

IEEE P2600 Meeting #36

June 23-24, 2008

Radisson Conference Center, Longmont, CO

Attendees

Chair: Don Wright, Lexmark
 Vice Chair: Lee Farrell, Canon
 Secretary / Lead Editor (2600.n): Brian Smithson, Ricoh

Carmen Aubry, Océ (by phone)
 Shah Bhatti, Samsung
 Nancy Chen, Oki Data
 Peter Cybuck, Sharp
 Nick Del Re, Canon
 Satoshi Fujitani, Ricoh
 Tom Haapanen, Equitrac
 Helmut Kurth, atsec (6/23)
 Harry Lewis, InfoPrint
 Ron Nevo, Sharp
 Glen Petrie, Epson
 Ole Skov, MPI Tech
 Alan Sukert, Xerox
 Jerry Thrasher, Lexmark
 Brian Volkoff, HP
 Bill Wagner, Konica Minolta

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 comments may appear in these minutes, indicated by {braces}, inserted by the Secretary for clarity.

Attendees.....	1
Administrivia [Wright]	2
Introductions.....	2
Agenda review.....	2
Minutes and Agenda approvals	2
IEEE patent policy	2
IEEE WG guidelines.....	2
Officers and Editors.....	2
Meeting schedule updates [Wright]	3
TCG update [Volkoff]	3
INCITS CS1 update [Thrasher].....	3
CCVF update [Sukert].....	3
Action items from previous meeting [Wright].....	4
PP evaluation ad-hoc status [Nevo].....	4

PP+Packages discussion [Smithson].....	5
Fax-network separation / SMI mediation discussion [Smithson]	6
Protection of NVS discussion [Smithson].....	9
P2600.1/2/3/4 Comments review [Smithson]	16
PP Guide ad-hoc status [Sukert].....	16
Schedule proposal [Smithson]	17
Next meeting details [Wright]	17
Production Printing environment/PP update [Lewis]	17
Closing [Wright].....	19

*** Called to order at 9:13 AM MDT 6/23/2008 ***

Administrivia [Wright]

The following administrative items were reviewed:

Introductions

Agenda review

Refer to meeting slides for detail <http://grouper.ieee.org/groups/2600/presentations/P2600-Jun2008.ppt>

Minutes and Agenda approvals

The May 2008 minutes were approved without changes. The June 2008 agenda was presented and approved with no changes.

IEEE patent policy

See slides for the policy: <http://grouper.ieee.org/groups/2600/presentations/P2600-Jun2008.ppt>

Patent policy was reviewed. No holders of potentially essential patents or applications were identified.

IEEE WG guidelines

IEEE guidelines on such things as inappropriate topics were reviewed. No issues were identified.

Officers and Editors

No changes.

Officers:

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary: Brian Smithson, Ricoh.

Lead editors:

Editor (2600): Jerry Thrahser, Lexmark.

Editor (2600.n): Brian Smithson, Ricoh.

Meeting schedule updates [Wright]

The most current P2600 meeting information is always available at: <http://grouper.ieee.org/groups/2600/meetings.html>

Aug 11-12, 2008

- Sharp Labs, Camas WA, with PWG (Aug 12-15)

Sep 9-10, 2008

- Sharp, Arlington VA

Oct 24, 2008 (only one day)

- Lexmark, Lexington KY, with PWG (Oct 21-23)

December 11-12, 2008 – tentative

- Equitrac, Plantation FL
- Note that PWG is meeting in Irvine at Samsung Dec 2-5)

No other schedule conflicts or issues were identified during this meeting.

TCG update [Volkoff]

(TCG web site: <http://www.trustedcomputinggroup.org/>)

- There have been no recent HCWG meetings
- waiting on PWG IDS
- we will be scheduling a meeting sometime after July 4
- Samsung and Fuji Xerox have joined TCG at the Contributor level, so they are entitled to join the HCWG or other workgroups.

