

**IEEE P2600 Meeting #10**  
**April 12-13, 2005**  
**Epson, Tokyo, Japan**

**Attendees**

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

Tom Haapanen, Equitrac  
Kazutaka Higo, Fuji-Xerox  
Takanori Masui, Fuji-Xerox  
Kenji Tsutsumi, Fuji-Xerox  
Harry Lewis, IBM  
Shigeki Kimura, Kyocera-Mita  
Jerry Thrasher, Lexmark  
Carmen Aubry, Océ  
Masahiro Suzuki, Oki Data  
Satoshi Fujitani, Ricoh  
Hiroshi Hosaka, Ricoh  
Yusuke Ohta, Ricoh  
Fusayuki Fujitani, Sharp  
Ron Nevo, Sharp  
Yamanaka Toshihiro, 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.

**\* Commenced at 9:15 AM 4/12/2005 \***

**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-Apr2005.ppt>

## ***Minutes and Agenda approvals***

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

## ***IEEE patent policy***

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Apr2005.ppt>

*Note that the IEEE Patent Policy was revised in March, 2005, after the most recent P2600 meeting. No response to question about patent disclosures.*

## ***Inappropriate topics review***

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Apr2005.ppt>

## ***Officers***

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary / Lead Editor: Brian Smithson, Ricoh.

Editors: Jerry Thrasher, Lexmark; Ron Bergman, Ricoh; Ron Nevo, Sharp.

## ***Meeting schedule update***

**May**'s meeting is confirmed for May 19-20 in Toronto, sponsored by Equitrac. Location and other information is posted on the web site at <http://grouper.ieee.org/groups/2600/meetings.html>.

*Note that the meeting will be held at a hotel, not at Equitrac's facility, and consequently there is a meeting fee of approximately US\$35 per day per attendee (cash only) to cover the morning Continental and afternoon snack.*

**July** 11-12 SFO/San Jose (most likely Cupertino) - w/PWG - at Apple

**Sep** 15-16 West Caldwell, New Jersey, at Ricoh

**Oct** 24-25 New Orleans - w/PWG

**Dec** 13-14 San Diego - considering HP site

The most up to date schedule for meetings in 2005 is listed on the slides <http://grouper.ieee.org/groups/2600/presentations/P2600-Apr2005.ppt>

### ***TCG update [Wright]***

- Brian Volkoff did not attend this P2600 meeting because of an impending blessed event.
- The most recent TCG meeting was March 29-31 in San Diego
- The Hardcopy Working Group met on March 30
- Ricoh has joined as a member of TCG
- The focus of the HCWG was use cases
  - Also discussed, for the benefit of new members and visitors, was the charter and scope [Smithson]
- P2600 has a liaison relationship with TCG
  - TCG President announced it at the member's meeting
  - It is not yet clear at what point TCG use cases can be distributed to the P2600 group
- What kind of use cases were discussed? [Masui]
  - High level use cases [Wright]
    - scanning to printer
    - scanning to server
    - scanning to storage device
    - print from client
    - print from server
    - print from internal storage
    - print from external storage
    - device management, local
    - device management, remote
  - purpose of TCG is to establish trust relationship
    - does not include copying, because you trust yourself
    - kinds of use cases are between devices
    - is the server trustworthy?
    - is there uncontrolled access to a storage device?
    - when you plug a USB flash drive into a printer, can the printer read all of the files?
    - those are examples

### ***Discussion of Protection Profile Registration [Wright]***

- This discussion arose from Masui's email to the group
- We talked about this early in the P2600 process and decided then to wait until later to discuss
- Options are
  1. get CC certification using the usual process (profile certification is less expensive than full device certification)
  2. register it under some registration scheme as per ISO 15292:2001
  3. neither certify nor register
- David Freas (of DAPS) called regarding PP registration

