

IEEE P2600 Meeting #13
September 15-16, 2005
Ricoh Corporation, West Caldwell, NJ

Attendees

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

Carmen Aubry, Océ (by phone)
Nancy Chen, Okidata
Peter Cybuck, Sharp
Satoshi Fujitani, Ricoh
Tom Haapanen, Equitrac
Takanori Masui, Fuji-Xerox
Ron Nevo, Sharp
Yusuke Ohta, Ricoh
Alan Sukert, Xerox
Jerry Thrasher, Lexmark
Brian Volkoff, HP

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

*** Commenced at 9:20 AM 9/15/2005 ***

Administrivia [Wright]

The following administrative items were reviewed:

Agenda review

Refer to meeting slides for detail
<http://grouper.ieee.org/groups/2600/presentations/P2600-Sept2005.ppt>

Minutes and Agenda approvals

July's minutes and September's agenda were approved without changes.

IEEE patent policy

Refer to meeting slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Sept2005.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-Sept2005.ppt>

Officers

No changes since July:

Chair: Don Wright, Lexmark.

Vice Chair: Lee Farrell, Canon.

Secretary / Lead Editor: Brian Smithson, Ricoh.

Editors: Jerry Thrasher, Lexmark; Ron Bergman, Ricoh; Yusuke Ohta, Ricoh (High Security PP); Ron Nevo, Sharp (Enterprise PP); Carmen Aubry, Océ (SOHO PP)

Meeting schedule update

Oct 24-25 Chicago, IL - w/PWG. No longer being held in New Orleans because of Hurricane Katrina. PWG has announced that they will hold their meeting at the Radisson in Chicago. More details will be posted to the mailing list.

Dec 13-14 Rancho Bernardo, CA – at HP site. Rancho Bernardo is about 30 miles due north of San Diego on I-15.

Jan 16-17 with PWG, location TBD

Mar 2-3, location TBD (somewhere on the west coast?)

Apr 6-7 with PWG, Mount Laurel NJ (near Philadelphia) at Okidata

May 17-18, location TBD

Jun 19-20, with PWG, Boulder CO at IBM

Jul 26-27, location TBD

Sep 6-7, location TBD

Oct 23-24 with PWG, Lexington KY at Lexmark

Dec 11-12 with PWG, location TBD

No conflicts were identified during this meeting. Suggestions for locations and hosts are requested.

TCG update [Volkoff]

- Use cases in process
 - goal is to complete by November meeting
- November meeting
 - relocated to San Francisco
 - Nov 7-9
 - General presentations plus HCWG
 - will try to schedule HCWG for late in day to allow teleconferencing from east coast and europe
- New members?
 - Sharp likely to join
 - also courting Xerox, Canon
 - none has joined as yet
- Next steps
 - technical committee reviews and comments
 - comes back two weeks later
 - then can move into specification process

INCITS CS1 update [Thrasher]

- CS1 is the US TAG for ISO
 - includes NIST, DHS, companies
 - 27-28 Sept meeting in DC
- INCITS T4 cryptography has now been rolled into CS1
 - so now one working group has all of security topics
- ISO 17799 has new 2005 revision
- Internal proposals:
 - min security standard for protecting sensitive data on network computers
 - NIST comments negatively
 - their objection is that you can't generalize, you need to do risk analysis
 - role-based access control for healthcare (RBAC)
 - enterprise dynamic access control (EDAC)
- SC27 working group 2
 - 15444-8 jpeg 2000 (secure jpeg)
- SC27 firs committee drafts
 - 18028-1 network security part 1 - management
 - 18028-5 part 5 VPNs
 - 18043 – IDSs
 - 14888-1 digital signatures part 1, general
 - 14888-3 digital signatures part 3, discrete logarithm-based mechanisms
- SC27 workding drafts (for comment and approval)
 - 24745 – biometric template protection

- 19792 – framework for biometric security evaluation and testing
- 18014-1 – time stamping services part 1 – framework
- 15946-1 – elliptic curve crypto part 1 – general
- 24761 – biometric authentication context
- SC27 final draft standards and amendments
 - 19790 – security requirements for crypto modulese
 - 10118-3:2004 – hash functions part 3 – dedicated functions, amendment 1 (adds SHA 224)
- New ISO JTC1 subcommittee on privacy technology
 - voting on chair closes this week
 - more info www.incits.org/tc_home/cs1.htm
- ISO TR 19791
 - extension to 15408 to support evaluation of operational systems
 - personnel, procedures, and processes
 - NIST is objecting
 - was submitted by Japanese certification body

Action items from previous meeting [Wright]