INCITS CS1 update [Thrasher]

(INCITS CS1 web site: <http://cs1.incits.org/>)

- No meetings since the last update
- A 30-day agenda has been posted for the July 23-24 meeting at Cisco, Raleigh NC
- On the agenda is a proposal to replace the “Standard for Protection of Personally Identifiable Information” (which ran into copyright problems with the PCI) with a proposal from NIST called “Small Organization Baseline Information Security Handbook” [Smithson]
- CC part 1 (ISO/IEC 15408-1) is out for letter ballot.

CCVF update [Sukert]

(No CCVF web site)

- There is a new letter from the US Army regarding their information security assurance requirements.

- CC evaluation by CCRA members is now OK, it is no longer restricted to CC evaluation by NIAP
- There is no longer a mandate for Medium Robustness
- There remains separate DoD lab evaluations for FIPS-140, and products must be capable of Kerberos and IPv6
- The call-for-papers for 9ICCC was extended by a couple of weeks.

Action items from previous meeting [Wright]

No action items were recorded or updated on presentation slides. The action item spreadsheet was reviewed and updated.

Pre-meeting:

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20080618.xls>

End-of-meeting meeting:

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20080623.xls>

Post-meeting reconciliation:

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20080708.xls>

- AI #246 (IEEE copyright issues for PPs) is still being worked on
- The call for sponsor ballot on the PPs will expired in June (six months after it was originally made) but we have been given an extension. We must start sponsor ballot by the end of July, or else we will need to reformulate the ballot body with a new 30-day invitation period.

PP evaluation ad-hoc status [Nevo]

Refer to slides for

detail <http://grouper.ieee.org/groups/2600/presentations/Longmont/IEEE-PP-Validation-6-2008.ppt>

- IPA will accept the PP if recognized by CCRA
 - however, IPA may interpret the PP to mean that the TOE (of an ST) must have full MFP function
- still need to resolve copyright/publishing issues with IEEE
- IEEE will issue another press release when the 2600 std is released
 - tentative publication date is 6/30/08 [Wright]
 - we need to get started on the press release [Wright]
- given the smaller PPs, could we get them done in 2 months instead of the original estimate of 2.5 months? [Smithson]
 - eval from atsec could be done in about 2 months [Kurth]
 - turnaround time after VOR is submitted is two or three weeks, plus some time for signatures [Kurth]
- PP-A will be done at NIAP, B/C/D will be done at BSI
 - possibly joint certification for PP-A; it has not been done before but we are discussing with NIAP and BSI [Kurth]

PP+Packages discussion [Smithson]

Refer to document:

<http://grouper.ieee.org/groups/2600/presentations/Longmont/Explanation%20of%20new%20PP%20structure.pdf>

- This new approach was reviewed at the Rochester meeting, and the only concern at that time was whether IPA would accept the approach. Now it appears IPA will accept this approach. We should approve it to go ahead with future drafts.
- This approach was created based on input from NIAP and from atsec:
 - NIAP was concerned about the complexity of the family of PPs (FoPPs) and particularly concerned about how the administrative and audit functions that are distributed among the PPs in the family would come together in an ST.
 - atsec was also concerned about the complexity and suggested that we had overspecified the assets and threats. Assets were defined in various states, like a workflow, as being in transit, at rest, waiting to be released to the output tray, etc. They thought that if we simplified the asset and threat model, we could put that in a common PP that address all of the assets, threats, and objectives, that would apply to all HCD configurations. Then, packages of SFRs (and only SFRs) could be used to address the specific needs of specific HCD configuration components.
- The PP+packages prototype was created very quickly and reduced the overall bulk of the drafts by about 2/3.
- The new approach addresses all of the concerns of the old approach, and does so without putting any threats or objectives in the packages. However, if it was needed, it is possible to make threats and objectives that are specific to a package. You can formulate threats and objectives in such a way that they are bound to a package [Kurth]
- Where to the PPs A, B, C, and D fall out of this? [Lewis]
 - The same as before, there are four PPs with packages for each.
 - Making the PP-C draft, one thing became apparent that wasn't obvious before, and that had to do with protecting deleted documents from offline salvage but giving no protection to any other state of document.
- Two other changes were made, but they were independent of the new structure. These changes are in the PP+packages draft, but would need to be put into the family of PPs if we were to continue using that structure:

- How we specify protecting data in nonvolatile storage from offline salvage. Before, we used FDP_RIP and FCS_*, but it turns out that FDP_RIP is not appropriate for this purpose and the new technique makes it possible to avoid specifying encryption as an implementation requirement.
- We took out flow control as a technique for preventing fax-to-network bridging and other network issues.
- Any objections to going forward with this approach? [Wright]
- We started this way, but IPA objected [Wright]
 - No, we started with one PP, then tried a packages approach and a family approach [Nevo]
 - It is similar to what we started with [Wright]
 - It is more similar to the packages approach that was proposed by Nevo and Cybuck, but this one does not have optional threats and objectives, to which IPA objected, and it also covers all of the configurations that we had intended to cover.
- Are we confident that IPA will accept this at the end? [Thrasher]
 - They said they approve of it [Nevo]
 - They won't put it in writing, but neither will NIAP [Smithson]
- Any objections?
 - {no objections}
- We go ahead with the packages+PPs approach.

Fax-network separation / SMI mediation discussion [Smithson]

Refer to document:

<http://grouper.ieee.org/groups/2600/presentations/Longmont/no-smi-mediation.pdf>

- We began four years ago with a requirement for assurance of fax-network separation, and we also wanted to protect against misuse of network interfaces and services.
 - When we started, in CCv2.3, I think we had the ability to use an SAR (ATE_FUN) that could handle the fax-network separation, but that went away in CCv3.X, so we needed to look for SFRs.
 - We tried many approaches, and eventually settled on using flow control SFRs for both fax-network separation (generalized to deal with controlling flow between any interface and a network interface) and misuse of the network interface (generalized to deal with controlling flow between a network interface and itself).
 - We found that flow control was not the correct solution, so the current approach uses access control. We can't use

- FDP access controls, because that's only for user data, so instead we're using management functions.
 - One of the problems we have always faced is that a particular device's solution may be the result of architecture or design, for example there is no data path between fax and network. So we needed to write the SFR in such a way that it does not require a TSF solution if the separation is accomplished by architecture or design.
- It also bothers me that I don't think there are any products that have this vulnerability, so it is as though we are codifying an urban legend.
- Would it help if the entire industry said that this problem does not exist? [Wright]
 - They will still ask us to unsolder fax connectors [Thrasher]
 - Some customers won't let you use a fax unless you can prove that there is separation [Sukert]
 - We've brought this on ourselves by some vendors certifying the separation. We'll get stuck putting it back into our STs even if it isn't in the PP [Volkoff]
 - I think that's true, and vendors could do it however they want to, using flow control or extended component definitions, or whatever.
- I asked David Freas of DAPS for his opinion, since he manages fleets of MFPs for government agencies, and he said that they really want it in the PP because it's a requirement to certify and putting it in the PP allows them to compare products more effectively.
- We need to find a solution that we can live with.
- Whether it makes sense or not, it needs to be in the ST, because the customers demand it [Wright]
 - Does it need to be in the PP?
- One of the original goals of writing the P2600 PPs was to establish a baseline for the whole MFP so customers can see that a product is certified and not need to look into the details of the ST to know that the baseline requirements are covered. [Thrasher]
- The original intent of PPs is that customers write the PPs to represent their requirements, and then vendors write STs that demonstrate that the requirements are fulfilled by their product, and evaluators independently test the ST and the product. As we are in a sense representing customers by writing a PP, I guess we need to put in the PP whatever the customers have been demanding.
- How are we going to validate it? [Nevo]
- Yes, if we agree that it must be in the PP, then what to we put in there and how can it be validated?
- This is a matter of specifying what shouldn't happen, a negative requirement [Kurth]