- DAPS is a civilian agency that does printing services for the US government
- Freas thinks it is possible to get NIAP to certify, at least for High Security and Enterprise environments, based on US military / Department of Defense needs
- Will Enterprise work for DOD? [Aubry]
  - Yes, for things like recruiting offices [Wright]
- NIAP is Common Criteria? [Haapanen]
  - NIAP is the agency that issues certifications in the US, including those for PPs [Wright]
- Would it still make sense to register all profiles with ISO? [Haapanen]
  - I don't know. It makes the PP known to people [Wright]
  - It "publishes" it, in a sense [Smithson]
  - Registration is how to inform users of its existence, but if the PP is not certified, then each vendor would need to have the PP evaluated with their ST and product certification [Ohta]
  - For SOHO and Public, the vendor could claim compliance with the registered {but not certified} PP [Haapanen]
    - Who would test that claim? [Ohta]
    - The customer would need to trust the vendor [Haapanen]
- I suggest we try to make progress on using DAPS for the HS and Ent PPs, then consider later what to do with SOHO and Public [Wright]
  - As a minimum, we should register [Nevo]
  - Depends on cost and process [Wright]
  - I don't think it is possible to register without certifying [Ohta]
    - I saw that it was possible [Masui]
    - I will look into that [Wright]
- Freas will try to attend the Toronto meeting, and will definitely come to the New Jersey Meeting [Wright]
  - Has he read our PPs? [Ohta]
  - He said he has gone through our documents, thinks they are good, and does not want to duplicate effort [Wright]

### ***Action items from previous meeting [Wright]***

Refer to slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Apr2005.ppt>

See slides for completed items

### **Sec 1**

- Open, awaiting input from others

## Sec 2

- Cross-check with original vuln list
  - Not done, some items need to be reviewed [Haapanen]
- Sec 4 team to determine which threats apply to which environments
  - Was tentative, still tentative [Smithson]
- Decide whether to include environments in the full standard
  - Still open

## Sec 3

- Missing sections
  - Some threats still don't have specific recommendations [Thrasher]
- Move asset section to Sec 1
  - Remains open
- Align with sec 2 threats and make recommendations
  - Is aligned, but {as above} some recommendations are not complete [Thrasher]

## Sec 4

- HS
  - Updates done [Nevo]
  - Need to do some more work on rationale [Ohta]
- Enterprise
  - 2<sup>nd</sup> draft [Nevo]
- SOHO
  - 1<sup>st</sup> draft [Aubry]
- Public
  - No work on this yet [Aubry]

## Discussion about Security Environments [Nevo]

- based on security level of assets as we have today
  - enterprise should also include corporate examples with different infrastructures
  - complex/centralized
  - simple corporate
  - these have similar security requirements
- would be easy to add another example [Wright]
  - needs to have an example of smaller corporate than "enterprise" [Nevo]
- what characterizes corporate is there is no regulation, only due care / due diligence [Aubry]
  - what distinguishes is network management and level of effort required to fulfill higher security requirements
  - we should not put too high of a requirement on everyone
- production environment is under Enterprise [Lewis]

