

IEEE P2600 Meeting #7
November 18-19, 2004
Clarion Rivermark, San Antonio, TX

Attendees

Chair: Don Wright / Lexmark
Secretary: Brian Smithson / Ricoh

Lee Farrell / Canon
Brian Volkoff / HP
Ron Bergman / Ricoh Printing Systems
Satoshi Fujitani / Ricoh
Stuart Rowley / Kyocera-Mita
Jean-Claude Longo / Océ
Wanda Nuckolls / Canon
Bill Wagner / NetSilicon
Peter Cybuck / Sharp
Harry Lewis / IBM
Yusuke Ohta / Ricoh
Ron Nevo / Sharp
Tom Haapanen / Equitrac
Nancy Chen / Okidata
Kazutaka Higo / Fuji-Xerox
Kentaro Ide / Epson
Takeshi Nakamura / Kyocera-Mita
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 9:00 AM 11/18/2004 ***

Administrivia [Wright]

The following administrative items were reviewed:

Agenda review

Refer to meeting slides for detail
<http://grouper.ieee.org/groups/2600/presentations/P2600-Nov2004.ppt>

Introductions

(see Attendees, above)

Minutes and Agenda approvals

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

IEEE patent policy

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Nov2004.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-Nov2004.ppt>

Meeting schedule update

Sharp confirmed for January 2005 meeting in Camas, WA.

February's meeting does not currently have a location. It is scheduled to be in Tampa, but if a member company has facilities in Florida and is willing to host the meeting (P2600 only, not PWG), please contact Don Wright.

We are still looking for a host for April 2005 in Tokyo.

PWG has reduced their meeting schedule for 2005 and will now have meetings only in January, April, July, and October. Since we have aligned P2600 meetings with PWG meetings, it is possible to change locations and dates for some previously scheduled meetings:

- For those meetings that would have taken place in conjunction with PWG, Don Wright proposed that we move the dates from Thursday/Friday to Wednesday/Thursday to make it easier to avoid weekend travel. Don also proposed to move the December 2005 meeting from Monday/Tuesday to Tuesday/Wednesday for similar reasons.
- The September meeting was scheduled to take place in Madison, WI, hosted by a PWG member. Since that meeting has been eliminated by the PWG, we are free to locate elsewhere. In the absence of other suggestions, Don proposed another meeting at the IEEE office in Piscataway, NJ.

The current schedule for meetings in 2005 is listed on the slides

<http://grouper.ieee.org/groups/2600/presentations/P2600-Nov2004.ppt>

TCG update [Wright]

- Don Wright made a request on 10/2 to establish a liaison relationship between P2600 and TCG. Prospects for this are positive.
- TCG member meeting was held 11/9 – 11/11/04 in Phoenix AZ
- The Hardcopy group had its first face-to-face meeting. Fujitsu, HP, IBM, and Lexmark participated. This meeting mostly consisted of work on the group's charter.
- Brian Volkoff will send TCG information to the P2600 list again for new members.

Action items from previous meeting [Wright]

Refer to slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Nov2004.ppt>

- Section 1: items complete.
- Section 2: Posted their work on the P2600 list, and updated just before this meeting. [Haapanen]
- Section 3: still a work in progress; Jerry Thrasher posted a draft [Wagner]
- Section 4: updates complete, alignment with section 2 complete, work on chapter 5 in progress [Nevo]
- January meeting's hosting arrangements finalized
- Section 1 drawing tool and graphics issue resolved

Content of standard [Wright]

It's time to start thinking about pulling sections into a single document, and need to reaffirm or establish new document editors. We should also consider whether we need two days for meetings or just one.

Section 1. Introductory Pages [Wright]

Refer to <http://grouper.ieee.org/groups/2600/drafts/June2004-Plan/P2600Intro-V05.doc>

Participant list

- Needs to be updated to reflect recent attendees.

Security environment examples

SOHO

- Added doctor's office

Enterprise

- Combined financial examples

- Added health insurance claims office (also represents a production printing environment)

Custom

- Copy shop / Internet café
- Added college campus
 - Should add “extensive access from Internet” to this description [Wagner]

Terms

- Updated HCD definition to be very general, “physical embodiment of digital document”.
- Should it include standalone scanners? HP Digital Sender is a good example. What about non-networked devices?
 - Same could be said for non-networked printers [Smithson]
 - No difference between non-networked devices and ones that have both network and direct interfaces. There are no new threats. [Wagner]
 - Most security on low end devices would need to be handled by the PC and physical security. [Wright]
 - Conclusion: yes, we’ll include non-networked devices. [Wright]