- We're specifying network-fax separation [Wright]
 - It's still a negative requirement. In CCv3.1 there is a new ADV requirement but it is not complete, and there is discussion about how to introduce those concepts in the next version of the CC [Kurth]
- A similar problem exists in firewalls, where there is an inner network and an outer network. [Kurth]
 - They use flow controls in firewalls [Aubry]
 - Yes. The firewall is a simpler case because it is a direct information flow. Indirect flow through filtering rules is still allowed [Kurth]
- If a vendor wrote a claim that they have fax-network separation, would it be validated by penetration testing? [Cybuck]
 - You'd also need to look at the code to see if there is a trap door [Kurth]
 - At EAL3? [Cybuck]
 - We would look at the design, not the code, and then design a penetration test for that design. [Kurth]
- We don't necessarily need to make a threat, and its difficult to write it because the asset is not easy to define, so if we don't have a threat, can we simply insert an assurance requirement in the PP that addresses this?
 - You still need either a threat or a policy and an objective, and evaluation is done against the objectives. Objectives should also be considered when doing vulnerability assessment. If you find a vulnerability, then you look at whether the attack effort is consistent with the EAL [Kurth]
- If we have an objective, can it be satisfied by an SAR without any SFRs?
 - You need to have some SFRs, even if they are just management SFRs [Kurth]
- The approach that we've tried {in 36c} uses management functions to turn on or off connections if those connections can possibly exist.
 - That is too simple, and that is also the problem using flow control, because you'll want to have some flow from one interface to another. You don't want to to prohibit useful functions [Kurth]
- There is a US PP for firewalls and they have an objective O.MEDIATE and they use flow control. Is our case similar? [Aubry]
 - I will look at that. You have to be careful because you don't want to close flows that are useful. In most cases, I've seen these better expressed as discretionary access control. [Kurth]
 - We got a comment from NIAP that they did not like our use of flow control for that purpose.

- Our current policy is general enough to cover many interfaces, not just fax modems, so there should be some case in which the SFR can be fulfilled, but we don't want to make it so general that someone could allow exactly what we are trying to prevent.
 - That is the challenge, to express what you want to allow and what you want to prohibit [Kurth]
- Does NIAP have these same views on these matters? Can we get their help? [Thrasher]
 - NIAP is undergoing a lot of changes, and the people writing things are fairly young and they rely on the evaluators who are more experienced [Kurth]
- I think we can find a way to express this. [Kurth]
- I think we agree at least that we are stuck with addressing this issue and work on a solution before the Camas meeting. It is more difficult than addressing it in an ST because we are trying to put it in the network package, because it is a threat against the network and not against the fax, but do so without implying a requirement that the fax function exists; and we are also trying to express it in a way that does not impose a TSF requirement in cases where the product architecture might prohibit fax-network connection.

Protection of NVS discussion [Smithson]

Refer to document:

<http://grouper.ieee.org/groups/2600/presentations/Longmont/no-offline-salvage.pdf>

- Another customer-driven requirement has been to protect data from being susceptible to disclosure in cases where the hard disk has been removed from the TOE. Originally it only applied to deleted document data, but it has been expanded to include live data and not just document data.
- Until recently, we had used FDP_RIP to require overwrites of deleted data and FCS_* to require encryption of live data. We found out that FDP_RIP would not be satisfied by overwriting data, and we had left all of the parameters of FCS_COP open which made it somewhat meaningless.
- The current approach is to treat sending data to a nonvolatile device that could be removed as “exporting” data. The problem is that the SFRs refer to transmitting data during the export process, and we have used those SFRs in a way that equates “transmission” with “storage” and equates “exporting” with storing in a device that might be removed sometime in the future.
- The fundamental problem is that the CC does not provide SFRs for protecting against threats that occur in the future and when the TOE and TSF are powered off.