- the examples in enterprise are mostly or all regulated by HIPAA, GLBA, etc [Smithson]
  - still is not a requirement for impenetrability, just due diligence/care [Wright]
- NIST recommendations suggest high security for health records [Aubry]
  - difference is between data in transit and data that is stored [Wright]
- definitions have a large gap between Enterprise and SOHO [Aubry]
  - enterprise is "complex centrally managed" and yet example of enterprise is local DA office
- need another diagram in enterprise that shows a simpler environment [Nevo]
  - one action item is to add explanatory text to guide use asset value and not the name or topology [Wright]
  - we can't dictate how people use their networks or devices, they can disable encryption features if they want [Haapanen]
    - then they will not get the benefit that the certified level represents, even though they pay for it [Aubry]
  - customers will likely have a mix of requirements, like HS and Ent [Smithson]
    - may even buy all HS devices and then by policy downgrade some to Ent level, it may be more economical to buy or manage that way
- SOHO environment may have requirements that prove to be expensive [Aubry]
  - in HS and Ent you have trained IT staff, network boundary, monitoring
  - in SOHO you don't have those things
- depends on the vendor or customer whether they use SOHO PP or not [Ohta]
  - some customers want to buy product with security functions and want the certification
  - in that case SOHO PP can be used
  - I don't know if it will be acceptable to customers, but at this moment we should continue to work on SOHO and not decide now to remove it
  - I am not proposing to remove it [Aubry]
- our customers must decide, no security expert can decide [Suzuki]
- conclusions? [Wright]
  - I think we identified a gap between Enterprise and SOHO and perhaps a problem of some examples in Enterprise that may be better served by HS [Smithson]
  - how about a flow chart or decision tree? [Thrasher]
    - there is a table in 1.4 that is supposed to fulfill this [Nevo]

- we should add examples of corporate environments [Ohta]
- HS and Ent are too similar? [Wright]
  - yes, SFRs look the same; also the threats list is almost identical [Nevo]
  - Ent should have lowered objectives [Ohta]
  - four PPs is OK, but we need a smaller gap between Ent and SOHO and larger distinction between HS and Ent [Aubry]
- public environment is not started because there are not as many threats and assets are more specific, it should be easier to create than other PPs [Ohta]

## Section 1. Introductory Pages [Wright]

Refer to <http://grouper.ieee.org/groups/2600/drafts/June2004-Plan/P2600Intro-V08.doc>

- SOHO drawing (no comments)
- Enterprise drawing
  - what about remote maintenance over phone lines? [Masui]
    - are there proprietary protocols for this connection?
      - Yes [Masui]
    - need to add a threat for that [Ohta]
    - government won't let you plug in a FAX phone line [Nevo]
    - is in a HS env? [Wright]
      - yes [Masui]
    - will add to diagram [Wright]
- HS drawing
  - will add maintenance phone line here also
- Public (no comments)

{see review draft slide for actions}

## Section 2. Vulnerabilities/Threats/Exploits [Haapanen]

Refer to <http://grouper.ieee.org/groups/2600/drafts/Section2/Section%20%20-%20threat%20details%20-%202005-03-31.doc>

- made changes from Plantation meeting, those requiring comment are listed here
- clarified that FAX means PSTN faxing using ITU standards, not Internet faxing using IETF
- t.tsf.cred.guess
  - should be Xs for HS and Ent [Wright]
- started adding vector definitions, haven't finished yet
- t.dos.net.flood
  - long description includes an objective [Smithson]

- should say that the threat is of a flood attack resulting in a sustained or persistent failure [Smithson]
- sec 4 team should verify threat descriptions against latest section 2 list
- where is social engineering? [Wright]
  - nothing we can do in the equipment to prevent that [Thrasher]
- possible missing threats
  - lack of multiple roles
    - is this a design deficiency? [Wright]
    - covered under t.tsf.conf [Smithson]
  - unlocked operator panel
    - means that normal person can do something they're not supposed to do, would be mitigated by autologout [Wright]
    - should not specify something so detailed; authentication might be done by proximity implant or something that automatically goes away when the person leaves [Smithson]
      - we did some consideration of likelihood and impact, but it seemed to be too site specific [Wright]
    - was a risk analysis done to consider the likelihood and impact to see what threats should be considered? [Aubry]
    - in threat list, those marked with "R" are handled by resiliency which can be verified [Ohta]
    - we tried to get at likelihood by looking at expertise and equipment required, but asset value or business impact was a problem for us because we are not a specific end customer [Smithson]
    - the threats are already described in section 2 [Aubry]
      - but this threat is not described in T.TSF CRED in the PP [Ohta]
      - but we cannot describe all possible vulnerabilities [Aubry]
      - it is marked for further looking at [Wright]
  - SNMP issues
    - is covered in sniff threats? [Aubry]
    - put in best practices [Wright]
  - best practices for manufacturers {as the result of discussion}
    - unalterable SNMP community name
    - inappropriate config and setup
    - using non-essential services, telnet, ftp, unblocked ports
    - virus infection vulnerabilities

