

**IEEE P2600 Meeting #5**  
**August 19-20, 2004**  
**Four Points Sheraton, Montreal QC, Canada**

**Attendees**

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

Nancy Chen / Okidata  
Peter Cybuck / Sharp  
Nick Del Re / Canon  
Lee Farrell / Canon  
Satoshi Fujitani / Ricoh  
Tom Haapanen / Equitrac  
Peter Hansen / Intermate  
Kazutaka Higo / Fuji Xerox  
Harry Lewis / IBM  
Ron Nevo / Sharp  
Wanda Nuckolls / Canon  
Yasuke Ohta / Ricoh  
Stuart Rowley / Kyocera-Mita  
Amir Shahindoost / Toshiba  
Yasuji Takeuchi / Konica Minolta  
Jerry Thrasher / Lexmark  
Brian Volkoff / HP  
Bill Wagner / NetSilicon  
Liang Zhao / Epson

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 8/19/2004 \*

**Administrivia [Wright]**

***The following administrative items were reviewed:***

***Introductions***

(see Attendees, above)

## ***Agenda review***

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

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Aug2004.ppt>

### ***Inappropriate topics review***

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Aug2004.ppt>

### ***Review of officers, editors***

Noted that the current Secretary has been absent for two meetings

### ***Date change for October meeting***

Will be hosted by Lexmark. There will be no charge for attendance. Hotel accommodations are open, and recommendations will be provided. Note that there is a one day shift from the previously announced schedule for this meeting. It is now schedule for October 7-8.

### ***Action items from previous meeting***

Draft section 1 received

Section 2 materials received

Section 3 outline received

Section 4 draft received

### ***Future meetings***

Looking for hosts for some of the upcoming meetings

- January 13-14 will be in Tampa, FL, not Maui [significant grumbling...]
- February 24-25 looking to hold in Portland, OR
- April 12-13 in Tokyo, moved out by a week from previous schedule
- May 19-20, Toronto (hosted by Equitrac)
- July 14-15 in San Jose w/PWG (possibly hosted by Apple)
- September 15-16 in Madison WI w/PWG
- October 27-28 in New Orleans
- December 12-13 in San Diego w/PWG

Question: Do we need to continue to use two days in the future?

Answer: yes, for now.

### ***Voting status***

After two meetings, you can request voter status. A formal request is needed (email OK), but is automatically granted. The request helps prevent voting status being given to people who do not plan to participate, avoiding future quorum issues.

## **Content of standard [Wright]**

### ***Sec 1 Introductory material***

### ***Sec 2 Vulnerability/Threats/Exploits***

"Meat on the bones" of the vulnerability charts

### ***Sec 3 Directives/Best Practices***

### ***Sec 4 Protection Profiles / Security Target Templates***

- "AAA" level security environment
- "AA" level security environment
- "General" level security environment
- "Public" level security environment

## **Trusted Computing Group Presentation [Volkoff]**

- <http://www.trustedcomputinggroup.org/>
- Proposing to start a hardcopy working group
- TCG and TCPA are essentially the same members
- Wants to give IEEE P2600 group opportunity to look at charter, consider joining

### ***TCG vs P2600***

- P2600 is device oriented, TCG is system oriented [Wright]
- Yes [Volkoff]

### ***Process***

- Meet via teleconference
- Quarterly meetings
- Could meet in conjunction with P2600, PWG
- Might fit all in 5 days if p2600 one day [Lewis]

### ***Charter***

For details, refer to Brian V's presentation slides which I assume will be published on the P2600 site.

- Hardcopy trust platform
  - Mainly security chips
  - Could have software implementations "TCG Light"
- Trust-enabled use cases
- Installation/configuration
- Document workflow not part of this charter
  - Printing an invoice, yes; moving the invoice around for approvals, no [Wright]
  - That is correct [Volkoff]

### ***Interaction with other TCG WGs***

- Peripheral group
- Client/server working groups
- Authentication
- Infrastructure
- TP module
- Best practices
- Marketing

### ***External experts***

- Will leverage existing tech where it can
- Extend existing platforms, add new standards only when needed

### ***Deliverables***

- Charter revision
- Dates have moved out

### ***Participating***

- Need to join at at least contributor member \$15,000
- Questions about how to relate TCG work to IEEE group without sharing drafts with non-TCG-members [general]
  - Possibly using the Industry Liaison program? [Wagner]
  - I'll find out [Volkoff]

