

**IEEE P2600 Meeting #9  
February 23-24, 2005  
Equitrac, Plantation, FL**

**Attendees**

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

Nancy Chen, Okidata  
Satoshi Fujitani, Ricoh (24th only)  
Tom Haapanen, Equitrac  
Harry Lewis, IBM  
Jean-Claude Longo, Océ  
Ron Nevo, Sharp  
Yusuke Ohta, Ricoh  
Alan Sukert, Xerox  
Sam Takeuchi, Konica-Minolta  
Jerry Thrasher, Lexmark  
Brian Volkoff, HP  
Bill Wagner, rugged individual  
Sameer Yami, Toshiba America Business Solutions

In the following sections, names of speakers are indicated by [square brackets]. The primary speaker for a session is noted at the beginning of the session as a default; others are noted in place.

**\* Commenced at 9:05 AM 2/23/2005 \***

**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-Feb2005.ppt>

***Minutes and Agenda approvals***

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

### ***IEEE patent policy***

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Feb2005.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-Feb2005.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***

**April's** meeting is confirmed for April 12-13 at Epson's facility in Shinjuku-ku, Tokyo, Japan. The P2600 meeting will be preceded by PWG meetings. Location information is posted on the web site at <http://grouper.ieee.org/groups/2600/meetings.html>.

**May** 18-19 Toronto - at Equitrac

- There is a conflict with AIM Show May 17-19, Philadelphia [Nevo]
- Propose move to May 19-20; Approved

**July** 14-15 SFO/San Jose (most likely Cupertino) - w/PWG - at Apple

- Propose move to July 11-12; No objections

**Sep** 14-15 New Jersey - at Ricoh? Otherwise IEEE

- Print 2005 is Sep 9-15 [Wagner]
- Could move to Sep 15-16
- Brian Smithson to confirm before next meeting, will take into consideration a move to Sep 15-16 [Smithson]

**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-Feb2005.ppt>

### ***TCG update [Volkoff]***

- Next general meeting of the TCG is 3/29 – 4/1 in San Diego.

- Negotiating with the board to be able to operate the working groups in a more open fashion
- Each group would decide if it wanted to operate in that way.
- That would let us share documents and take comments from outside the hardcopy device working group [Wright]

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

Refer to slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Feb2005.ppt>

See slides for completed items

#### **Sec 1**

- Bibliography from all sections
- Terms from all sections
- Refer to mitigation techniques from sec 3 rather than NIST
- Define assets from sec 3
- Add acronyms from sec 2/4 (maybe 3)
- Add explanatory text based on asset value and not just nature of environment

#### **Sec 2**

- Cross-check with original vuln list, need to reconcile with new list resulting from sec 2 and 4 reconciliation
- Sec 4 team to determine which threats apply to which environments

#### **Sec 3**

- Missing sections partially done; have been outlined
- Align with sec 2 threats and make recommendations

#### **Sec 4**

- OK

### **Section 1. Introductory Pages [Wright]**

Refer to <http://grouper.ieee.org/groups/2600/drafts/June2004-Plan/P2600Intro-V07.doc>

#### **SOHO**

- SOHO environment as defined doesn't have firewalls or anything like that [Thrasher]
  - Should assume basic firewall [Nevo]
  - Where does it say no firewall? [Wright]
    - Below figure 1 [Thrasher]

- Could change to "there may be no network-based security" (or those security devices that are present are out of date) [Wright]
- We should recommend use of firewall in SOHO env [Ohta]
- What happens if we don't assume that there's a firewall? what could we do differently (in the device)? [Wright]
- Someone looking at P2600 would likely be interested enough to include a firewall [Thrasher]
- (comment not intelligible due to noise) [Longo]
  - You might find SOHO-like environments with enterprise reqts [Volkoff]
  - Last time we decided to put some text in the spec regarding SOHO with higher security reqts [Thrasher]
- In SOHO the device may also be connected to a FAX phone line [Cybuck]
  - Does anyone really have a modem line that bridges the network or accesses FLASH? [Volkoff]
  - It's a fear without much basis. Some devices have modem connections for diagnostic access to the device. [Cybuck]
- IPV6 is coming into play now also [Volkoff]
  - Firewalls aren't going to work in that case
  - IPSEC would be expected to secure all sessions

