

**IEEE P2600 Meeting #6
October 7-8, 2004
Lexmark, Lexington KY**

Attendees

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

Lee Farrell / Canon
Brian Volkoff / HP
Satoshi Fujitani / Ricoh
Jerry Thrasher / Lexmark
Jean-Claude Longo / Océ
Daniel Manchala / Xerox
Bill Wagner / NetSilico
Peter Cybuck / Sharp
Harry Lewis / IBM
Yusuke Ohta / Ricoh
Takanori Masui / Fuji-Xerox
Liang Zhao / Epson
Ron Nevo / Sharp
Tom Haapanen / Equitrac
Nick Del Re / Canon
Nancy Chen / Okidata
Ben Arazi / university professor

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 10/7/2004 *

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-Oct2004.ppt>

IEEE patent policy

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Oct2004.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-Oct2004.ppt>

Review of officers

Mr. Deschrijver has resigned as Secretary. Lee Farrell moved to accept the resignation, Jerry Thrasher seconded. Vote by hands: unanimously accepted.

Entertained nominations for Secretary: Brian Smithson nominated himself. No other responses. Vote by hands: unanimous approved.

Meeting schedule update

Sharp confirmed for February 2005 meeting in Camas, WA. Still looking for a host for April 2005 in Tokyo.

Discussions at PWG resulted in potential swap of January and February meetings. Could Sharp host the meeting in January (which would be for the whole week – they would also host PWG)? Peter Cybuck said that Sharp would look into the matter.

Meetings in May and beyond are listed on the slides

<http://grouper.ieee.org/groups/2600/presentations/P2600-Oct2004.ppt>

TCG update

- Conference call was held on 9/16/04.
- Don Wright made a request on 10/2 to establish a liaison relationship between P2600 and TCG
- First official conference call will be 10/18 at 10am (pacific time)
- Next TCG member meeting will be 11/9 – 11/11/04 in Phoenix AZ
- Is there a concept of an “observer”, e.g. a member of TCG but not of a particular working group, who could access working group info? [Thrasher]

- Yes, you can put in a request. Companies can have only one voting member, but any number of observers [Volkoff]
- Any employee of a member company can join/leave working groups, just make a request. [Wright]

Action items from previous meeting

Refer to slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Oct2004.ppt>

TCG items complete.

Meeting 6 setup complete.

Section 1 items complete.

Section 2:

- Threats review complete.
- Categorize, short/long descriptions, and mapping to security environments: in progress, needs group discussion [Haapanen]

Section 3 items in progress

Section 4 items in progress

Content of standard [Wright]

Sec 1 Introductory material

Sec 2 Vulnerability/Threats/Exploits

Sec 3 Directives/Best Practices

Sec 4 Protection Profiles / Security Target Templates

- Changed from previous categories to new ones that are aligned with NIST Security Checklist document

As we pull this document together, we'll need an overall editor. We now have four documents, but need to start thinking of it as one document.

Section 1. Introductory Pages [Wright]

Reference materials

- Bibliography and Reference sections need to be reviewed and reconciled – which ones are references and which are not. Also need to include items that are being identified in Section 3 and put them here.

- Have a list of terms and acronyms now, but need to go through the document and pick out others. If you know of some that should be included, send them to me.
 - I have a document of 50 pages of terms and acronyms, I'll look for softcopy. [Thrasher]

Security environment

- Section 3 comment: identifies functional environment security, but it seems like that's already been done here in section 1 (1.3.x)
 - Was intended to correlate, not identify [Wagner]
 - Does it specify detail on hardcopy issues in those environments? [Wright]
 - Yes, to ensure correlation, if needed, provide more detail [Wagner]
 - It's an around-and-around process between the sections [Wright]
- Security Environment information has been based largely on NIST 800-70.
 - New version has come out. [Thrasher]
 - Has anyone reviewed? [Wright]

SOHO env

- Token Ring is mentioned in SOHO, is it appropriate to leave in?
- We still see TR out there [Volkoff]
- Wireless is more of a concern [Wagner]
- Will take out TR, put in 802.11 and PNA [Wright]

Enterprise env

- References to security publications: do any of the vendors have whitepapers that could/should be referenced here? These would need to be available on a more or less permanent basis (no response)

High Security env

- Same diagram as Enterprise, except more detail, internal firewalls, PKI servers