- Nonetheless, customers seem adamant about this requirement, and that was confirmed by a recent conversation with DAPS.
- None of the PPs or STs for operating systems address this issue, they rely on the environment to protect disks from being removed [Kurth]
- FDP_RIP is designed to protect, for example, the content of one job from being accessed by a subsequent job. That is the same way it is used in operating systems, the data from one completed process is not accessible by a subsequent process [Kurth]
- There are different ways to protect against offline salvage that do not require encryption. Some devices won't give up data unless they are provided with a key. [Kurth]
 - Like an access control [Nevo]
 - Yes, if you have a generic confidentiality requirement then such a device would satisfy the requirement. But it may not be acceptable to the government. [Kurth]
- There are devices that encrypt the data themselves. [Wright]
 - If you used one of those devices, it would need to be separately certified because to certify it yourself you would need access to information that you probably can't get from the vendor. I don't know if any of them have been certified [Kurth]
- There are two kinds of disk drives, one that uses a key to access data but does not encrypt on the platter, and the other also requires a key but the key is used for decrypting the data. Can those be considered to be similar from the PP point of view?
 - Whatever is done by the device must be considered to be part of the environment, so you would need to make that the requirement of the PP and if you perform the encryption yourself then you would add those SFRs to your ST. [Kurth]
 - I don't think NIAP would accept leaving it to the environment [Nevo]
 - That is how operating systems do it today [Kurth]
 - I can see NIAP complaining if we draw a dotted line around the TOE but exclude the disk drive.
 - It is not a problem if it is in a protected environment, but if the storage device is intended to be removed, then either the printer must encrypt the data or the protection must be done by the device, it is the responsibility of the ST author [Kurth]
- So you need a separate package for the removable storage device [Nevo]
 - The NVS package only addresses removable devices now. The definition of "removable" is a question.

- The concern is that if I use a standard disk drive that will work in a PC, it doesn't matter if it is made to be removed or can easily be removed with four screws [Thrasher]
 - This depends on the assumption you make about the environment. [Kurth]
 - I don't think we can make that assumption [Wright]
 - We already do make that assumption. If someone can access the MFP to remove a disk drive, then they could do many things, and all bets are off.
- There is a different case, in which the MFP is being decommissioned or redeployed. [Thrasher]
 - That's a different matter, it could be solved by a full disk overwrite, or degauss, or physically destroy, we aren't addressing that in the PP. We're addressing the situation where data is sitting on the disk in between jobs or after hours.
- It sounds like if we are going to address this case, and if we want to be able to use self-contained protection in devices, then we'll need to assume it is handled by the environment, and for cases where the TOE performs the protection, then provide app notes to instruct the ST author to add SFRs as needed.
 - But app notes do not force anyone to do anything [Nevo]
 - It will prompt the evaluator to ask how the ST author is addressing the matter.
 - An app note can force the ST author to address the problem in some way. [Kurth]
- So are we going to address this issue in the PP?
 - We need to put something in the PP about offline salvage, without saying offline salvage [Nevo]
 - If we say that the NVS package must be used for removable storage, then it makes it more clear why we are using "export" functions.
- It moves the issue of removable to the ST. But what is "removable"? What if the customer engineer can remove it? Is that removable? [Wright]
 - Don't say removable, just talk about nonvolatile storage [Nevo]
 - So if you have a small flash memory on your controller card, and it's nonvolatile, you'll need to encrypt it?
 - If it stores data that we have defined in the PP, then you need to protect it. [Nevo]
 - The way it is written now, the device must be "practicably removable by an unauthorized person". And we did not define exactly what data, so it is User Data and TSF Data.
 - If you extend it to every storage device, then it really applies to every storage device [Kurth]

- You have to define what is the valuable data and protect it in any device [Nevo]
- An E²ROM that stores configuration data? [Kurth]
- That could contain valuable data.
- But if you can't rely on the physical protection of the device, then encryption won't help because I can intercept the data before it gets to the device. [Kurth]
- We decided that we are not going to protect the internal communications [Nevo]
- What we do in an evaluation is look at whether the combination of threats makes sense. If you say there is a threat that someone can remove the disk, but you don't have a threat that someone can intercept the internal communications, we would wonder how that can be. [Kurth]
- We defined the attack as taking data off of the disk, not intercepting the data. [Nevo]
- But you could unplug the disk cable and connect the disk to your laptop and take data off the disk. It would be easier than unbolting the disk from the MFP.
- You need to rely on some assumptions of physical security. There are only a few devices that do not have that assumption. [Kurth]
 - Like smartcards. And even then, they only have a few tamper-related SFRs.
 - So if you have a physical protection assumption, you only need simple access controls [Nevo]
 - As long as you don't have any storage that is intended to be removed [Kurth]
 - And that's all we have now, access controls and confidentiality/integrity controls for network traffic.
- There is an assumption about the strength of the attacker and you mitigate the risk according to the strength of the attacker. You don't eliminate it, you manage the risk. [Cybuck]
 - It is combined with the EAL. If you look at the CEM, you look at the attack, make sure it doesn't violate an assumption, and then look at the effort needed for an attack, and if it is more effort than the EAL justifies, then you don't worry about it. [Kurth]
- So if the normal use is not to remove a storage device, then you don't need to worry about. But if the normal use is to be able to remove it, then you need to deal with it [Nevo]
 - But you can walk up with a USB memory [Petrie]
 - It is not part of the TOE [Nevo]
 - We need to distinguish between system storage devices, that are part of the TOE, and personal storage devices, that are not part of the TOE.

