

**IEEE P2600 Meeting #8
January 13-14, 2005
Sharp Labs, Camas, WA**

Attendees

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

Nick Del Re / Canon
Wanda Nuckolls / Canon
Tom Haapanen / Equitrac
Takanori Masui / Fuji-Xerox
Brian Volkoff / HP
Harry Lewis / IBM
Stuart Rowley / Kyocera-Mita
Jerry Thrasher / Lexmark
Bill Wagner / NetSilicon
Nancy Chen / Okidata
Satoshi Fujitani / Ricoh
Yusuke Ohta / Ricoh
Ron Bergman / Ricoh Printing Systems
Peter Cybuck / Sharp
Andrew Ferlitsch / Sharp
Ron Nevo / Sharp
Chuck Pickett / Sharp
Bogdan Plewnia / Sharp
Craig Whittle / Sharp

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 1/13/2005 *

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-Jan2005.ppt>

Minutes and Agenda approvals

November's minutes and January's agenda were approved.

IEEE patent policy

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Jan2005.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-Jan2005.ppt>

Meeting schedule update

Sharp confirmed for January 2005 meeting in Camas, WA.

February's meeting was confirmed for February 23-24 at Equitrac's facility in Plantation, FL (near Fort Lauderdale). Details are posted on the web site at <http://grouper.ieee.org/groups/2600/meetings.html>.

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>.

Don proposed schedule changes for the May, September, and December meetings. These meetings are not being held in conjunction with PWG, so we have more flexibility in scheduling. The proposed changes move the meeting dates from Thursday/Friday to Wednesday/Thursday or from Monday/Tuesday to Tuesday/Wednesday, in order to make travel easier. The proposed changes are:

- May 19-20 → May 18-19
- September 15-16 → September 14-15
- December 12-13 → December 13-14

No objections were heard, and the schedule will be changed accordingly.

The current schedule for meetings in 2005 is listed on the slides
<http://grouper.ieee.org/groups/2600/presentations/P2600-Jan2005.ppt>

TCG update [Wright]

- Have had several phone conferences, mostly organizational matters and use cases for this environment.
- Brian Volkoff has been elected as Chair of the group.
- Charter has been approved.
- Next general meeting of the TCG is 3/29 – 4/1 in San Diego.
- Regarding relations with P2600:
 - TCG is focused on establishing a trusted connection between the HCD and upstream servers or clients
 - It's accomplished through specs (secured memory location, mandatory encryption techniques, etc.)
 - Doesn't specify security of the device itself like P2600
 - Liaison between groups is still being worked on with IEEE Board of Directors. Legal/contractual issues, mostly to do with IEEE IP policy.
 - How will that manifest for this group is mostly access to documents, could show us the charter, may show other documents for review of impact, comments.
 - P2600 members will probably not be able to attend meetings unless also a member of TCG. There is some possibility that one non-TCG member could act as liaison, but that role would probably be given to a member of both.
 - Regarding future requirement to synchronize, such as for encryption, most specs are public. HCWG of TCG won't create new encryption specs, will use existing ones.
- TCG HCWG is still soliciting memberships, such as from Ricoh and Sharp. [Volkoff]

Action items from previous meeting [Wright]

Refer to slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Jan2005.ppt>

Section 1. Introductory Pages [Wright]

Refer to <http://grouper.ieee.org/groups/2600/drafts/June2004-Plan/P2600Intro-V06.doc>

Updates from previous meeting

- Participant list has been updated. Also other updates have been made as noted in the document.

Terms

- In the PP, TOE can be a subset of the HCD. Should that be shown in Section 1 also? [Nevo]
 - Definitions from other sections will be pulled forward into Section 1. In the case of the PP, since it needs to stand alone, they will be duplicated. [Wright]
- If shown in a list of abbreviations, should it also be defined in the text? [Wagner]
 - IEEE requires definition in first occurrence. IEEE editors will ensure that if we don't. [Wright]
- Some threat mitigation recommendations appear in Section 1 that also appear in Section 3. Is there going to be some segregation of what goes into what sections? [Thrasher]
 - Those came from NIST definitions directly. We'll clean them up, remove recommendations and leave that for section 3.
- The assets aren't described anywhere, and yet we talk about threats and recommendations in section 3. [Thrasher]
 - Aren't they in section 4? [Wright]
 - Yes, but they should appear earlier so they can be referenced earlier. [Thrasher]
 - OK so we'll pull definitions of assets forward into beginning of section 2 or end of section 1. [Wright]
 - Assets and environments? [Nevo]
 - We could keep it simple and just define assets. Maybe before the definition of environments, we'll have to work on that. Or in the terms and definitions section.