### ***Enterprise***

- Need an icon for big MFP
- Should there be a PSTN connection shown on the figure? Also should show web servers etc in DMZ? [Wagner]
- Should print servers be shown [Lewis]
  - Trying to keep it general, otherwise too complex
  - To show examples for someone who is trying to design a network with print spoolers or servers [Lewis]
  - Hierarchical relationship between spoolers and printers should be represented [Volkoff]
  - Added
- Should show external users with VPN [Nevo]
  - Added
- What about authentication servers? [Nevo]
  - We get to that in HS environment
- Mitigations need to be aligned with section 3

### ***High Security***

- Will add our changes from Enterprise into this section/diagram also
- Mitigations to be aligned with section 3

### ***Custom/Public***

- Tried to show some back-end systems separated from public
  - Does the internal/external systems really loop through the ISP? [Smithson]
  - Tried different ways of showing this and it didn't work too well
- Should show some server(s) in public area [Cybuck]
  - Added
- Also FAX line to PSTN [Cybuck]
  - Added
- Wireless access? such as for hotels, internet cafes [Cybuck]
  - Added
- Need more words in this section. Like mitigation techniques?
  - Would like to replace mitigation parts with pointers to Sec 3
  - Sec 3 is not organized by environment [Haapanen]

### ***Custom/Legacy***

- Also need more words in this section (regarding recommendations)

### ***Other issues***

- Concerned about environments, SOHO doesn't account for high value assets [Haapnen]
  - When we discuss assets, we'll recommend people use different environment in high value or regulated assets [Thrasher]

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

Refer to <http://grouper.ieee.org/groups/2600/drafts/June2004-Plan/Section%20%20-%20threat%20details%20-%202005-02-23.doc>

- Table columns indicate PP coverage what about whether they apply (vis a vis section 3) to the environment at all? [Thrasher]
  - That's what code "G" is for [Wright]
- IETF Fax removed
  - There's an RFC now so we may see more support [Wagner]
  - Could get a negotiation/handshake DOS attack [Thrasher]
  - Put in T.DOS.NET.CONNECT? or T.DOS.NET.CRAFT? [Wright]
  - Not packets, but malformed protocol [Haapanen]
- What happened to T.DOS.IMP? [Thrasher]
  - Rolled into T.UD.IMP along with other threats like T.DOS.SNIFF.IMP [Smithson]
- T.UD.IMP.FAX
  - How to handle in PP? [Wright]

- Can't do without secure fax devices, shouldn't mandate in PP [Smithson]
- What about IETF fax? could use encryption there [Wagner]
- In general, should refer to PSTN wherever we say FAX
  - Need to add some text about that [Wright]
- Should also take out PP coverage of T.UD.SNIFF.PHONE [Nevo]
- T.TSF.CRED
  - If encryption is required for network sniffing, then it will also work for EM network sniffing [Ohta]
    - This table is about requirements in each environment which may be different even if countermeasures are same [Smithson]
  - Using PostScript to access credentials? Or getting credential through audit logs [Sukert]
    - Is handled by encryption also [Wright]
- Encryption for Enterprise is too high of a requirement
  - Device must support, not necessarily be used though [not sure who said]
- Vector components need to be defined [Wright]
- Does all that vector info need to be in the final document? [Wright]
- What about T.DOS.NET.CRAFT and the note about protocols? [Wright]
  - Included in the description, let Tom decide [Wright]
- Does T.RESOURCE.PEER also account for connecting to serial ports? [Sukert]
  - "local" interface includes that; also firewire, etc. [Wright]
- T.UD.ACC vs. T.UD [Wright]
  - Sec 4 has T.UD, sec 2 has T.UD.ACC [Smithson]
  - We keep it to 3 levels in the PP [Nevo]
  - What about T.DOS.PHY? PP only describes output tray protection [Wright]
  - Change name in sec 4 [Wright]
- Does T.UD.ACC.NORMAL include guessing a PIN number? [Sukert]
  - It's more of a credential thing than a document thing [Wright]
  - Adding T.TSF.CRED.GUESS [Wright]
  - Could be physical access or network [Smithson]
- Expertise ratings: "novice" should be "layman", as defined by CEM [Smithson]

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

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

- Document is now in two sections:

- Best practices
  - Threat mitigation considerations
- Asset discussion at intro still needs to be done
- Softened language
- 1.2.1 out of the box configuration
  - Wording changes needed [Wright]
  - Done
- Are "back doors" covered? [Sukert]
  - T.UD.ACC.HACK (covers user documents, not credentials) [Nevo]
  - Others covered in 1.2.x
- How about turning things off, like rlogin? [Sukert]
  - 1.2.1 number list #2 [Smithson]
- 1.3.1 reference to T.TSF.AUD.\*, why is it listed as a physical threat? [Smithson]
  - I guess it means physically/electrically altering an access control box [Smithson]
  - Needs to be reworded [Wright]
- Reference to locked output bins, what about locked document feeders? [Sukert]
- Why isn't "wiping the disk" included in 1.3.1.4? [Wagner]
  - Because 1.3.1 is about physical security [Smithson]
  - 1.3.2 describes technical techniques
- Should "removable disk" be included in 1.3.1.4? [Smithson]
  - This is about techniques, not recommendations yet
- 1.3.1.4 should only describe theft of imaging unit, and have a separate section for theft of disk
- Discussion of PINs and passwords isn't just for authentication, it's also for authorization [Sukert]
  - Yes, we address one then the other
- References to vendors and products shouldn't be used; need to be reworded to minimize the use of trademarked names [Wright]
- 1.3.2.2 PSTN Fax, we don't have a threat about non-repudiation elsewhere [Chen]
  - It's not the FAX protocols that provide non-repudiation, it's the transmission (phone records, etc) [Wagner]
- Threat mitigation
  - (various changes)
  - How about having a table that lists which environments apply? [Wright]
    - Or a table that shows likelihood of occurrence in that environment
    - Or it gets too subjective [Wright]
    - Already gave that some consideration about what to include in the PP
    - Let's think about this more [Wright]

- List updated and uploaded

## Section 4. Protection Profile

Refer to [http://grouper.ieee.org/groups/2600/drafts/Section4/HSD\\_Protection\\_Profile-High\\_Security\\_Environment-v181.doc](http://grouper.ieee.org/groups/2600/drafts/Section4/HSD_Protection_Profile-High_Security_Environment-v181.doc)

### Chapters 1-4 [Nevo]

- Added firmware as an asset
- Figure 1 - box should include interfaces [Sukert]
- 2.2.3.4 firmware paragraph should be changed to indicate access controlled update and signed image [Volkoff]
  - This isn't the place to talk about signing and access control
  - Make it a general statement to include flash, disk, etc. [Cybuck]
- Add paragraph numbering for "TOE Architectural Description" [Sukert]
- Should add descriptions of Scanner and Printer [Sukert]
- 3.1.3 A.PHS is new
  - If we don't assume external network protection, then the TOE must protect [Ohta]
  - Should say that external threat is minimized, not eliminated; the most significant threat is internal [Cybuck]
  - This paragraph should not say "the TOE will protect" because there are other protections [Ohta]
  - This assumption is about the environment in which the TOE will be deployed, not about anything the TOE will do to protect itself [Smithson]
  - Propose we use a previous language from A.ACCESS [Ohta]
  - That makes it too protected, no threat from internal [Chen]
  - Propose we say that the environment will protect the TOE from external people [Thrasher]
- Should we roll up the T.DOS threats into one?
  - Not yet, we still need to address T.DOS.PHY which would have a different objective [Smithson]
- T.EA need to change names, check descriptions, to match section 2
- Need to look at T.UD.SNIFF.PHONE; was removed from all PPs [Ohta]

### Chapter 5 [Ohta]

- Will add full description for FAU\_GEN.2
- Made terminology (such as about different categories of users) to match the previously used terminology
- Suggest that we define "other administrators" somewhere in the PP [Sukert]
  - The assignment is to be filled in by authors of an ST based on this PP [Smithson]
- (discussion / couldn't reach consensus) leave as is

- FAU\_STG.4
  - Is it to prevent events or prevent loss of event logs? [Wagner]
    - Prevent the event
  - Would be more clear to say "prohibit the execution of" [Wagner]
    - Can't change it, per CC
  - Can insert some informative text? [Wright]
    - Only to refine or narrow the scope
  - We will try to add "execution of", and see if evaluator accepts it
- FCS\_COP.1
  - Includes audit log? [Nevo]
    - Yes, that is part of management data
  - Need to specify minimum standards
    - Can be different for different industries or countries [Cybuck]
    - For a given algorithm, key sizes get larger over time to maintain strength [Smithson]
    - Some countries may not allow key sizes above certain level [Nevo]
    - Should this specify what is encrypted, disk, flash, main memory? [Nevo]
      - Should leave open because some markets may require different things, such as encryption in memory [Cybuck]
      - Is this for permanent information or includes temporary information? if temporary, how to test? may require reading the code [Nevo]
      - We have a CC certified product that encrypts in memory, so it is possible to do [Cybuck]
  - Will leave as is
- FDP
  - What about volatile storage? [not sure who said]
  - Need to exclude volatile storage
  - Added into FDP\_RIP.1
- FPT
  - Removed FPT\_RCV.2 because it requires explicit action
  - Instead, put in assurance testing requirement FPT\_TST.1