- You can make an assumption that personal storage devices are protected by the owner [Kurth]
 - That kind of device would not be part of the TOE [Wagner]
 - You have control of the USB interface, but not the device [Kurth]
- The package would be for nonvolatile storage devices that are removable in normal use [Nevo]
 - You could have an optional package for that [Kurth]
 - Or can it be an app note in the PP? [Nevo]
 - It is up to you, the vendors. If it is something that vendors will likely implement, then the package would help define how it is done and possibly define it for compatibility purposes [Kurth]
- Let's consider the case of a physician who has patient records on a printer that he leases from some IT provider, and the IT provider replaces the printer. Is the physician responsible for that? It is OK to say that the TOE Owner is responsible for handling it, but as a practical matter the physician won't know how to wipe the disk. [Wagner]
 - Wiping the disk may not be an option, because if the printer is broken, then the disk wipe may not be available for use. The only thing that helps is for the physician to have a contract with the IT provider to assure that the disk won't be reused if the device is replaced, and that is how it is normally done [Kurth]
 - Don't you get a better feeling if the data is encrypted? [Wright]
 - Yes, but that is a feature.
- What is the problem of putting encryption in the PP? [Nevo]
 - If you want to sell to the US government, they will require FIPS 140, and that would be recognized by Canada, Japan, and the UK, but it would be a problem in other countries. So you need to leave the encryption SFRs open in the PP [Kurth]
 - If you have an ST validated in the US scheme that specifies FIPS 140, does it break mutual recognition? [Cybuck]
 - No, it doesn't break mutual recognition. And if you have it validated in Germany, you would still need to get the cryptography validated by a FIPS 140 lab. FIPS 140 must be done regardless of CC validation. The difference is that NIAP will not let you make a statement about cryptography in your CC validation unless it is also FIPS 140 evaluated [Kurth]
 - It is not a NIAP requirement, it is a US government requirement [Thrasher]

- Yes [Kurth]
 - What if you are getting a product validated for non-US-government use? Would NIAP still require FIPS 140? [Thrasher]
 - At this time, NIAP is doing work for US government consumption. If they did one for another customer, they might lift the FIPS 140 requirement [Kurth]
- The SFRs in the FCS class are not intended to require encryption; they are intended to require how you do encryption.
 - For that reason, they are more specific than most other SFRs. [Kurth]
- Conclusion? [Farrell]
 - We have several issues to deal with: (1) what is the definition of “removable”, and (2) how to specify the protection, either as a specific implementation like encryption or as a more general requirement like confidentiality.
 - We would put an app note about FIPS 140 for NIAP but leave it to the ST author? [Cybuck]
 - At the moment we don't have any FCS class SFRs, we are using data export SFRs that require confidentiality, and we could put an app note that says typical implementations use encryption, FIPS 140 may be required for US government sales, and some customers also want overwrite, see DoD or other standards for that.
 - We will try to make the NVS package more understandable and make the scope more clear.
- Currently, the NVS package is applicable to environments A, B, and C, but I think that in the public environment, requiring NVS doesn't really enhance security. It's a nice feature, but the user is really depending on the trustworthiness of the system administrators because they could turn off the NVS protection. So I propose that we limit NVS to environments A and B.
- So we'll limit the scope to removable media, but leave it to the ST author to specify what that means? [Sukert]
 - You'll need to say that any device that is intended to be removable must be protected, and leave it to the ST author to demonstrate how they do that [Kurth]
 - The ultimate objective is to protect user and TSF data, and in many cases you'll want to rely on the environment for that, and you should set a minimum requirement in the PP author and let the ST author do more if they wish [Kurth]
- You'll include overwrite in the requirements? How will you do that? [Sukert]