- inappropriate printing/copying (money, etc)
- already covered {as the result of discussion}
  - getting DHCP, WINS, SMTP, etc addresses
  - unauth access to unprotected management interface
  - taking offline
  - compromised user ID/pin to release a job
  - unnecessary services
  - unauth watermark, signature, stamp
  - unauth endorser for signature/stamp
  - unauth repl/mod of job ticket (t.ud.imp.\*)
- DHCP, BOOTP impersonation
  - is on by default in many devices [Thrasher]
  - can't do much about it
- fraudulent print job appears to be something it isn't
  - out of scope -- social engineering
- Bates stamp alteration
  - t.tsf.conf.dev
- disable money printing protection
  - t.tsf.conf.dev

### Section 3. Directives/Best Practices [Thrasher]

Refer to <http://grouper.ieee.org/groups/2600/drafts/Section3/Section3-Draft0.008.doc>

- threat/mitigation cross reference by user environment
- requires a threat per environment table
- made a first cut of that
- probable, possible, improbable
  - terms are about risk [Smithson]
  - more standard term to use is low, medium, high [Aubry]
    - are there standards for those terms? [Wright]
    - yes, NIST document 800-30 for definitions [Aubry]
- is a good approach?
  - may need to include a statement that we are not giving specific advice, but are treating threats as though they have these likelihoods, please examine for yourself [Smithson]
- document organization / tables
  - put H/M/L risk by environment in section 2 [Smithson]
  - put Best Practice mitigations, etc, AND pointer to PP if available, in section 3 [Smithson]
  - add to detail threats: HML table or line per environment AND pointer to section 3 mitigation techniques [Wright]
  - in section 3, unspecific pointer to each PP that applies (if any)
- everyone reads section 3 for Toronto! [Wright]

## Section 4. Protection Profiles

### *High Security*

Refer to [http://grouper.ieee.org/groups/2600/drafts/Section4/HSD\\_Protection\\_Profile-High\\_Security\\_Environment-v192.doc](http://grouper.ieee.org/groups/2600/drafts/Section4/HSD_Protection_Profile-High_Security_Environment-v192.doc)

- fix visio diagrams – they have a printing problem [Wright]
- 3.2.3 intro could should be reworded : "after attack, may not work, for example ..." [Wright]
- t.dos.prt.prt talks about document volume, how to quantify? [Aubry]
  - volume was removed from sec 2 list [Smithson]
  - volume still appears in t.dos.fax [Wright]
- need to align sec 4 with sec 2 threats [Wright]
- are all subthreats listed in sec 4? [Wright]
  - idea was to have the higher level description represent all subthreats in the description [Smithson]
  - why not then list as separate threats? [Wright]
  - because later parts of the document expand per threat. this only works if the grouped threats can be met by the same objectives, requirements, etc [Smithson]
  - only if the risk is low can you eliminate one of the subthreats from the description [Aubry]
- priority is different from DOS attack, from a testing standpoint, it is not well met by resilience [Ohta]
- where to draw the line, just H or H&M? [Smithson]
  - depends on how the analysis turns out and how much you want to spend [Aubry]
    - if you have only 20 H and 30M, you might draw the line at H
    - if you have 2H and 18M and 30L, you might draw the line at H+M
    - also depends on how much you can afford
  - in HS env, the printer may have low value relative to data, so DOS is not such a big deal but UD is [Nevo]
- Chapter 1-4 changes [Nevo]
  - should change 2.3.11 and 2.3.12 to represent subsystems and be consistent with section 1 (physical embodiment of electronic etc.) [Wright]
  - other PPs have policy assumptions about good network management and security practices [Aubry]
    - is possible to have policy assumption, but is needed? if we have such assumption, what good does it do? [Ohta]
    - helps in cases like rogue DNS server or making the firewall assumption effective [Aubry]
    - is there some sample text we can use, and is there a downside of having such an assumption? [Smithson]