### ***Who thinks their company might consider joining?***

[no hands raised]

- It would be too soon to get approval to spend money for a September meeting [scribe missed...]
- Meeting schedules will probably slip out [Volkoff]
- Most participating companies are in chips, computers, broader product lines, except Lexmark [Wagner]

### ***Questions/Comments***

- Is the intention to publish specs? [Wagner]
  - When they're done, I think so [Wright]
  - Much of the current documents came from TCPA [Volkoff]
- Began as an internal computer thing to secure data as it moved around inside the PC (by Intel), then morphed into a broader industry consortium [Lewis]
  - Yes, includes negotiating trust between devices. Would extend to printers in that way. [B Volkoff]
  - 2600 would be "what", TCG would be "how"? [Lewis]
  - At a low level [Volkoff]
- Will this division have an effect on the scope and form of the IEEE spec? [Wagner]

- Not clear yet. For example, a TOE using 2600 PP might use work from the TCG to implement part of it. [Wright]
- Will send out the charter and web addresses this afternoon
- Date will be last week August/first September probably certainly before TCG quarterly

## Section 1. Introductory Pages [Wright]

- List of participants will be updated
- Ballotting committee (including 2600) will be listed later

### Overview

- Scope/purpose are from the PAR
- Could be changed, for example, by working with TCG

### Security environments

- NIST published a document in the last couple of weeks. Has categories that may be relevant [Volkoff]
- We should look at it. It is a checklist for specifying security in various devices. 800-70 is the document number. See <http://csrc.nist.gov/checklists/SP800-70-DRAFT.pdf> [Wright]
- Categories [Volkoff]
  - SOHO
    - Trusted users
  - Enterprise
    - Firewalled, less trust for users
  - High security
    - Multi firewalling
  - Custom
    - Legacy is typically a custom
- MFDs on network or not? [Volkoff]
  - In enterprise, mentioned as being on network
  - In SOHO, shown as connected to PC
- Should we use this? [Wright]
  - This validates our work. We should align with NIST. [Volkoff]
  - Advantage of coordinating is the checklist concept [Wagner]
  - Would it help to use a matrix of the different dimensions of security vs particular environments and map our A, B, C, D to NIST's? [Smithson]
    - That's what we did, plus we added legislative mandate [Wright]
    - Public versus home – seems very different to me because of access, public is physically public and home is physically private [Smithson]
    - Moving home from D to C and creating Public (as a “Custom”), we map well to NIST [Wright]
- This doc is about how to develop checklists. Should IEEE develop one? [Wagner]

- I looked at list of checklists, some from vendors. See: <http://csrc.nist.gov/pcig/cig.html> [Wright]
- NIST would probably accept one from IEEE [Wagner]
- Is this an interim step in advance of CC? [Nuckolls]
- In addition to. Could be used when CC not required or appropriate, or while waiting for CC certification. [Volkoff]
- Less rigorous technique for stating security functionality of your device. Some customers may not need a CC document, but would appreciate a methodology. [Wright]
- Is a hardening guide [Volkoff]
- Checklists help with security at system level, and CC help with the individual pieces [Cybuck]
- Checklist describes what, not why [Wright]
- Best practices guide: NIST has way to put in manufacturer, model, and perceived environment, to get checklist appropriate for your situation See <http://icat.nist.gov/> [Volkoff]
- Brainstorming from sec 3 could be the input to creating a checklist [Wagner]
- So should we adopt these categories? [Wright]
  - If we create a public one [Wagner]
  - What about public with gateway into intranet? [Chen]
  - Just call it custom? [Lewis]
    - Need to give it a specific name/example [Wright]
  - Hardcopy has the additional aspect of consumables we're trying to protect [Wagner]
    - Lower interest category [Wright]
    - Does that fit in similar category to unauthorized use or DoS? [Smithson]
      - Yes [Wright]
- Resolved:
  - Will adopt NIST plus add one for Public
  - Will move Home to SOHO category
  - Will remove reference to ranking the "level of security"

### ***Terms and definitions***

Will move into front matter

### ***Bibliography and references***

Currently just placeholders

Will begin to replace

Difference between bibliography and reference

- Bib has info used or is fundamental to concepts
- Ref has specific references, like NIST 800-70

### **Questions/comments**

- Would we have checklists? [Chen]
  - Probably not, but could have info for checklist developers [Wright]
- Is this for both mfrs and users? [Wagner]
  - That is the intent [Wright]

### **Who is editor?**

Subgroup retains ownership for now.