Custom env

- Needs a lot more work
- NIST had an example of a wireless system in a warehouse, which we removed. Instead, we used public library and public access hardcopy devices
- Also included "legacy" environment from NIST, which includes older systems like Win98 and (recent announcements from MS) Win2000 clients

- Should include legacy hardcopy devices also? [Wagner]
 - Yes, we should address that too [Wright]
- How much do we want to put in the “custom” space?
 - Public library is good [Wagner]
 - Legacy? [Wright]
 - Yes, many people start with that [Wagner]
 - One point of view would be to include all of the legacy protocols that collectively our hardcopy products support? [Smithson]
 - Turn them off [Wagner]
 - That’s one way, and we could say that in this doc [Smithson]
 - Also interior firewalls [Wright]
 - How about college campus? [Lewis]
 - Could be Enterprise [Wright]
 - Much more aggressive users and uncontrolled devices [Thrasher]
 - Wouldn’t want to mix it in with Enterprise, because of that [Lewis]
 - Will add it as Custom [Wright]
- Better to use Internet Café as generic term for “high tech coffee shop” [Wagner]

About the examples we use:

- We have two financial examples in Enterprise; might want to change one of them
- How about healthcare? [Nevo]
 - Like a doctor’s office, in SOHO? [Wright]
 - That could be one, but also need hospital or insurance [Nevo]
 - We have SOX and GLBA examples, need HIPAA [Thrasher]
 - Will add hospital or insurance in Enterprise, and medical clinic in SOHO, also Production Printing in Enterprise [Wright]
- Need someone to review/update the diagrams
 - Someone with the tools and talent
 - Consistent, non-vendor graphics (like the ones in the NIST doc)
 - Correlates with document content
 - We have some tools and access to the people who created the NIST document [Cybuck]
- I’m interested in how this can apply to production print environments; would the group be interested in my focus on that? [Lewis]
 - Would be appropriate, as an Enterprise env? [Wright]
 - Might be Custom, or High Security [Lewis]

- We have a local DA's office, how about Social Security or such? [Nevo]
 - Both are public sector [Wright]
 - DA is local, SS would be covered by Federal guidelines [Wagner]
 - Federal customers might be an audience of this document [Cybuck]
 - Will add something federal, like SS office, IRS office, or Army Recruiter [Wright]
 - We could go on and on with examples... [Lewis]
 - We should choose examples that are most likely to be looking at this document for guidance [Cybuck]

Section 2. Vulnerabilities/Threats/Exploits [Haapanen]

Refer to <http://grouper.ieee.org/groups/2600/presentations/lexington/Section2issues.ppt>

All other sections have been depending on this one. Goal is to have a list of threats in categories that aren't going to radically change during the development of this document.

Began with the original vulnerabilities list of 200+ threats from 2nd meeting. Latest revision combined items, cleaned up descriptions, cross-referenced to the original list, and started including threat details. Uses Smithson's model of threat vectors.

Refer to <http://grouper.ieee.org/groups/2600/presentations/lexington/Section2threats2004-10-04.doc>

Issues for group discussion

What are agent roles?

- Brian's document had insiders, outsiders. Some others had good/evil :-). What information is essential to be conveyed here?
- One question to answer is: do we list all likely agents for each threat? [Smithson]
- Example: anyone could do EM sniffing, but who would have a real motive? [Haapanen]
- Also consider if someone is trying to attack the device or use the device to attack something else [Cybuck]
 - That was the direct vs. indirect outcome dimension [Smithson]
 - Yes, this attack allows you to make another attack [Haapanen]

- We should declare out of scope anyone authorized to do something doing something they shouldn't be doing [Wright]
 - So a service person removing a hard disk wouldn't be considered? [Haapanen]
 - They're supposed to remove a hard disk. You could say that the hard disk is supposed to be erased before its removed. [Wright]
 - You could say he is authorized to remove the disk, but not authorized to read its contents [Thrasher]
 - Approach I took was to look at agents in terms of what they were authorized to do [Smithson]
 - Anyone who removes the hard disk is a threat, but there may be some cases where you can only attack if you're authorized to do something [Haapanen]
 - Depends on if the attack is defined in terms of what you're authorized to do, like if you're authorized to print B&W but not color, then if they figure out how to print in color, then it's a threat. Is the authorization specific to the individual or role, or to the task being done? [Wright]
 - I think we need to flatten this to less than four dimensions [Wright]
- Back to what we're trying to get out of this, for example, what are you going to do with this information in section 4? [Haapanen]
 - Categories will help answer this question [Nevo]
- Reason I chose the dimensions I did was that, for example, if a normal user can look at their job status and it also shows them information about other jobs, like filenames or URLs or email subject lines, then by giving them access to job info so they can look at their own, you've perhaps unintentionally given them access to other's info that they don't need to know. That's why I used a role-based agent definition, so you could look at what they can do versus what they should be able to do. [Smithson]
- Inside vs. outside, what did that mean? Organization, or building? [Haapanen]
 - Inside or outside of the organizational structure [Smithson]
 - Cleaning staff could insert a laptop with 2 NICs and slide under the MFP for a man-in-middle attack. Inside the building, outside the organization [Haapanen]
 - That would be inside because of physical access [Longo]
- What about inside/outside network, if a firewall isn't correctly configured then someone outside the firewall could get access as though they were inside, do we consider that? [Haapanen]
- How about good/evil? Does it make a difference? [Wright]
 - Was intended tongue-in-cheek [Haapanen]