Work to be done

- Identify additional terms and definitions, and bibliography and reference items (ongoing work)
- Work on the graphics, now that we know what tool was used (Visio, latest rev)
- What about references to memory sanitization? There is new work going on at NIST about this, although it isn’t funded. [Cybuck]
 - Most of this is in Section 3 [Wright]
- References are fairly dynamic. Looking up our existing references, some have already become obsolete. [Wagner]
 - Should be careful about the stability of references that we cite [Wright]
 - Could we have a disclaimer at the beginning of those lists that urges people to check for updates? [Smithson]
 - I’ll check with the IEEE editorial staff about how to cite these kinds of references, especially web references [Wright]

Section 2. Vulnerabilities/Threats/Exploits [Haapanen]

Refer to <http://grouper.ieee.org/groups/2600/drafts/Section2/Section%20%20-%20threat%20details%20-%202004-11-11.doc>

The overview section is based on discussions from the Lexington meeting. We removed references to the original vulnerabilities list from the document (but we will still cross-reference them as a check). The overview section also contains our first take at what are applicable environments for each threat, but it is up to the Section 4 team to review and determine these.

Issues for group discussion

Are man-in-the-middle attacks out of scope?

- TCG can help prevent MIM attacks, using crypto techniques [Volkoff]
- Can't do it with just the printer, need to protect from end to end [Longo]
- IPsec would do that [Volkoff]
- We need to identify all threats even if we can't address them in the PP [Wright]
- Some threats are out of scope for the PP but in scope for P2600 [Smithson]
- They would be addressed in section 3 [Nevo]
- In a High Sec environment, motivation is also high [Ohta]

In the PP, we have some other threats, like T.UD.NORMAL and T.UD.HACK [Nevo]

- In the PP we must consider at first that there are no security functions present, then look at threats (like someone can access someone else's documents), then add security functions to deal with those threats (like user IDs and PINs) [Ohta]

Other proposed changes that came up in the Section 4 work [Smithson]

- Combining and reconciling Integrity threats, plus Sniff M-*, and DOS.IMP all are impersonations that have a similar characteristic that they attack a document
 - Were split because some they are disclosure, integrity, or denial of service [Haapanen]
 - I'll get with Tom about this later
- We lost T.RESOURCE?
 - We'll look into that. Not sure where it would go [Haapanen]
 - We proposed a separate category.
- Change names on T.EA's, "RELAY" refers to a specific mail relay service, suggest "SERVICES" instead. Also, "NOTIFY" refers to one kind of problem, but other exploits of applications could be damaging, suggest "APPS" instead.
 - How about EA.DOS? [Wright]

- Could be OK, might be confusing with other DOS's in the list.
- T.UD.SNIFF, some of them aren't strictly sniff attacks (e.g. passive), they are more active man-in-middle attacks. Suggest they changed to T.UD.IMP or something like that. T.UD.SNIFF.AB should really be a TSF because it's an indirect attack.
- I'll forward the list to Tom and we can work on it offline.
- One of the problems is that in the PP, we roll these threats up to a higher level and deal with them there, and inconsistencies show up when you do that.

Detail section

- Where are the traceback numbers? [Wright]
- We'll cross-check them and remove numbers. Are there any volunteers to do this? (none) Then we'll do it

Terminology for skill level, where did it come from? [Cybuck]?

- Ohta-san proposed it in Lexington, came from CC CEM v2.2. Also defined there are levels of specialization of equipment. [Smithson]
- These should be put in the definitions? (yes) [Wright]
- Validators look at those [Cybuck]

How do we counter a net flood? [Ohta]

- Cannot prevent, and other devices are also attacked by such a flood, so these shouldn't be considered.
- Device should be able to recover once the attack has ceased. Also, the network stack shouldn't fail. [Wright]
- Also, other functionality of the device should be able to continue, e.g. attack on the network interface doesn't screw up the FAX phone interface [Smithson]

T.DOS.PRT

- Should be left in, or is this a network attack? [Wagner]
- Leave in, it's different. Is "physical" a good term to use? [Wright]
- In the PP, we defined "local" interface to mean anything in close proximity (<10m) that included USB, IrDA, Bluetooth [Smithson]

T.DOS.PRT.PRIORITY

- How to distinguish between too many users printing too much stuff, and someone deliberately submitting jobs as an attack? [Longo]
- One would be from a single user, other from multiple users. [Wright]
- Device needs to be able to handle the threat, even if it's accidental [Wagner]
- This threat specifically refers to priority [Smithson]

- Is “proficient” required to send lots of print jobs? [Chen]
- Only if priority change is factored in [Wright]

T.DOS.FAX.HOOK

- There’s no countermeasure for this [Wright]
- Could detect lack of dial tone and notify the operator [Wagner]
- Won’t help if someone is trying to send a fax inbound [Wright]
- Could poll the line for a dial tone periodically [Wagner]

IETF Fax

- Need to leave this in and figure out if there are additional threats due to IETF faxing. [Wright]

T.DOS.PHY

- Mechanical and electrical, are different? [Nevo]
- Hard to separate them out [Haapanen]
- Novice skill? Not for electrical alteration [Nevo]
- It’s the minimum skill requirement for the threat [Haapanen]

Note: During the lunch break, Smithson and Haapanen reviewed PP updates to the Section 2 threats list and agreed upon some changes, but continued review at the meeting would be against the published threats list.