### ***Chapter 6 [Ohta]***

- Added some description in this section
  - 6.2 allows for subsets depending on the functionality of the TOE
    - May not be acceptable to CC evaluators
    - Cybuck to check with NIAP, Ohta with CC evaluators in Japan [Cybuck]
  - 6.3 allows for some functions be performed in combination with IT, e.g. user authentication

- May need to revisit the language in previous sections where we say that it must be addressed by the TOE [Cybuck]
- Aren't there PPs for operating systems that go outside for authentication? [Thrasher]
  - There are STs, no accepted PPs yet [Wright]

## **Chapter 7 [Smithson]**

- Need to remove A.ACCESS [Nevo]
- Add OIE.GENUINE [Sukert]
- Why T.UD normal and hack don't refer to network interfaces? [Sukert]
  - Network objectives protect packet [Ohta]
  - O.NETWORK is just for transmission [Ohta]
- What about T.UD.IMP [Sukert]
  - Need to look at that
- T.TSF.CRED, why not apply to monitoring events? [Sukert]
  - Would apply to T.TSF.CRED.GUESS [Wright]
- Name reconciliation
- Remove "reduce motivation of the attacker"
- T.UD.PHY needs objective
  - Is only for .OUTPUT
  - Will need to be changed throughout PP
  - Address with O.I&A and O.ACCESS
  - Add to table 10
- T.UD.ANALYZE
  - Needs an objective in the HS environment
  - O.PROTECT doesn't help, how about OE.LOCATION
  - Work on this offline
  - Add to table 10
- T.RESOURCE
  - Narrow to T.RESOURCE.PEER
- T.DOS.IMP
  - Add to table 10
- T.DOS.PHY remove
- T.DOS.IMP remove
- Modify assumptions in tables to correspond to current set
- 7.2 to be completed for next meeting

## **Enterprise PP [Nevo]**

Refer to [http://grouper.ieee.org/groups/2600/drafts/Section4/HSD\\_Protection\\_Profile-Enterprise\\_Environment-v182.doc](http://grouper.ieee.org/groups/2600/drafts/Section4/HSD_Protection_Profile-Enterprise_Environment-v182.doc)

- Beginning of document stays the same in all versions
- How many will there be? [Longo]

- Four: HS, enterprise, soho, and public
- Why not have EAL2, EAL3, EAL4? [Longo]
- EAL4 is a very different kind of PP [Wright]
- Is each a superset? [Longo]
  - Not necessarily
  - Threats are different, some increase even in less highly valued asset environments [Cybuck]
  - We do have a goal for the HS PP to be a superset of all others [Smithson]
- Took out telephone line in Enterprise
  - Some of our customers are concerned about that [Sukert]
  - Secure phone lines are used in HS, not typical in enterprise [Cybuck]
  - Would those customers be more of a HS environment? [Thrasher]
    - Perhaps, I can't answer that [Sukert]
- All network traffic needs to be encrypted? [Longo]
  - No, just storage
  - O.NETWORK needs to be looked at in enterprise environment [Longo]
- Authentication over network and walkup authentication: where do we specify the level of authentication?
  - Relies on the strength of function SOF [Ohta]
  - For HS it's SOF medium [Ohta]
  - For Ent medium is OK [Ohta]
  - So they are the same
  - The PP is a "what" document, not a "how" [Sukert]
    - Threats and objectives are the same [Sukert]
    - Difference will appear in chapter 5 [Sukert]
  - Can weaken SFRs as long as you still meet the desired EAL [Wright]
  - Some threats and objectives may be removed in Ent; others might be same [Ohta]
  - Objectives may be weakened perhaps
  - When table 11 is updated for HS, it can be used to look at which objectives are effected by the removal of threats [Smithson]
- OE.LOCATION removed
- Need to proceed with chapters 5-7