- I think that in the previous drafts, we required encryption and overwrite in A and B, and only overwrite in C. But we don't have a way to require overwrite, and as I said, I don't think it makes sense to require NVS in environment C.
- That's in conflict with the 2600 std. [Thrasher]
 - We'd need to change the objectives in the compliance clause from "shall" to "should".
 - We'd also need to change the description of the environment. It says that one of the security expectations is that documents are protected from disclosure of residual information after completion of jobs [Thrasher]
 - That's residual information protection, you already have that in the PP [Kurth]
- {agreed to remove NVS package from PP-C}
- If an MFP has a disk drive that is mounted with screws, is it designed to be removed or not? [Aubry]
 - That depends on the assumption of whether someone can approach the MFP with a screwdriver or not [Kurth]
 - We have an assumption about protection of the environment, and to make a threat about removing an internal disk drive contradicts the assumption.
 - But we all have disk drives like that and we still have encryption or e-shredding. Customers ask for that even for disk drives that are not externally removable [Aubry]
 - The ST author may always do more than the PP. By adding encryption for the internal disk drive, you could lower the requirement for environmental protection [Kurth]
 - For our customers, if the disk is removable then they don't ask for e-shredding because they take the disk and lock it up [Aubry]
 - After business hours, the environment is not so well protected [Thrasher]
 - But if the disk is intentionally removable, then it increases the risk that someone will grab it and take it away [Kurth]
 - If your hard disk is removable, you should have guidance to the user that the disk drive should not be removable by unauthorized personnel and that if it is removed for storage it must be locked up for protection [Kurth]
- So vendors can still apply the NVS requirements even if their device isn't designed for removal, and that provides a standardized way to conform to customer demand that internal disk drives are protected.
 - But if it is not part of the PP, and a vendor uses encryption, then the encryption is not subject to evaluation? [Wagner]

- No, if you make a claim that is supported by encryption, then the encryption would be evaluated, and if you are selling to the US government, then it would be subject to FIPS 140 [Kurth]
- This is a function and capability that every vendor does, at least in some of their products, but we are trying to avoid putting it in the PP [Thrasher]
 - There is a difference between having a feature in the product and having it certified, and we are having a lot of trouble defining it is a requirement.
- {overall conclusion: written proposals to be sent to mailing list for discussion and agreement between meetings}

P2600.1/2/3/4 Comments review [Smithson]

Refer to comments:

http://grouper.ieee.org/groups/2600/comment-tracking/P2600_2008_06_v01.pdf

And comments with resolutions:

http://grouper.ieee.org/groups/2600/comment-tracking/P2600_2008_06_v03.pdf

And to the PPs:

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.1-36c-proto.pdf>

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.2-36c-proto.pdf>

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.3-36c-proto.pdf>

<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.4-36c-proto.pdf>

- {some comments were related to the NVS and SMI packages; these were deferred pending proposals and decisions about those packages}
- {most other comments were not controversial, see the resolution document for details}

PP Guide ad-hoc status [Sukert]

Refer to

document: <http://grouper.ieee.org/groups/2600/presentations/Longmont/PP%20Guide%20Outline%20v1.1.pdf>

- Held status meeting on Jun 18th:
 - Based on latest PP restructuring proposal we have enough information to start all Guide sections
 - Assigned specific chapters or sections to team members (see Revised PP Guide Outline for assignments)
 - Still would like Atsec feedback on PP Guide outline
- Current Plan
 - Create extended outline for all sections by Jul 4th
 - Provide completed text for posting and review at Aug P2600 Meeting by noon Jul 28th
 - Will try to have as much as we can by then

Schedule proposal [Smithson]

Refer to document:

<http://grouper.ieee.org/groups/2600/presentations/Longmont/schedule37b.pdf>

- {new schedule was proposed, discussed, and approved}

Next meeting details [Wright]

Refer to meeting slides for

detail: <http://grouper.ieee.org/groups/2600/presentations/P2600-Jun2008.ppt>

and to the meeting web page for most current status of upcoming meetings:

<http://grouper.ieee.org/groups/2600/meetings.html>

- P2600.1/2/3/4 PPs are under change control
- Deadline for posting documents: July 28 2008
- Deadline for posting comments: August 4 2008
- Next meeting will be August 11-12, 2008
 - Sharp Labs of America
5700 NW Pacific Rim Blvd.
Camas, WA 98607
 - No hotel block
 - PWG will meet at the same location August 13-15.