T.UD.SNIFF.EM

- Also refers to sniffing radiation from the device, not just from network cable? [Wright]
- Should be separate [Cybuck]
- Will add under T.PHY, may end up elsewhere [Wright]

T,UD.SNIFF.DNS and .IMP

- Need to clarify differences. [Wright]

T.UD.SNIFF.M-*

- Need Will be combined with T.UD.INT.* under T.UD.IMP [Smithson]

T.UD.SNIFF.AB

- Will become a TSF [Smithson]

T.UD.SALVAGE.DISK

- What about reading overwritten data with more sophisticated skills and equipment? [Wright]
- Is direct or indirect? [Yami]

- Could read password file, replace disk, attack later [Haapanen]

T.TSF.CRED

- Should be indirect threat, only.
- Aren't credentials assets? Therefore, these would be a direct impact. [Wagner]
 - No, or yes, but not the same type. The only point of stealing one type (credentials) is to use them to attack the other type (documents). [Smithson]
- For indirect threats, should the outcome be direct or indirect? [Haapanen]
 - Indirect outcome could be a very long list, in some cases [Smithson]
 - Should use the indirect asset being threatened, and list the direct outcome. Should also have a definition of fields at the beginning of the table [Wagner]

Next steps

- Don Wright noted changes and will send to Tom.

Section 3. Directives/Best Practices [Wagner]

Refer to <http://grouper.ieee.org/groups/2600/drafts/Section3/Section3-Draft0.003.doc>

This is still a work in progress. Some areas are redundant, some items have been dropped, Jerry Thrasher had little time to edit after receiving the draft. Sections labeled "still needs updating" haven't changed since Lexington. Also, need to update to match new threats from Section 2.

Discussion

- 1.3.5 Should audit logs also include non-privileged operations like printing something (who, when, what)? [Wright]
 - This adds a vulnerability because you're storing potentially sensitive information like document names [Wagner]
 - Isn't the audit log already secure? [Wright]
 - The difference is that document names may need to be protected from disclosure (read access), but system events may only need to be protected from alteration (write access) [Smithson]
- 1.3.5 This should also log "any access to cryptographic keys" [Yami]
- A way to handle threats and countermeasures section is to have a table of threats with pointers to paragraphs elsewhere that describe the appropriate countermeasure(s). This would be less confusing, especially considering different security environments.

- Also, some countermeasures may be at the manufacturer level while others are at the user level [Wright]

Next action

- Bill and Jerry to review/update marked up copy from Don

Section 4. Protection Profile

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

Chapter 2 [Nevo]

- Added “authorized user” and “unauthorized user”
- Table 2: Customer Engineer doesn’t need to be an employee of the vendor [Wagner]
- Added “maintenance port” and “foreign device interface”
 - Is sufficient to have one type of external interface, or separate the analog coinbox type from the digital type that is more of an IT function [Cybuck]
- What is “HSD”? [Wright]
 - Previously it was MFP, which is too specific. Used the term Hardcopy Systems and Devices, taken from the title of the P2600 spec. [Smithson]
 - We used HCD Hard Copy Devices in Section 1 [Wright]
 - I’ll change it globally [Smithson]

Chapters 3-4 [Smithson]

- Added “competence” along with “trust”
- Should customer engineer be trusted? In some environments, you might have someone watching over them.
 - Could you say “while CE has access, they will be monitored”? [Wright]
 - Can’t always assume that. How about saying that they are assumed to be trusted, and that customers may want to take their own measures if they don’t trust them? [Smithson]
 - We’ve been asked not to allow the CE to defeat security settings. There’s something about this later under configuration management, ensuring that once installed it can’t be altered [Cybuck]
 - Sufficient to say that they aren’t authorized to alter security settings? [Wright]
 - To some degree you have the same issue with administrators. CE just gets a snapshot, but administrators have access to everything. [Rowley]
 - User can choose the administrator, but not the CE [Ohta]