- Maybe this agent thing comes into play only when needed. Example: using electron microscope to examine the drum. [Haapanen]
 - Sophistication of role isn't in there [Wagner]
 - NIAP uses skilled vs unskilled. Skilled vs unskilled comes in to the PP [Cybuck]
 - In the CC they have three expertise levels: layman, proficient, and expert. They also consider equipment: standard, specialized, and bespoke (not readily available to the public). Not necessary to use in this level of PP, but useful to consider. [Ohta]
- Should we use expertise and equipment instead of agent roles? [Haapanen] (generally agreed)

Intentional vs. other?

- "Intentional" was voted on 3:1 by the subteam
- Accidental things could be done intentionally [Wagner]
- For it to be a threat, you'd need to take advantage of it intentionally [Smithson]
- Agreed [Haapanen]

Naming scheme

- Should use a "T" to start [Smithson]
- PP groups them together, and this scheme should work [Ohta]
- Assets aren't at the top of the hierarchy? Access is closer to what we would countermeasure.

General network issues: address them or not?

- Should we consider things like ping floods, applicable to all network devices and not just hardcopy?
- (generally agreed)

Inbound and outbound attacks?

- How about outbound threats, like using an open email relay?
- (generally agreed)

How broad or specific?

- Example: deleting resources with PDF, PjL, mgmt tools
 - Seems like that's asset-oriented [Smithson]
 - We put everything in the printstream as one item, and mgmt tools as another [Haapanen]

- Read vs modify/delete?
 - Some PPs have four: access, modify, use, and abuse. They are very asset-oriented. [Thrasher]
 - Countermeasures could be the same [Haapanen]
 - Not always. To protect against access, I would encrypt. To protect against modification, I would need to do a message digest. [Thrasher]
 - What the man-in-the-middle intended to do with the data could determine how much you want to protect against it [Wagner]
 - Those are the outcomes. I had five: disclose, alter, interrupt, destroy, and use, but those map into the four pretty well. I think it's important, too. [Smithson]
 - We'll represent it in the "outcome" category [Haapanen]

Top-level category discussion

- Sharp has a proposal for categories [Cybuck]
 - Refer to
<http://grouper.ieee.org/groups/2600/presentations/lexington/SharpCategories-preliminary.ppt>
- List of threats in the PP should be short, like a dozen or so. I also noticed that in many PP's, the threats are described with a verb – neither asset-oriented nor access-oriented. Also, the number of threats we'll use in the PP is a subset of those that need to be dealt with in the P2600 standard. [Smithson]
- Some of this list is asset, some is access [Wright]
- (informal vote on asset top level vs access top level – inconclusive)
- I think we should concentrate on assets. The law we're trying to comply with is the protection of confidential information, which is the asset [Thrasher]
- Some threats don't include the asset, like man-in-the-middle [Nevo]
- That's a threat of data access or data modify [Thrasher]
- Or if it's an external asset, that can be considered too [Smithson]
- Another way to think of this is that if there isn't an asset, then there's no need for securing it [Smithson]
- Anyone want to make a case for access or something other than asset? [Wright] (no response)
- Number of threats would be smaller with assets [Haapanen]
- I think the matrix would be the same, assets X accesses [Thrasher]
- They might combine to a smaller number [Smithson]
- It might be more optimal to think in terms of access, for example if you had a locked door, fence, razor wire, and surveillance cameras, which is the access, you could apply that to a house, office, or prison, which would be the asset, so I think gets down to an access control. We're going to need to think of an asset in an environment. [?]