Refer to slides for detail

<http://grouper.ieee.org/groups/2600/presentations/P2600-Sept2005.ppt> and to pre-meeting action items file <http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20050912.xls>

- Logistical items
 - all done

Definitions and acronyms

- Alan Sukert agreed to take on this task
- do we need to worry about common criteria terms?
- IEEE dictionary
 - Smithson has a copy [Smithson]
 - latest edition, is 2000
 - it's a compendium of terms used in other standards [Wright]
- IEEE standards guide says that we don't need to list definitions that are already in their dictionary unless it adds clarity to do so [Smithson]
- NIAP is concerned that we're using terms that they use differently or they use different terms [Cybuck]
- we should look first at 15408, then NIAP, then IEEE [Wright]
- we should be consistent on how we use terms and acronyms
 - examples:
 - DOS or DoS
 - e-mail or e-mail

- draft by next meeting

Section 8 items (AI #6) [Thrasher]

- original action item was completed
- new sections were added (recommendations for IT, mfrs, and users) which now need to be completed

New PP annex with NIAP robustness definition AI #12 [Smithson]

- completed but neglected to publish it

What to do about NIAP instruction #10 (AI#20) [Cybuck]

- Cybuck got some comments from NIAP
- Institute of Defense analysis analyzed NIAP
- NIAP is a partnership of NIST and NSA
- NIAP started as a memo, not really a department and has no budget
- used to be equal (NSA and NIST)
 - NIST lost budget
 - NSA took over
 - NIST is coming back
 - But NIAP still has a DoD focus, commercial was neglected
- recommendations
 - have proposed that NIAP in the US be given department status with a budget
 - more work with international community
 - we should consider NIAP CIMs to be something that will appear in CC V3
- Cybuck asked if NIAP would take our PPs and certify them?
 - they need a lab needs to evaluate
 - they are happy to see that IEEE is doing this
 - they might author "government" PPs based on the IEEE PPs
 - NSA customer advocates would first have to document customer needs
 - DAPS or such organizations could make the request
 - our use of "High Security" is not EAL2
 - our basis for HS vs Enterprise was mostly asset based [Wright]
 - maybe we should call it "high value asset", "medium value asset", etc.
 - CC V3 will take a different approach to encryption
 - international signers of the new agreement could require implementations that are approved by a "national authority" in place of FIPS

- won't be required, but will be described as desirable for data transit and storage
 - SO, if things work out this way, NIAP could accept an ST evaluated in Japan without FIPS
 - CC V3
 - can use V3 now
 - can evaluate using V2 up to July 14 2006
 - status of v3? [Wright]
 - 3.0 available now
 - still subject to comments [Ohta]
 - 3.1 is expected to be approved in July 2006, will incorporate those comments
 - they asked why we don't use NIAP basic robustness CIM
 - if we don't use it now, we'll need to change it later
 - are they suggesting that NIAP stuff will be in v3? [Wright]
 - yes, that's what they're saying
 - after cc v3 is adopted, NIAP CIM will no longer be needed? [Ohta]
 - yes
 - there are some things that may be NIAP specific, like cover page format [Wright]
 - they have some problem about clause 7 and how it relates to the PPs
 - clause 7 needs a table that shows which threats are in which PP [Nevo]
 - yes, also need to describe how we rolled up subthreats in the PP - especially where we don't roll all of them up in some cases [Smithson]
 - they want us to map threat level to level of risk assessment
 - summary
 - lab is needed to validate our PP
 - NIAP might generate the government version
 - conform with robustness manual recommendations
 - follow ccv3
 - reconsider the use of term "high security"
 - revisit the relationship of threats list to pp
 - where does DAPS fit in? [Wright]
 - DAPS is like any other major customer of NIAP, and they go to a customer advocate IN NSA and make a request that they assign staff to this
 - If the White House gives them a budget, then it will happen faster
 - NIAP relies on the labs to do the bulk of the work
 - Cybuck works in the Software Assurance Working Group in DHS
 - CC evaluations have focused only on simple vulnerabilities, not the whole system

- they are promoting a new approach that involves tools to help validate network security

NIAP instruction 9 (AI #60) [Ohta]

Refer to http://grouper.ieee.org/groups/2600/presentations/Cupertino/CIM_No.9.doc and to <http://grouper.ieee.org/groups/2600/presentations/WestCaldwell/The%20US%20PP%20or%20Neutral%20PP.ppt>

{Ohta is retiring from the P2600 project, Smithson will assume his action items and will continue with the HS PP}