- Can't assume a CE doesn't have authority to change security settings in this place, we would need to assume it as a threat and then make a security objective out of it later, unless we're assuming it as a policy [Smithson]
- I think it's more of a policy that administrators won't give CEs usernames, passwords, etc. to make such changes [Wright]
- How can the user be confident of that? [Ohta]
- The equipment would need to not allow that [Wright]
- Objective would be that the TOE must prevent CE from altering security settings [Ohta]
- Then the assumption of trust needs to be removed and we deal with it in threats, objectives, requirements [Smithson]
- Either you have trust, or you have policies in place to mitigate your lack of trust [Wright]
- It's a reasonable requirement that the administrator password is required to change security settings. Peter said he already came up against that. [Rowley]
- Also need to require that there are no backdoors to bypass passwords that the CE has access to [Cybuck]
- None of this precludes a device from giving the CE the ability to change security settings. [Wright]
- I'll write it up as the CE is trusted or the customer will take measures [Smithson]
- A.ACCESS, removed assumption that it could be connected directly to the Internet, also removed assumption that it could be connected to a phone because that's a threat.
 - Should be more general to say Internet or other untrusted network? [Wright]
 - Is the term "firewall" sufficient? [Wagner]
 - The TOE should not depend on this assumption at all. In high security environment, the motivation is also high [Ohta]
 - This is a first line of defense [Wright]
 - We describe the environment elsewhere, but in this section we need to make assumptions that reduce threat [Ohta]
 - We talked before about removing the assumption about physical access, are you talking about network access also? The whole assumption? [Smithson]
 - Physical assumption lets you ignore the threat of a hammer and crowbar [Wright]
 - Authorized users could use a hammer and crowbar [Smithson]
 - We'll look at the broader implications of taking out A.ACCESS and report back on this for next meeting [Smithson]
- Threat sections need to be made consistent with Section 2 as now revised. Some of those revisions were made in advance. One thing we'll need to look at is that our descriptions at the higher level of detail matches with Section 2's descriptions at the lower level of detail.

- Removed “copier drum” from T.SALVAGE because it was a significantly different type of threat in terms of difficulty, expertise, etc., in contrast to removing a removable disk. If we want it back, it should be a different threat and consider how to countermeasure it.
 - Could discharge the device [Cybuck]
 - Or a policy to copy black pages and white pages before removal [Wright]
 - It’s difficult for a vendor to provide an automatic function to countermeasure this. It would need to be mitigated by procedures and policies [Ohta]
 - We’ll make it a separate threat for now [Wright]
- Chapter 4 has had less internal review by the Section 4 group, but we have basic agreement.
- O.PROTECT is new.
- O.DOS is new and probably needs a new name, like O.RECOVERY. Definition as shown only specifies that an attack on one interface won’t clobber another interface. Other suggestions are that the TOE will recover after the attack, without intervention.
 - Also shouldn’t cause a network stack failure or something that gives root access [Wright]
 - Should also protect assets during the attack [Nevo]
 - If you’re tying up the marking path with an attack, then you can’t copy. [Wagner]
- O.GENUINE is new, but shouldn’t require software and an external interaction (as currently specified). It should be some kind of mechanism.
- O.NETWORK could be either an IT requirement or a non-IT requirement, depending on how it’s written.
 - I think it should be an IT requirement [Wright]
 - It’s a bit more actionable as a non-IT requirement [Smithson]
 - We’ll highlight it for consideration [Wright]
- Table at the end of Chapter 4 is for review, but will ultimately be moved to Chapter 6. T.UD.PHY and T.DOS.PHY have no objectives because we can’t think of any that the TOE could provide.

Chapters 5-6 [Nevo]

- No changes in Chapters 5-6 since Lexington, we wanted to talk about items to get comments for our upcoming work.
- What to do with full audit logs or nearing-full logs?
 - Options are stop working, stop logging, notify administrator, overwrite old logs, and/or email old logs or new items to administrator. [discussion]
- FCO proof of origin, is this practical? Wasn’t this dropped in DAPS? [Wright]
 - We’ll probably remove this one [Smithson]

- SO – SFR cross reference needs to be revisited.
- 5.1.X Crypto requirements are missing [Wright]
- Are these SFRs at EAL2? [Wright]
 - Some listed are EAL3 [Ohta]
 - Need to fix that [Wright]
- 5.2.5 Security Target (ASE) should clarify that descriptions are in the CC. [Wright]
- 5.3 needs to be written [Wright]

Next steps [Wright]

- Recheck acronyms and send to Don
- For next meeting, have a draft of Chapters 5 and 6
- Send list of issues to the group before the next meeting

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-Nov2004.ppt>

See you at Sharp's facility in Camas, Washington, in January 2005.

**** Adjourned at 11:45AM, 11/19/2004 ****