- Those would be different ways to mitigate a threat. The threat is the same. [Wright]
- It's easier to do it this (Sharp) way because it's obvious what to do, like T.NETWORK means you need to protect from the network. [Nevo]
- But your proposal is neither asset nor access, it's both. Do you just pick and choose which way you want to go when they fit in more than one category? [Wright]
- If it's specific to an application, it goes under one of those (scan, fax, etc), if it's the network then it goes under network, if it's user data then it goes under data. [Nevo]
- Have you mapped these threats into your proposal? [Wright]
- No [Nevo]
- I'd like to propose that we try to map threats into something like this [Ohta]
- It's important we decide on this today [Nevo]
- Can we try to do it right here as a group? [Wright]
- One difficulty is that we'll make a committee decision looking at the pieces, but will turn out to be difficult to implement in practice. I think to really deal with this, one needs to look at this holistically and see what patterns emerge. [Smithson]
- (mixed discussion)
- (Ohta distributed a draft category scheme)
Refer to
<http://grouper.ieee.org/groups/2600/presentations/lexington/RicohCategories-preliminary.txt>
- Agreed to work on this in three groups tonight, and review/decide tomorrow: Sharp group, Ricoh group, Section 2 subteam

Individual threat review discussion

Refer to

<http://grouper.ieee.org/groups/2600/presentations/lexington/Section2threats2004-10-04.doc>

- N.T.IP.DUP is the same as N.T.IP.DNS? [Smithson]
 - No, different technique, different outcome [Haapanen]
- N.T.S.DOC different from N.T.S.CRED because outcomes are so different
- N.P.LOOP same as N.P.CRASH? [?]
- N.P.CHANNEL could be PDL or IPP
- N.P.PRIORITY is same as denial of service? [Wagner]
 - Too generic [Wright]
 - How to mitigate? [Thrasher]
 - Like OS scheduling [Haapanen]
 - Sometimes server policy [Wright]
- MI.FAX capture/intercept and forward unchanged is essentially the same as sniff [Wright]

- M.C.IMAGE combined with SETTINGS
- M.C.SECURITY distinct from other settings because they open other holes. Should keep separate?
 - Yes [Wright]
- M.DATE same as SETTINGS? [Wagner]
 - Yes
 - May be important because of SSL certificates [?]
 - Not just FAX, so let's leave it in
- M.FW.APPLET depends on what the sandbox allows; M.FW.UPDATE can do anything the machine can do
- M.ID.AUDIT should be same as SETTINGS? [Thrasher]
 - Doing so, you loose the ability to prioritize protecting this [Wagner]
 - Combined with SETTINGS
- M.ID.SPOOF same as N.IP.DUP
- F.MOEBIUS was a joke, could be a simple loop of paper
- What about connecting to a FAX with continuous negotiation? Wasn't that in the list before? [Wright]
 - Or keep throwing it into retraining mode [Smithson]
 - Added back into the list
- What about IETF FAX?
 - Special kind of print job [Wright]
 - Has special protocols that can be screwed up. Complex negotiation, also [Wright]
 - Can you provide examples? [Haapanen]
 - Will make a note about it [Wright]

Section 3. Directives/Best Practices [Thrasher]

This section is about how to address hardcopy issues of security in the identified environments.

For the threats identified in section 2, how to address them? [Wagner]

First section: what's unique about hardcopy security in these environments. Legislation, industry guidelines, directives, etc.

All that stuff is in the June meeting, there was work already done, look on the web site for links [Wright]

Next section is architecture considerations. General kinds of things to think about from an architecture standpoint.

Security features/techniques

- Physical security. Should be limited to device.
 - Should declare building/room security out of scope and provide a few references, like NIST or ASIS [Wright]
 - Isn't the audience different? Manufacturers for architecture, customers for building/room security [Smithson]
 - Yes, the document is for both audiences [Wright]
 - Did you include camera viewing of documents (from outside device)? [Wright]
 - Also viewing console, like "shoulder surfing" [Smithson]
 - They are different, add both [Wright]
- Authorization and access control
 - Should be authorization, not access control? [Wagner]
 - OK
 - What about using LDAP or other external servers for walk-up access? [Haapanen]
 - Also recommending against use of fixed/unchanged passwords for service, etc. [Smithson]
 - Some use SMTP server authentication also [Wagner]
 - And one-time passwords [?]
- Usage logs and audit trails
 - Need more on this
 - There are examples in BITS reference
- Stored data protection and disposal
 - New version of DOD 5220 is being done at NIST. Old one was done in the 1970's
 - Also consider degaussing using xray or UV techniques? [?]
 - I don't want to reference standards (in German or Russian) that haven't been reviewed by someone who can read them [Wright]