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

### ***Color coding re-employed***

### ***Identifies physical, network, and FAX phone vulnerabilities***

### ***Started from original list of 220 items [T. Haarpenen]***

- First, how can they get in
- Then, what damage can they cause
- Other dimension is physical access exploits
- Retained numbering
- Weeded out duplicates

### ***Unclassified items***

- Which are out of scope of this effort, i.e. Social engineering?
  - Might include some things in a checklist [Wagner]
  - Yes, could be addressed by BP or checklist [Haarpanen]
  - 10.05.11 Social engineering out [Wright]
- 10.05.13 Inappropriate install/config
  - See section 3
- 10.05.21 Intercept/infer info to facilitate social engineering
  - Example: FAX group with accounting names, use to pretend you authoritative [Thrasher]
  - Covered under other threats that have to do with protecting info on device [Wright]
  - Duplicate of 10.05.15 [Wright]
- 20.00.14 dupe of 10.05.15
- When combining dupes, sometimes use original text and sometimes merge [T. Haarpenen]
- 20.01.02 - refers to what?
  - Probably looping postscript job, now 20.00.14b [Haarpanen]
- Noticed that there are several numbers that are used multiple times, e.g. 20.00.14. Will add A, B, C... for now
  - Numbers don't make sense for final document; they are here just to maintain a trail [T. Haarpenen]
- 23.03.04 duplicate of others, like 10.06.03

- 25.06.02 already classified [Thrasher]
- 24.01.01 duplicate of others that are more specific

***Is there anything that covers default passwords that aren't changable? [Smithson]***

- Covered under weak passwords, directive [Wright]
  - What if you can't change them? [Smithson]
  - Also magic key sequences to put in service mode [Haarpanen]
  - Some can password protect [scribe missed...]
- We have to require passwords, no defaults [Haarpanen]

***How do we categorize vulnerabilities like replacing firmware or rogue applets? [Haarpanen]***

- Some that are so broad may need to be made into their own category, since they effect the whole device and thus fall into all categories
- [General discussion]
- Some things are device oriented, others are system oriented [Wagner]
  - Could branch some things off to TCG when that relationship is firmed up [Wright]
- Need to define what's appropriate for each environment [Nevo]
  - Need to further refine the vulnerability list then see what applies to the environments [Wright]
- Would this go into checklists? They are manufacturer-specific, so then to fulfill the reqts of a particular environment using a particular product, you would need to follow their checklist for that. [Haarpanen]
- Maybe need additional classification or application -- severity or something about what is being threatened [Wright]
- [General discussion about generality of effects, difficulty of attacks, sophistication of different types of attackers]

***Next steps [Wright]***

- Descriptive paragraphs on each
- Defer classification/dimensions until later [Haarpanen]
- Should the vulnerabilities team try to talk about environments for each threat or leave that to the PP team?
  - Another issue is that PP vulnerability is the deficiency, and our list is more like threats [Cybuck]
  - SNMP v1 with public is a vulnerability [Wagner]
    - Yes, and using that to do something is the threat [Wright]
  - We are trying to steer the list toward vulnerabilities [Haarpanen]
  - [general discussion about threats vs. vulnerabilities]
  - Threat is the general problem, vulnerability is the device's susceptability to that threat [Ohta]
  - Consequence depends on the environment [Wagner]
  - It is important in the PP to have identified those threats [Ohta]

- Categories may not be right [Nevo]
  - We weren't sure [Haarpanen]
  - Like access control is tightly coupled to authorization. Authentication is finding out who you are, and authorization and access control are about what you can then do. [Wright]
  - May be better to categorize on type of assets or type of attacker [Ohta]
  - Does the TCG have categories? [Nevo]
  - [general discussion]
  - Maybe its best to have columns, because there is information here that we don't want to lose [Wagner]
  - Should as a group agree on categories, then subgroup does the work?
  - We should stick with widely known categories [scribe missed...]
  - [lengthy general discussion, not reaching particular consensus]
  - Definitions from CC: Threat is any circumstances or events with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of services [Chen]
  - Confidentiality, Integrity, and Availability are the broad objectives of security. The others listed here, Access control and authentication/authorization, are mechanisms for achieving them (among others), and it may be worthwhile to retain those objectives in columns when considering threats or vulnerabilities [Smithson]
  - There are too many dimensions here, so I suggest that the Section 2 team takes first pass at categorizing on mechanisms and consequences, but defer the final categorization and organization of them until later in the process [Haarpanen]
- Resolved
  - We're going to add descriptive text
  - Make the list in terms of threats, not vulnerabilities or consequences
  - Determine which apply to which environments (first pass)
- Who is editor of this material?
  - Not ready for integration yet, so subgroup retains