- what about SOHO or Corporate? [Ohta]
  - for SOHO, you can't assume the same things, it depends on environment [Aubry]
- concerned about inconsistency between HS and Ent PP [Ohta]
  - need to continue this offline with a specific proposal [Wright]
- {OK} to delete belt and drum from 4.1.3. and 4.1.4 [Ohta]
- {OK} to remove OE.GENUINE in favor of self test [Ohta]

## ***Enterprise [Nevo]***

Refer to [http://grouper.ieee.org/groups/2600/drafts/Section4/HSD\\_Protection\\_Profile-Enterprise\\_Environment-v191.doc](http://grouper.ieee.org/groups/2600/drafts/Section4/HSD_Protection_Profile-Enterprise_Environment-v191.doc)

- chapters 1, 2 are (and should remain?) the same in PPs
  - possible difference is the actors
  - in SOHO for example the network and device administrator would likely also be a or the user
  - may be OK to continue to list the roles separately
- A.LOCATION, are outsiders more likely in Enterprise?
  - they are at least authorized visitors
  - saying "do not exist" is too absolute, better to say that the risk is minimal
- A.NETWORK
  - should include antivirus as an assumption?
  - there will be a security functional requirement, which applies also to HS [Ohta]
  - we talked about having an assumption for network management, wouldn't that cover it? [Thrasher]
  - is the objective for the TOE or for the environment? [Aubry]
  - environment [Ohta]
  - do we need to add anything to A.NETWORK? [Wright]
    - it should be OK as is, especially since A.NETWORK is about limiting access and not about things like antivirus. those will be handled in a new SFR [Smithson]
  - should we have more or different description of the firewall for HS to differentiate it from Enterprise?
    - I think it is better to make a generic statement that refers to what is appropriate to the environment and then use that text in all PPs [Smithson]
  - second bullet is not in HS [Ohta]
    - it is implied by the first one [Aubry]
    - removed [Wright]
- T.UD.IMP / SNIFF
  - should be removed from Ent?
  - I can see IMP, but SNIFF? [Ohta]

- sniffing is not so easy in corporate environment, it can be detected in a managed network [Aubry]
- even on a switched network, you can slip a laptop and hub under an MFP and sniff [Haapanen]
- but asset value is the issue, if the asset value is high enough then the HS environment should be used [Aubry]
- sniffing is a good mechanism for breaking the I&A mechanism [Ohta]
  - UD.SNIFF could go, but TSF.CRED.SNIFF should stay [Aubry]
- but encryption is cheap, and looking forward, even cheaper [Haapanen]
  - management and key infrastructure is costly [Aubry]
- agreed to remove sniff and imp for Uds [Wright]
- can we document our rationale for the decision? [Farrell]
  - it is in section 1 of P2600 [Nevo]
  - decision is that in the enterprise env, the value of a single asset is does not justify sniffing, but multiple assets justifies sniffing credentials [Wright]
- T.DOS
  - is the value of a DOS attack sufficient to make it worth doing in an Ent environment? [Wright]
  - not NET.CONNECT
  - what about the PRT attacks?
- T.RESOURCE vs T.RESOURCE.PEER
  - is different between HS and Ent? [Masui]
  - should be same, HS version will apply to Ent [Nevo]
- sniffing vs salvage
  - if it is not worth sniffing, isn't it also not worth salvaging? [Thrasher]
  - sniffing is for one document, salvaging is for multiple documents [Wright]
  - sniffing can be for multiple documents [?]
  - salvage gets copied and scan-to-fax documents [Wright]
  - MFPs are often leased, then returned [Nevo]
  - agreed to leave as an issue [Wright]
- O.I&A
  - is necessary for Enterprise? [Wright]
  - many companies use, for accounting if nothing else
  - it is OK to turn off the feature [Wright]
    - in that case they are not running in the certified configuration [Ohta]
  - administrator can decide what mechanism or policy to use [Ohta]
  - could put something in best practices about recommending manufacturers to provide granularity [Wright]