Threat mitigation recommendations

- Nothing in there yet. Intend to have a threat matrix or description of recommended mitigation techniques
- Differentiate between manufacturer action and customer action [Wright]
- Sec 2 will identify threats and in what environments they apply, so Sec 3 will reference the threat and describe mitigation [Wagner]

References

- Needs to be moved to bibliography or reference
 - I will do that [Wright]
- Everything from FISMA and beyond is referenced in the document. Others are NIST documents.

Will need to assign some sections to people before the end of the meeting tomorrow.

Section 4. Category proposal review [various]

Ricoh [Smithson]

Refer to <http://grouper.ieee.org/groups/2600/presentations/lexington/RicohCategories.xls>

- First we looked at indirect threats, and CC has a slightly different category for those: TSF (TOE Security Function threat) which simplifies things. TOE includes documents, physical assets, direct threats to things we're trying to protect. TSF includes threats to those things that are there to secure the TOE assets. There's a diagram from the CC in our proposal.
- T.DOCUMENT contains documents (in process, not residual), regardless of how they're accessed
- T.SALVAGE contains documents in residual form, removing disk or examining drum
- T.USERINFO contains job info, user IDs, email, phone numbers, everything except passwords
 - Changing the address book shouldn't have been in this category, it's a T.DOCUMENT
 - Question about MI.MGMT, I think it belongs here, but I wasn't sure
- T.RESOURCES has to do with consumables and use of the device. Use includes unauthorized use and also using the device but avoiding accounting
 - Items in (parens) I think were deleted from Tom's list
 - M.SERVICE was deleted, also M.WEB [Haapanen]
- T.SERVICES is use of the MFP by authorized users, includes denial and impediment of service
- There are three TSF
- T.TSF.SOFTWARE includes applets and full firmware
- T.TSF.PERMISSION includes security settings, regular settings, and obtaining credentials by any means, which in themselves don't do anything but can be used to effect a direct threat to something
- T.TSF.AUDIT is for covering up security events or avoiding accounting
- P.DISK can also retrieve scanned data, which isn't residual, and that would be under T.DOC [Masui]
 - I agree, should fall into document category. Also didn't include other kinds of media like flash or RAM [Cybuck]
- Management data should be under USERINFO as a subcategory [Nevo]
- Government people want to know about threats to environment, so that should be a separate category [Nevo]

Sharp [Nevo]

- T.USERDATA
- T.USERDATA.MGMT, can have some categories underneath
- T.MFP or T.DOS for denial of service
- T.OS or could be T.SOFTWARE for applets and firmware
- T.IT or T.ENV for environment
- So salvage would be under two headings, T.USERDATA and T.USERDATA.MGMT [Wright]
- Main reason we didn't put management data under document was because it was a TSF, an indirect. Nobody cares what the IP address of the machine is unless you're going to do something nasty with it [Smithson]
 - The CC wasn't written with MFP's in mind [Cybuck]
 - We're not that different [Smithson]
 - We're trying to make a clear and understandable document [Nevo]
 - We're also trying to follow the conventions of the CC. By describing only the TSF threat and not what indirectly is threatened, you don't have to describe all of the possible outcomes of obtaining management data. Also, it lets you forget about data that really doesn't threaten anything, like accessing the system date and time off of an MFP. [Smithson]
- We didn't categorize individual threats in this scheme
 - We learned a lot by doing that [Smithson]
 - It forces you to look at each item [Haapanen]
- What about using a service like telnet to attack other devices? [Wagner]
 - There were threats listed for attacks on web server and attacks on other services, I don't know why they were different [Smithson]
 - We'll look into where that went. Was removed because it was a vulnerability, not a threat [Haapanen]

Section 2 group [Haapanen]

- Two-level hierarchy
- SVC contains NET, PRT, FAX, PHY, and IMP (network, print, FAX, physical, and impersonation)
- DOC contains SNIFF, PHY, RES, and INT (sniffing includes network, EM, phone; others are physical, residual, and integrity)
- SEC contains CRED, CONF, and AUD (credentials, configuration, and audit)
- What about external services? How to separate them out? [Nevo]
 - We need an understandable, readable scheme; there are many options [?]

