiFi setup to sniff EM
 - We had assumed that EM only meant sniffing the outside of a network cable [Smithson]
- One thing I did was to extend the columns and filled them with the Section 3 H/M/L and Section 2 R/P/G/N/X/etc and then looked for anomalies:
 - Not applicable in Section 2, but not Low Risk in our analysis (found two of those, in Enterprise)
 - Looked for Low in Section 2 and High in our analysis, or High in Section 2 and Low in our analysis (three in Ent, seven in SOHO, four in Public)
 - Also looked at threats that were off by one level between Section 2 and our analysis (there were many of them)
- FIPS-199 contains useful definitions [Cybuck]
- also consider calculating based on detailed threat and environment definitions [Smithson]
- for high skill level requirement, we can't consider unless EAL4 [Ohta]
 - EAL6-7 high attacker
 - EAL5 medium attacker
 - EAL 2-4 low attacker
 - EAL1 ---
- Plans [Wright]
 - Develop more detail directions and guidelines for performing the assessment {Smithson, with help from Aubry}
 - Re-run the assessment with the new information from this meeting and the guidelines {Haapanen}
 - Involve more people in doing the assessments
 - just this meeting's attendees [Smithson]

- Look at the results and propose which threats should be removed or added to PPs.
- Smithson to provide a timeline for definitions and directions, input, and results
- It is needed before Enterprise PP can continue [Nevo]
 - It would be best to continue as much as you can without [Smithson]

Closing [Wright]

- We did not go through High Security or Enterprise at all, so we should not move Enterprise into the “managed” column
- Wait until Don publishes comments from this meeting
- Then Ohta-san to modify draft
- Smithson to act as check-in/check-out person for PPs
- Comments Excel database will be published as a guide for what needs to be done in each section

See you in Cupertino in July, 2005.

**** Adjourned at 2:00 PM, 5/20/2005 ****