Section 2. Vulnerabilities/Threats/Exploits [Wright]

Refer to <http://grouper.ieee.org/groups/2600/drafts/June2004-Plan/Section%20%20-%20threat%20details%20-%202005-01-11.doc>

Threat applicability to environments

There was a lengthy discussion about how threats should be related to the four defined environments. The major areas of concern [of various speakers] were:

- Does an X in the column mean that it applies to the PP, or that it should be considered in section 3?
- Should all listed threats be listed in section 3?

- What is the criteria for placing an X in the column? That it is a likely threat? That the asset value is high, even if the threat is unlikely? That it is a threat which matters to the user? That there is a technical mitigation for the threat?
- What does it mean if we don't include an X for an environment? Does that imply that there is no threat and no need to worry about it in that environment?
- Do we consider reliance on firewalls? Even if it doesn't eliminate a threat, does it reduce it enough to make it not worth an X in some environments?
- Do we trust inside users in SOHO? In High Security?
- Should SOHO include telecommuters who, operating in a home office, are effectively extending their Enterprise network?
- Should these columns be included in the document, or used only during document creation and then removed for publication?

We resolved to use different letter designations in the columns:

X = addressed specifically by the protection profile

R = addressed in protection profile by resiliency/recovery from the threat

N = not applicable or very low probability

G = nothing in profile, but general techniques are provided in section 3

P = addressed through physical security

We also resolved to use this table for specification development, but possibly describe threats and their applicability to environments in other ways in the final document.

- T.RESOURCE
 - It's listed incorrectly in the table, and should be its own high level category [Wright]

What about SOHO environments that are regulated?

- Is a doctor's office really SOHO? It's regulated by HIPAA and therefore has specific security capabilities required by law. [Wagner]
 - We have a doctor's office example in section 1 description of environments [Wright]
 - Could we put a disclaimer in section 1 about SOHO, stating that if they're in a regulated industry, even if topologically SOHO, they should consider Enterprise environment instead. [Smithson]

Section 3. Directives/Best Practices [Thrasher]

Refer to <http://grouper.ieee.org/groups/2600/drafts/Section3/Section3-Draft0.006.doc>

- Assets will be discussed at the end of section 1 [Wright]
- Should this section about HIPAA, etc, discuss specific implications for HCDs? [Nevo]
 - The legislation isn't that specific in most cases [Thrasher]
 - Regulations change, vary from country to country, can't provide that detail in this doc [Wright]
 - Need some help with how to describe regulations and (to whatever extent) their implications on HCDs [Thrasher]
- Will move asset discussion to sec 1, keep discussion of laws in sec 3 but "light" treatment
- Rephrase initial "practices" as such, not as recommendations (they come later)
- In subsection 3, make sure references to section 2 threats are consistent with section 2
- Should we make references to different password policies or provide our own or should encryption be discussed in detail?
 - No, provide general intro and references
- Plans: for each threat in section 2, a paragraph about why its important in each environment, then a discussion of how to mitigate

Section 4. Protection Profile

Refer to http://grouper.ieee.org/groups/2600/drafts/Section4/HSD_Protection_Profile-High_Security_Environment-v172.doc

Chapters 1-4 [Nevo]

- Definition of TOE
 - Started with whole HCD
 - Want to allow subsets
 - Example: data security kit [Smithson]
 - Important for vendors to define TOE as small as possible/necessary [Ohta]
 - Agreed
 - Could any of the blocks in figure 2 be defined as the TOE? [Wagner]
 - My understanding is that you need to be compliant with all elements of a PP, so it might be hard to pick a subsystem [Cybuck]
- Terminology
 - Authorized vs. unauthorized
 - Revised definition is more consistent with rest of document [Smithson]