Conclusions [Wright]

- Who cares except for the Section 2 and Section 4 groups?
- Breakout of the three proposing groups and let them decide

Section 4. Protection Profile [Nevo]

- Threat categories need to be changed again based on today's discussions
- Will environments be supersets/subsets?
 - Yes, except perhaps custom
 - I hope High Sec will be superset of all [Ohta]
 - Some assumptions about environments work in other environments
 - Even if not hooked to a network, same protection is needed [Ohta]
- Does residual data on RAM need to be protected? [Smithson]
 - CIA waits 72 hours before RAM is considered powered down [Cybuck]
- Are supplies and services not a concern of PP? [Wagner]
 - Not supplies, but yes services [Nevo]
- Procedurally, new or changed threats should go into sec 2 and then flow back into sec 4, we shouldn't change them here. Otherwise we end up out of sync [Smithson]
- Adding Flash with hard disk seems reasonable. RAM seems like a different threat if it is to be added at all [Smithson]
- Do "internal users" include those on the network from external location through VPN? [Manchala]
 - Yes
- What about the term MFP? P means peripheral, and these devices aren't peripherals anymore [Manchala]
 - MFD could be used [Nevo]
 - P could be Product [Smithson]
 - The term doesn't include non-multifunctions [Chen]
 - Should use a generic term for hardcopy devices; will add to section 1 [Wright]
- Some devices have maintenance ports, which can be custom connectors and not like regular serial ports [Wagner]
 - Will add that to the table [Nevo]
- Should removable hard disk be added to figure 2? [Manchala]
 - Yes [Nevo]
- What about installation issues? [Manchala]
 - Belongs in section 3 [Nevo]
- Assumption: can customer engineer be trusted? [Manchala]
 - Yes [Nevo]
 - These assumptions were based on my first draft, and I didn't consider customer engineer to be trusted [Ohta]

- If you install/configure system in high security env, someone from the organization oversees [Manchala]
 - That's an organizational policy [Cybuck]
- Net and non-network objectives
 - Should really have IT and non-IT env, according to CC [Smithson]
 - Is it necessary to have non-net? [Nevo]
 - No, not necessary [Ohta]
- 4.2.2.1 weak passwords, should refer to section 3? [Manchala]
 - Can't refer outside of PP because PP needs to also be a standalone document, but good point that we can't use a term that isn't well defined [Smithson]
- 4.2.2.3 assumes there will be a firewall? [Manchala]
 - Yes, we're imposing something on the user, should change that [Cybuck]

Threat Category breakout [Haapanen]

Issues discussed during the breakout session

- Document and user info vs. mgmt data
- Regular data vs. residual data
- Attack on the device vs. using the device to attack others
- Agreed to base categories on Section 2 proposal

Final

Refer to

<http://grouper.ieee.org/groups/2600/presentations/lexington/ThreatsCategoriesFinal.doc>

- Names might change, but organization was decided
- T.DOS for denial of service
 - NET for network
 - PRT for print stream
 - FAX for fax items
 - PHY for physical
 - IMP for impersonation/man-in-middle
- T.UD for user data
 - SNIFF for network
 - PHY for physical
 - SALVAGE for residual
 - INT for integrity
- T.TSF for indirect threats
 - CRED for credentials
 - CONF for configuration
 - SW for applets and firmware
 - AUD for audit data
- T.EA for external attacks

Section 3 assignments [Wright]

- Align security environments with 800-70 draft

Action item review [Wright]

Section 1

- Update as marked up

Section 2

- New hierarchy
- Threats applicable to each security environment (E/H/P)

Section 3

- Divide and assign work

Section 4

- Update as marked up
- Align with Section 2 threats
- Work on clauses 5 and beyond in light of agreed upon threats and hierarchy
- Would like to propose that editorship rotate to the west coast [Smithson]
 - (sidebar discussion)
 - Agreed that Sharp will do their markup edits and Section 2 alignment in one week (to 10/18), then Ricoh will have one week (to 10/25) for editing, then back for subgroup review and general P2600 distribution. Also agreed that intermediate drafts would be posted to the P2600 reflector.

Other

- Sharp to look into availability for hosting a week in January instead of February
- Who can host in Tokyo? Looking for volunteers.
- Wright to send to Cybuck the sketches of Section 1 figures; Cybuck to get them done
- TCG conference call on October 18
- See you in San Antonio in November!

* Adjourned at 12:00PM, 10/8/2004 *