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

Based on the brainstorming session we had in July in El Segundo [Wright]

#### ***Document status***

- We don't really have a group, or a leader, and so we're looking for volunteers. I had other obligations, so I didn't have time to contact the others in the group. I strongly suggest that it be looked at critically and make adjustments.
  - Should key into section 2 tightly

- With some effort, might be ready for group review in October meeting
- Intent is to have a holistic view of the environment
- May be modified about system view / TCG
- Refers to existing directives and standards
  - NIST 800-37, 800-23
  - ISO 14443, 15693
  - Need more references
  - Is there a public doc on CAC card? (CAC is contactless smart card) [Wright]
    - Will see about getting info, there is an SDK. Used for everything in DOD, building access, signon to PC, etc [Cybuck]
    - Uses ISO standards etc, but content is specific to DOD [Wright]
- Taking items from brainstorming and putting them into structure
  - Statements of desirable actions
  - Not how to do it
  - Were motherhood statements, need more detail
- Categories are similar but somewhat different from section 2
  - Physical security
  - Device implementation
  - Authentication
  - Encryption
  - Audit trail
- Intent of this section: [Wright]
  - We've identified the threats
  - This section shows how to eliminate or mitigate the threats
  - The PP lets you evaluate how well a device provides protection in a particular environment
- [presented individual items in the categories – Wagner]

### **Comment**

- Are all the items from the brainstorming in this doc? [Wright]
  - Yes, some are consolidated [Wagner]
- How/where does SSO or other external authentication fit in? [Smithson]
  - In some cases, machine authenticates itself AND user authenticates to machine (through an external mechanism) [Wagner]
  - We'll need to support whatever customers need/want [Wright]
- Does this section address policy or configuration distribution? [Smithson]
  - Yes, some systems use smart cards and servers [Cybuck]
  - Lexmark has mgmt products that push common configurations to multiple devices [Wright]

### ***Next steps***

- Additional material -- standards that need to be called out [Wright]
- A lot of standards out there, should go through to see which to adopt [Chen]
- Needs coordination with section 2 [Wagner]
  - When will section 2 be renumbered? [Wright]
  - We'll do new categories, needs group review, then renumber. Use legacy numbers for now. [Haarpren]
- What else from a content perspective? [Wright]
  - Add some meat to the bones [Wright]
  - And pointing to external references [Wagner]
  - How about users vs manufacturers? [Rowley]
    - To mfrs, provide capability to turn off ports; to users, turn off ports not needed / turn on ports needed [Wright]
- Could this section suggest implementations? [Cybuck]
- How much detail to provide? Depends on many things about the product and implementation. [Wagner]
- How to turn into a standard? [Wright]
  - Same division and organization as section 2? [Wright]
  - Need to decide on organization of document, like sec 2 specifies threats, sec 3 describes how to go about dealing with them [Wagner]

### ***Who is the editor? [Wright]***

- Need people for this group
- Jerry Thrasher "volunteered"
- Also Lee Farrell, Bill Wagner, Wanda Nuckolls

## **Section 4. Protection Profile [Nevo]**

### ***Based on Ricoh, Sharp, and DAPS PPs***

- Tried to get best from both
- Waiting for input from other groups

### ***TOE description***

- Users, administrators, CEs
- TOE block diagram, architecture
- A draft, needs to be made internally consistent because it is a patchwork of several documents [Cybuck]
- Terms are taken from an SNMP document, and are as general as they can be [Lewis]