- Ohta's presentation was written before hearing Cybuck's feedback from NIAP
- customer behavior:
 - US govt requires NIAP CIM
 - other govts may now want to adopt NIAP PPs
 - may develop their own PPs
 - customers may or may not use NIAP CIM
- does CC v3 address this issue?
- if HS is NIAP PP, US is happy but other govts may need to develop own
- if all PPs are neutral, US must develop own PP with NIAP
- in any case vendors must certify twice
- suggestion
 - neutral PPs for High, Corporate, and Public
 - Corporate is between Enterprise and SOHO
 - US PP for High
 - neutral PPs should be hierarchical
 - vendors still need to certify twice for High
- could upgrade high to EAL3 or EAL4 [Cybuck]
 - or degrade enterprise [Nevo]
- so the neutral PPs would adopt as much of NIAP as possible, but not NIAP interpretations or requirements like FIPS, this way the threats and terminology are consistent and it is easier to make a US govt version [Smithson]
- according to Cybuck comments, we would not need to write the govt PP
 - as long as we adopt v3 and NIAP CIM to some extent [Wright]
 - isn't NIAP CIM in v3? [Thrasher]
 - when will v3 be international standard? [Thrasher]
 - apparently, next summer [Cybuck]
 - (Jerry) bring it up at the next CS1 meeting [Wright]
- when is NIAP going to get a budget? [Thrasher]
 - they're doing presentations now [Cybuck]

- will there be an increase in commercial focus then? [Thrasher]]
- DHS is getting much more concerned about commercial infrastructure protection [Cybuck]
- only thing we should do is v3
- consensus is we do v3 PPs that are neutral using NIAP CIM where not objectionable for non-US government use [Wright]
 - what is required to update to v3?
 - cctoolbox not updated [Ohta]
 - need to review v3 [Ohta]

Various items

- AI #21, 22, 25, 26, 27, 28, 60 closed by upcoming conversion to CC V3.0
- AI #33
- AI #43 completed by virtue of eliminating redundant information in the two sections
- AI #44 becomes cross-references, not consistency check
- AI #47 needs to be reflected in SOHO PP
- AI #49 examples still need to be written
- AI #52 complete: leave PPs in the P2600 document, at least for now
- AI #53, complete: answer is yes
- AI #61 is duplicate, subsumed by #64
- AI #65, 66 remain open for HS PP

Device/security settings (AI #64)

- what is meant by loss of reputation? [Smithson]
- security settings seems to be data-related [Cybuck]
- is device settings related only to presentation/cosmetics [Wright]
- is device setting A, and security is C and I? [Smithson]
- what is a loss/disruption in service? what if you want staples and the stapler was disabled? [Smithson]
- need to get clarification from Yami [Wright]

Document reorganization [Wright]

- New/current editing assignments are as follows:
 - clause 1 & 4: Wright
 - clause 2 Wright (interim)
 - clause 3: Sukert
 - clause 5: Cybuck
 - clause 6: Volkoff
 - clause 7: Thrasher
 - clause 8: Haapanen

- HS PP: Smithson
- Ent PP: Nevo
- SOHO PP: Aubry
- public pp: (open)
- annexes
 - Password/PIN generation (clause 8, Thrasher)
 - Card authentication (clause 8, Thrasher)
 - Biometric authentication (clause 8, Thrasher)
 - Remote authentication (clause 8, Thrasher)
 - Algorithms and key sizes (clause 8, Thrasher)
 - Disk overwrite (clause 8, Thrasher)
 - Informative References (clause 2, Wright)
 - Additional definitions (clause 3, Sukert)
 - Bibliography (clause 2, Wright)
- if you encounter references (normative or informative) in your section, collect them and e-mail to Wright
- Smithson to send doc files to editors

Threat Analysis resolution [Smithson]

Refer to

<http://grouper.ieee.org/groups/2600/presentations/Cupertino/ThreatsAnalysisWorksheet-consensus.xls>

- Change T.TSF.CRED.EM/.DISK in HS env from Medium to High?
 - yes
- Change T.RESOURCE.COPY in Pub env from Medium to High?
 - yes
- Change T.RESOURCE.PEER in Pub env from Medium to High?
 - yes
- Change T.RESOURCE.EXHAUST in Pub env from High to Medium?"
 - yes
- Change T.TSF.CRED.GUESS in all envs to High?
 - yes except SOHO: medium
- Remove T.UD.SNIFF.PHONE from HS PP?
 - yes
- Cost issues in general
 - we are considering this
- EM threats in general
 - no, ME is different
- Change T.UD.ACC.NORMAL in Pub env from Low to Medium?
 - low value data -- ask for rationale
- Remove T.DOS.FAX.(LOOP|VOLUME) from PP?
 - yes
- Remove T.DOS.FAX.TRAIN from PP?
 - yes
- Include T.UD.SNIFF.NET in all PPs?