## 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-Feb2005.ppt>

- PP creation
  - Soho and Public versions: Jean Claude to take both

- Total doc
  - Sect 1 and 2 ready after updates from this meeting
  - Sect 3 (minus mitigation strategy) ready now (look for 08)
  
- Administrative:
  - Brian Smithson to get confirmation on Ricoh location in New Jersey for September meeting, keeping open a possible date shift
  - Brian Volkoff to look into HP locations in San Diego for December meeting
  
- Section 1, remaining from Camas meeting:
  - Bibliography pulled in from all sections
  - Terms pulled in from all sections
  - Refer to mitigation techniques from sec 3 rather than NIST
  - Define assets from sec 3
  - Add acronyms from sec 2/4 (and maybe 3)
  - Add explanatory text based on asset value and not just nature of environment
  
- Section 1, new:
  - Enterprise m Mitigations to be aligned with section 3
  - High Security: add our changes from Enterprise into this section/diagram also
  - High Security Mitigations to be aligned with section 3
  - Custom environment, Public: Need more words in this section? Such as, mitigation techniques? (Would like to replace mitigation parts with pointers to section 3, but Sec 3 is not organized by environment)
  - Custom environment, Legacy: Also need more words in this section (regarding recommendations)
  - When we discuss assets, make recommendation to use different environment (other than SOHO) in situations involving high value or regulated assets
  
- Section 2, remaining from Camas meeting:
  - Cross-check with original vuln list, need to reconcile with new list resulting from sec 2 and 4 reconciliation
  
- Section 2, new:
  - T.UD.IMP.FAX: In general, should refer to PSTN wherever we say FAX. Need to add some text about that
  - Vector components need to be defined
  - Does all that vector info need to be in the final document?
  - Expertise ratings: "novice" should be "layman", as defined by CEM

- Section 3, remaining from Camas meeting:
  - Complete the missing sections that are partially done/outlined
  - Align with Sec 2 threats and make recommendations
  
- Section 3, new:
  - Asset discussion at intro still needs to be done
  - 1.3.1 reference to T.TSF.AUD.\*, why is it listed as a physical threat? Needs to be reworded
  - 1.3.1.4 should only describe theft of imaging unit, and have a separate section for theft of disk
  - References to vendors and products shouldn't be used; need to be reworded to minimize the use of trademarked names
  
- Section 4, remaining from Camas meeting:
  - Sec 4 team to determine which threats apply to which environments and provide to Sec 2 team
  
- Section 4, new:
  - Ch 1-4:
    - Figure 1 - box should include interfaces
    - 2.2.3.4 firmware paragraph should be changed to indicate access controlled update and signed image. Make it a general statement to include flash, disk, etc.
    - Add paragraph numbering for "TOE Architectural Description"
    - Should add descriptions of Scanner and Printer
    - T.EA need to change names, check descriptions, to match section 2
    - Need to look at T.UD.SNIFF.PHONE; was removed from all PPs
  - Ch 5-7:
    - Add full description for FAU\_GEN.2
    - 6.2 allows for subsets depending on the functionality of the TOE. Cybuck to check with NIAP, Ohta with CC evaluators in Japan, to see if this is acceptable.
    - 6.3 has similar issues to above.
    - What about T.UD.IMP? Need to look at
    - Name reconciliation with section 2
    - Remove "reduce motivation of the attacker" from all objective rationales
    - T.UD.PHY needs objective. Will need to be changed throughout PP. Address with O.I&A and O.ACCESS. Add to table 10.

- T.UD.ANALYZE. What objective to use? Work on this in the subgroup. Add to table 10.
- T.RESOURCE: Narrow to T.RESOURCE.PEER, adjust descriptions as needed.
- T.DOS.IMP: Add to table 10
- T.DOS.PHY remove
- T.DOS.IMP remove
- Modify assumptions in tables to correspond to current set
- 7.2 to be completed for next meeting
- Enterprise PP:
  - All network traffic needs to be encrypted? O.NETWORK needs to be looked at in enterprise environment
- SOHO and Public PP's:
  - Jean-Claude to make first drafts. Coordinate with existing PP team to determine when to get the best snapshot from which to begin work.

See you at Epson's facility in Tokyo, in April 2005.

***\* Adjourned at 1:00PM, 2/24/2005 \****