### ***User assumptions***

- What's the user's supposed to do, what's the admin supposed to do

- About the assumptions, it reasonable to assume that users or even administrators won't use weak passwords? [Smithson]
  - It's another way of saying that users are required to use strong passwords somehow, you could follow up with a policy requirement [Cybuck]
  - But you don't need the policy if you have this assumption. Seems like we're brushing it off [Smithson]
  - There's a certain burden you have to put on the user [Cybuck]
  - There are environments where users are managed by an LDAP server, then you wouldn't have any problem. The purpose of the profile, how we're going to have the target evaluated, we have to make some assumptions like that a sufficiently strong password will be used, you can't make that a requirement [Wright]
  - I just wondered if this the correct way to write this requirement? [Smithson]
  - This is an example, a profile that could be adapted by a manufacturer to make a particular security target [Wright]

### ***Threats***

- These are buckets in which section go [Wright]
- They need to be reconciled one way or another [Lewis]
- Some section 2 items don't fit in these buckets [Wagner]
- These are taken from Ricoh PP [Ohta]

### ***Organizational policy***

- Seems curious that this is empty [Wagner]
- It's a site policy, unique to sites [Cybuck]
- How about strong passwords? [Smithson]
  - That would be an example [Cybuck]
- Maybe this should be reworded so that it isn't so exclusive of organizational policies [Lewis]
- Maybe we should list some that might be included [Wagner]
- Passwords would be a good example. There isn't a policy that we're referencing. [Cybuck]
- Is that really the point? Isn't it more about that there is a policy we assume will be in place for this PP to provide the protection appropriate for this environment? [Smithson]
- We make assumptions about the environment, but I'm not sure we should make assumptions about policies [Cybuck]
- Could we say it's recommended that organizations should have a password policy, for example? [Chen]
- Those go in section 3, directives and recommendations [Wright]
- PP's I've seen, 80% or so do not have anything listed in this section [Ohta]

## **Objectives**

- Is this the level of detail intended, or just an outline? [Wagner]
  - This is the level of detail [Nevo]
  - We need to look at consistency of level of detail with other sections [Cybuck]
- Must the device counter packet sniffing? [Wright]
  - Was a carryover from another document.. At least for things like admin passwords. [Cybuck]
  - An objective like this requires all compliant devices to provide that facility [Ohta]
  - Some example should be provided [Wright]
  - Protection profile needs to be detailed [Ohta]
- Does O.MONITORING mean that the audit is done by the TOE? [Wagner]
  - The device could do the audit, something else could do the audit [Wright]
  - The sentence doesn't make sense. Is it trying to say that audit data will be available? [Smithson]
  - Some description of this objective is needed, identifying that there is a choice of where to perform the audit [Ohta]
- What about the non-network environment? [Wagner]
  - These are placeholders, final content will address [Cybuck]
  - How about console operations? neither network nor non-network [Wagner]
  - The PP is for a specific environment [Ohta]
  - So if this one is for Enterprise, we would assume networked [Wright]
  - We don't need 4.21 and 4.2.2 [Ohta]
- The PP should have IT environment and non-IT environment [Ohta]
  - So an op panel would be non-IT? [Wright]
  - If there are objectives related to a server, they would be listed in an IT environment PP [Ohta]
  - Each environment will have a set of objectives that are different [Wright]
  - Yes, a new choice of words may be needed for each environment [Cybuck]
- Why is "physical location" listed under networked environment? [Wagner]
  - Even in a network environment, you still care about where the machine is. If you're in a public environment, this objective can't be there. [Wright]

## **Requirements**

- Seems very inconsistent with previous sections [Smithson]

- Were generated by the NIAP tool, we'll need to look at and eliminate appropriate for each environment [Nevo]
  - Was this generated from the toolkit based on CC2.1 or 2.2? [Smithson]
  - We got an updated CD from NIAP [Cybuck]
- We went through this exercise with DAPs [Cybuck]
  - We took a lot out in DAPs [Wright]
  - This one is based on the list AFTER taking stuff out from DAPs [Cybuck]
  - I think it's still too much [Ohta]
- This PP was from several PPs, and inconsistencies must be resolved. I don't recommend this approach. Either base it on one or start from zero. [Ohta]
  - This may just be a place where we place notes about what we want to include in the real one [Cybuck]
  - So we would run the tool again, using those notes, to generate a clean one [Wright]
- Did we decide if we were going for EAL2 or EAL3? [Wright]
  - We decided not to do EAL4, but left 2 or 3 open [Cybuck]
  - EAL3 is not required for some environments [Nevo]
- This was copied from the CC? [Ohta]
  - Yes, once it's done there will be a lot of making references to the CC documents [Cybuck]
- Do these [assignment:number] things need to be specified? [Wright]
  - They may be product specific [Cybuck]
  - They can be a range [Ohta]
  - It does represent work to be done on the PP [Lewis]
  - Some of these might be included in section 3 as a best practice [Wagner]
  - Some of these we might specific, others we could leave generic [Wright]
  - Some may depend on the environment [scribe missed...]
  - Referring to the Ricoh PP, 5.1.3, I didn't assign a number but refined the requirement and added actions; compare with the Sharp PP [Ohta]
    - So you left the number unassigned because it's an administratively defined number [Wright]
    - Yes [Ohta]
    - For the second part, you specified a fairly specific action; should it be less prescriptive? [Nevo]
    - We can work through those and make it less specific [Wright]
    - It might be related to security objectives [Cybuck]