- can also allow anonymous IDs [Ohta]
- by limiting access, haven't we authorized a user to use the device? [Thrasher]
  - they may be authorized, but not identified and authorized at the device [Wright]
- O.MONITOR
  - security logging is common through the enterprise now, and to claim security without having logs would be lame [Lewis]
- O.FILTER
  - merge objective into O.NETWORK [Nevo]
- OIE.GENUINE removed, O.GENUINE remains, supported by self test SFR [Ohta]
- still need to update chapters 5-7 for the Enterprise objectives [Ohta]
- question about 6.3 [Aubry]
  - in some cases, I&A may be achieved using local mechanisms OR by IT environment, which may be a problem for PP evaluators [Ohta]
  - needs comment from NIAP via Cybuck [Smithson]

## **SOHO**

Refer to [http://grouper.ieee.org/groups/2600/drafts/Section4/HSD\\_Protection\\_Profile-SOHO\\_v3.0.doc](http://grouper.ieee.org/groups/2600/drafts/Section4/HSD_Protection_Profile-SOHO_v3.0.doc)

- Not reviewed at this session. Will be updated. [Wright]

## **Public**

- Not available for review.

## **P2600 in general [Wright]**

- New management processes:
  - Proposed changes **MUST** be emailed to the reflector at least one week before the meeting
  - This applies now to Sections 1-3 and to the High Security PP of Section 4
  - New sections will be added as they mature
- Merged P2600 document
  - Want to have a merged document of Sections 1-3 plus the HS PP for review in Toronto
  - Target for first draft of the merged document: first week of May [Smithson]

## **Action item review [Wright]**

Refer to meeting slides for list of action items for and before the February meeting: <http://grouper.ieee.org/groups/2600/presentations/P2600-Apr2005.ppt>

- Risk assessment (H/M/L) by threat in each environment
  - (Smithson, Ohta, Nevo, Aubry, Haapanen made a plan after the meeting)
- Merged document
  - First draft in first week of May [Smithson]
  - Draft including Sections 1-3 plus HS PP to be reviewed in Toronto
- Administrative:
  - Don Wright to continue conversation with David Freas regarding help from DAPS regarding the PPs
  - Don Wright to clarify TCG/P2600 liaison relationship to see what/when TCG documents can be distributed to P2600 non-TCG members
- Section 1:
  - Better corporate enterprise example to be added
  - Section 1.4.1.1 consider decision chart for selecting environment
  - Add text indicating the drawings are examples/concept charts. Not all components will be present in all implementations.
  - Telephone line connections to MFP/HC devices for remote maintenance, etc. in enterprise environment as well as in high security environment.
- Section 2:
  - Updates as per meeting
  - Threat 10.05.04 – unlocked operator panel
  - None of the other highlighted brain storm threats need to be addressed.
- Section 3,:
  - Updates as per meeting
  - Some threats still need specific recommendations
  - Change to High/Medium/Low risk
  - Everyone to detailed review of revised section 3 for Toronto meeting. There will be a test!
- Section 4:
  - High Security
    - Updates as per meeting

- Which threats to include? Should be an outcome of the risk assessment (hi/med/low). Who?
- Discussion item on assumptions about the network environment.
- Enterprise
  - Updates as per meeting
- SOHO
  - Not reviewed
- Public
  - What is the schedule for first draft?

See you in Toronto in May 2005.

***\* Adjourned at 12:30PM, 4/13/2005 \****