- yes in enterprise, no in soho and public
- Include T.TSF.CRED.EM in Ent and Pub PPs?
 - no
- Include T.UD.SNIFF.NET in Ent PP?
 - yes (already)
- Smithson to change and issue new spreadsheet

Comments [Wright]

Refer to <http://grouper.ieee.org/groups/2600/comment-tracking/P2600-comments-database-Sept%202005.xls>

- #2 HS PP, figure should show operating panel and local interfaces as part of the TOE
 - closed
- #5 still open for HS PP
 - add to action item list?
- #7 needs to be put in the HS PP
 - add to action item list?
- #10 rejected
 - so change HS PP from ALTER to IMP
- #11 address in Best Practices
 - write up methodology
- reword definition of external environment for clause 6 (and PPs)
 - yes, new definition is: “external environment consists of other IT equipment that is interconnected or interoperates with the HCD”

Security Environment Names

- These new security environment names were proposed and accepted by the participants. However, before making changes, we'll get feedback from NIAP via Cybuck.
 - High Asset Value Environment (HAVE)
 - General Enterprise Environment (GEE)
 - SOHO Environment (SOHOE)
 - Public Environment (PE)

Enterprise PP review [Nevo]

Refer to <http://grouper.ieee.org/groups/2600/drafts/FullSpec/PP-E-12a.doc>

- Most changes were in sections 1-4
- Threats included in the PP were based on the most recent threat analysis available
- {we reviewed changes and did some minor markup of the document}

Protection Profile validation [Cybuck]

Refer to <http://grouper.ieee.org/groups/2600/presentations/WestCaldwell/NIAPUpdate.pdf>

- which labs?
 - CSC
 - SAIC
 - COACT
 - others
- need to do cleanup and validation
- all PPs should go through one lab
- who manages?
 - Cybuck helps get it started
 - Wright and Smithson are contacts
- funding
 - pass the hat?
 - gov't funding? unlikely
 - need to get quotes
 -

Project Schedule [Wright]

- Order of operations
 - IEEE review then Lab review?
 - if Lab first, then IEEE needs changes, certification would be invalidated
 - if IEEE first, then lab needs changes, IEEE would complain
 - best approach is to get lab to review up to the point of submission, then get IEEE review done, then back to the lab with minor changes and then submission
 - PPs are normative, and IEEE might want to make substantive changes
 - then maybe include lab as part of the ballot process
 - initial ballot through IEEE
 - lab gets this too
 - do needed recircs to get close
 - run through the lab
 - recirc the lab's final copy
 - submit to revcom
 - someone will need to eval twice, and IEEE is less expensive
- clause 1-8 changes before Oct meeting
- HS and E PP V3 drafts for October meeting
- Two full days in Chicago to get docs in shape.
- Get SOHO and Public caught up by December meeting.
- Form IEEE Ballot Body in 1Q06

SOHO PP review [Aubry]

Refer to http://grouper.ieee.org/groups/2600/drafts/FullSpec/pp-s-12a_with_lines.pdf

- Access terminology table: Maintenance port could be shared with other interface, such as network, local, or telephone. (this applies to all PPs)
- Assets (in table and in 2.2.3) should be synced up with clause 6. Should include HCD availability and External Environment (applies to all PPs)
- Should we list assets that have no credible against them in the SOHO environment?
 - Should explicitly state that no threats against those assets were considered to be significant in this environment
- Section 3, line 5, 19, etc. remove Resources
- (3.1.1) Administrators will configure the equipment according to the mfr's recommendations.
- (3.1.3) Reword to reflect that the location is monitored by those authorized to use the TOE during business hours and they would notice intruders, and it is locked up during non-business hours
- (3.1.4) Alter firewall assumption
- (4.1.3) O.NETWORK eneds new language regarding port/protocol filtering (applies to all PPs)
- page 25 FIA-AFL.1 remove, FIA-UAU.7 keep
- 5.1.3 FTA_SSL.3 needs an app note to say that it refers to local session
- OE.TRAIN gets put back in as OE.INSTRUCTION – same assumption except no training is assumed
- T.UD.PHY remove
- Other notes may appear in Wright's marked-up copy of the SOHO PP sent to Aubry

Action items for October [Wright]

Refer to complete post-meeting Action Items list

<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20050916.xls>

- Tell Carmen we're moving to CC V3.
- Edits to Clauses 1-8 before October Meeting
- Conversion of E & HS PP by October meeting.
- Brian V – Rancho Bernardo area hotels and info.
- Results from initial discussions with Labs (Cybuck/Sukert/Wright)

Closing [Wright]

See you in Chicago in October, 2005.

*** Adjourned at (about) 12:30 PM, 9/16/2005 ***