### ***Rationale***

- What is this (objective vs threat/assumption) table? [Wright]

- It shows that each threat/assumption is met by an objective [Cybuck]
- There is another table that shows requirements that meet objectives [Smithson]
- What are these notes? [Wright]
  - Placeholders that we may eliminate or revisit [Cybuck]
  - This was also from the Ricoh PP [Ohta]
- A lot of the tables that follow are generated by the NIAP tool, and will be regenerated [Wright]
  - Yes [Cybuck]
- Some of the tables were taken from the DAPS PP, which was incomplete, so the tables are incomplete [Ohta]

### **Appendix A**

- Should this be moved up in the IEEE spec? [Wright]
  - It should be consistent with the rest of the spec [Cybuck]
- Is it required for the PP?
  - I don't know, it's usually there [Cybuck]
- Will there be more? [Wright]
  - If we define our own, like for example there is no MFP in this list [Cybuck]
- In the Ricoh PP, I listed the acronyms used in that PP, so the PP can be independent from the IEEE spec. Acronyms not use in the PP should not be included in the PP. [Ohta]
  - We'll need to explain that to the IEEE editor [Wright]

### **Next steps**

- For each environment, uniquely created [Nevo]
- Need summary reports from other groups [Cybuck]
  - Especially section 2 [Wright]
  - And environment specifications [Nevo]
- If there are best practice statements that apply to everyone, they should be in there [Cybuck]
- Cleanup and correlation before getting other input [Nevo]
- Editors: Ron Nevo and Brian Smithson [Wright]

## **Action item review [Wright]**

### **Section 1**

- Align security environments with 800-70 draft
- Update terms and definitions to include PP items, etc

### **Section 2**

- Review all threats and make sure they are threats

- Identify categories and categorize threats and consequences
- Have a short description and a long description
- Try to map to security environments (as a trial)

### **Section 3**

- Gather existing specs/standards/directives for inclusion
- Begin writing and organizing various best practices techniques to match section 2
- Divide into manufacturers section and users section (subservient to threats)

### **Section 4**

- Clean up PP1,2,3,4
- Align with security environment description
- Which environments?
  - Start with hi sec first [Nevo]

### **TCG**

- Distribute information [Volkoff]
- Investigate TCG liaison program [Volkoff]

### **Informative or normative? shall vs should [Lewis]**

- We're citing directives [Wagner]
- We'll need to assess later and see if it's a guide or a spec and change type accordingly [Wright]
- I thought PP was the "shall" and section 3 was "best practices" [Rowley]
- We discussed this earlier and it was just as squishy [Wagner]
- You'd never get it into the 802 committee with "shall" in a guide
- IEEE defs
  - Dominated by "shalls" is a spec
  - Dominated by "shoulds" is a recommended practice
  - Dominated by "mays" with some "shoulds" is a guide

### **Upcoming meetings [Wright]**

- Tried to space them out by six weeks or so, and miss various holidays
- One or two days? Leave it at two days for now
- Sponsor ballot happens when we say we're done, then we deal with whatever comes in from that, so the group doesn't become unchartered after that
- Next meeting in Lexington, I'll provide details about that. There won't be a reservation page, so please RSVP when the call goes out so I can plan for space.

- The following meeting is in November in San Antonio. We don't know the hotel yet.
- Subgroups are welcome to stay to get some work done before your flights, since we have the room available.

\* Adjourned at ~11:30 AM 8/20/2004 \*