- Particular user can be auth for some things, not for others [Smithson]
 - Agreed
- Revised figure 1
 - Should add arrow from CE to Operation Panel [Masui]
 - Should be indicated as an example, not a definition of the TOE
- Revised figure 2
 - Should add output bin [Cybuck]
 - Should be indicated as an example
- Roles
 - Roles are typically not hierarchical, but are compartmentalized [Whittle]
- Access issues
 - We removed access protection assumption because TOE still needs to protect
 - Threats are the same inside or outside firewall [Thrasher]
 - Couldn't think of a threat that existed outside the firewall that couldn't also exist inside [Smithson]
 - Hadn't we said something different, that in some environments we trusted insiders? [Wagner]
 - You have more sophisticated attackers in high security environment [Thrasher]
 - In SOHO, we can make other assumptions as a practical matter [Nevo]
 - If we don't have any assumption of firewall, or physical protection, then cc evaluator will not agree to lower than EAL4. I am wondering if we should have a reduced scope assumption about firewalls and external physical [Ohta]
 - If we're going to protect higher value assets that require a higher EAL, then maybe we need to break out some of these assumptions and requirements so we can address them [Cybuck]
 - I think the assumption is appropriate [Lewis]
 - Assumption is coupled with whether you trust every insider, and I don't think you can say you trust every insider [Thrasher]
 - Can we retain the physical security assumption [Wagner]
 - It makes more sense to leave that in [Cybuck]
 - From CC point of view, administrator is generally trusted, but general user is not trusted even in HS env [Ohta]
 - Agreed to keep physical, remove network
- Threat list
 - Will need to sync with section 2
 - T.ud.phy inconsisten with assumptions [Masui]
 - Also is not addressed by an objective [Smithson]
 - We will address

- Objectives
 - OE.NETWORK removed, needs to be put into section 3
 - Need to put OE.LOCATION back in [Wagner]
- Need to add Firmware to assets [Masui]

Chapters 5-7 [Ohta]

- Changed style to CC style
- FAU_STG overwrite OK?
 - Need audit preservation for things like HIPAA [Nevo]
 - Minimum reqt is to provide "stop", mfr can provide other options if they want
- Encryption
 - Must have encryption [Wright]
 - Don't want to specify particular encryption
 - If we specified something here, it could be out of date [Nevo]
 - Different industries have preferred standards, but they are also changing [Cybuck]
 - Suggestions belong in section 3
- EAL2 chosen, but is an open issue
 - EAL4 requires source code eval
- Can we assume a sophisticated attacker in EAL2? [Thrasher]
 - Need to add AVA_VLA.4 [Ohta]
 - Has dependencies ADV_IMP.1 and LLD.1 [Ohta]
 - Makes it very close to EAL4 overall [Ohta]
 - Difficult to do [Ohta]
- TOE genuinity - deferred to later
- SOF claim - is a probability function
- Chapter 6 is a new chapter: application notes (rationale becomes chapter 7)
 - Can we simply reference P2600 spec instead of including? [Smithson]
 - PP must be self contained
- Chapter 7 is the previous Chapter 6
 - Rationale showing objectives fulfill threats
 - Put back table 10 o.access, oe.location, oe.network

Question about HCD subset [Masui]

- You need to address everything, if your product does not include parts that are addressed by the PP [Wright]
 - For example, if you do not have disk drive, your ST can exclude it [Wright]
 - You cannot artificially exclude something that is present [Wright]
- May not be acceptable from some evaluators [Ohta]

Action item review [Wright]

Refer to meeting slides for complete list of action items for and before the January meeting:

<http://grouper.ieee.org/groups/2600/presentations/P2600-Jan2005.ppt>

- PP
 - Need to make updates to High Security PP
 - Then adapt to Enterprise, then the other two
- Merging sections
 - Lead editor for the whole spec: Jerry Thrasher “volunteered”
 - Merge sections 1, 2, and 3 soon
 - Make each PP a normative annex
- Schedule
 - Originally we proposed to be ready by June
 - Although we may not make that date, we should remain aggressive
- Next meeting in Plantation FL, Feb 23-24
 - Lots of hotels around
 - Rates vary

See you at Equitrac’s facility in Plantation, in February 2005.

**** Adjourned at 11:45AM, 1/14/2005 ****