Production Printing environment/PP update [Lewis]

Refer to

document: <http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/P2600.5-36c-proto.pdf>

- do customers want security?
 - mostly PCI compliance
 - nothing shown at Drupa
 - but the same could have been said when we started P2600
- what is prod printing?
 - heavy-duty cut-sheet?
 - variable data / trans promo?
- does trans-promo get content feeds from outside, which adds new attack paths? [Smithson]
 - to some part of the workflow, not necessarily to the printer itself
- how applicable are P2600 things to prod printing? [Volkoff]
 - there are uses, logging, communication
 - there is audit logging; usually closed networks; operator is more of a combined user and admin; trust of personnel is more important; a lot of the threats are similar, and security issues are getting more attention [Sukert]
- is it better to come out from AFPC or IEEE? [Volkoff]

- might get more attention from the industry if from AFPC, but then it would be reinventing the wheel
 - but it would be efficient to create a subset of one of the existing PPs
- production printing is usually in a protected environment, similar to the PP-A environment [Petrie]
 - you cannot use it because you need to remove user identification and authentication [Aubry]
 - the operator must log in [Petrie]
 - there is no protocol in IPDS for that [Aubry]
 - it is between the printer and the print server, and the operator logs into the print server
 - this is where the AFPC might help
- is there a distinct environment for production printing? [Wagner]
 - at least one, maybe two
 - it is a manufacturing environment; the printer itself is a high value asset
- if you have a printer that is not connected to an external network and it is in a protected environment, where is the threat?
 - The operator is a threat, but also there are management interfaces from external networks
- If you have advertising merged with phone bills, where do the ads come from? Are they from outside? [Thrasher]
 - They are cached internally, you could not keep up with production printing speeds if you needed to go outside to retrieve ad content
- Our customers want is to show that the print flow is secure and not connected to management interfaces, and that print data is deleted after the job is completed [Aubry]
 - Does this warrant a PP?
 - It would be better to do a PP for the print server, but that is out of scope for this group [Aubry]
- I think that at least the P2600 std should be expanded to include a production printing environment compliance clause, even if we do not have PPs [Sukert]
 - Expanding the P2600 would require definition of the environment, adding assets or threats, etc. [Thrasher]
 - I did a first cut of that a while ago [Sukert]
 - It is still posted on the web site [Smithson]
- We need to decide, sometime, if we should open a new PAR for this work [Wright]
 - What is the situation with that?
 - If we want another PP, we need to make a new PAR. Also, if we want to expand the 2600 standard, we need a PAR for that. [Wright]
- Where would this PP get validated? [Thrasher]

- It is frustrating that we are having problems getting schemes to accept our PPs.
- NIAP said they can only do one PP this fiscal year [Smithson]
- We could hire atsec again and have them get it done in Germany [Sukert]
- There is advantage of having NIAP validate it and put “US Government PP” on the cover [Thrasher]
- It means that they not only validated the PP, but they consider it to meet the requirements of the US government [Smithson]
- If we did a production printing PP in the P2600 group, would it be the same group of people? [Volkoff]
 - Some of them.
 - I can't see Lexmark championing this, so it would need a new chair [Wright]
- If it is done in AFPC, we couldn't use the content from the P2600 PP work because of copyright
 - Also, P2600 WG has built some experience that would be useful; not to repeat the same mistakes [Smithson]
- {conclusion: those companies who are interested must take the lead in gathering consensus and proposing the project}

Closing [Wright]

*** Adjourned at 3:35 PM MDT (11:35 PM CEST!), 6/24/2008 ***