

IEEE P2600 Meeting #43

April 30 – May 1, 2009

Oki Data, Mt Laurel, NJ

May 13, 2009

1. Attendees

Nick Del Re	Canon
Lee Farrell	Canon
Glen Petrie*	Epson
Harry Lewis	InfoPrint
Jerry Thrasher	Lexmark
Don Wright	Lexmark
Carmen Aubry*	Océ
Nancy Chen	Oki Data
Brian Smithson*	Ricoh
Ron Nevo	Sharp
Peter Cybuck	Sharp
Bill Wagner	TIC
Amir Shahindoust*	Toshiba
Alan Sukert*	Xerox

* via telephone

2. Administrivia

Don Wright led the meeting and provided the planned agenda topics:

- Welcome & Introductions
- Update and Approve Agenda
- Review and approve March Minutes
- IEEE Patent Policy Review
- 2009 Meeting Schedule
- Update on PWG-IDS/TCG (Nevo)
- Update on INCITS CS1 Working Group (Thrasher)
- Update of CC Vendor's Forum (Smithson)
- Review of Action Items from March Meeting
- Protection Profiles Status
- PP Evaluation Financial Issues (Nevo)
- Evaluation Status (Smithson/atsec)
- Other issues raised on e-mail
- Guide to P2600 PPs ad hoc status (Sukert)
 - * Draft
 - * Comments
 - * Status of the Guide (Farrell)
- Production Printing Profile (Sukert)
- Schedule Review
- Other items
- Posting and Comment deadlines for the July Meeting

- Next meeting details

3. Review and approve March Minutes

There were no objections to the Minutes.

4. Review IEEE Patent Policy

Don presented the “Participants, Patents, and Duty to Inform” slide:

- All participants in this meeting have certain obligations under the IEEE-SA Patent Policy.
Participants:
 - * “Shall inform the IEEE (or cause the IEEE to be informed)” of the identity of each “holder of any potential Essential Patent Claims of which they are personally aware” if the claims are owned or controlled by the participant or the entity the participant is from, employed by, or otherwise represents
 - “Personal awareness” means that the participant “is personally aware that the holder may have a potential Essential Patent Claim,” even if the participant is not personally aware of the specific patents or patent claims
 - * “Should inform the IEEE (or cause the IEEE to be informed)” of the identity of “any other holders of such potential Essential Patent Claims” (that is, third parties that are not affiliated with the participant, with the participant’s employer, or with anyone else that the participant is from or otherwise represents)
 - * The above does not apply if the patent claim is already the subject of an Accepted Letter of Assurance that applies to the proposed standard(s) under consideration by this group
(*Quoted text excerpted from IEEE-SA Standards Board Bylaws subclause 6.2*)
- Early identification of holders of potential Essential Patent Claims is strongly encouraged
- No duty to perform a patent search

He provided a few IEEE Patent Policy related links, saying that all participants should be familiar with their obligations under the IEEE-SA Policies & Procedures for standards development:

- Patent Policy is stated in these sources:
 - * IEEE-SA Standards Boards Bylaws
<http://standards.ieee.org/guides/bylaws/sect6-7.html#6>
 - * IEEE-SA Standards Board Operations Manual
<http://standards.ieee.org/guides/opman/sect6.html#6.3>
 - * Material about the patent policy is available at
<http://standards.ieee.org/board/pat/pat-material.html>

5. Call for Potentially Essential Patents

Don provided an opportunity for WG members to identify or disclose patents that any WG member believes may be essential for the use of the P2600 standard. No one responded.

6. IEEE Meeting Guidelines

The list of Other Guidelines for IEEE WG Meetings was presented and reviewed with the group:

- All IEEE-SA standards meetings shall be conducted in compliance with all applicable laws, including antitrust and competition laws

Items relevant to the P2600 group:

- ISO 15408 Revision to CC V3.1
 - * ISO 15408-1 is currently in FDIS stage,
 - * ISO 15408-2 was published in August 08
 - * ISO 15408-3 was published in August 08
- ISO PDTR 15446 (PP Guide) Revision
 - * ISO TR 15446 is currently being published (on agenda for May Plenary)

10. Update of CC Vendor's Forum

Alan Sukert reported that there has been a lot of e-mail about what seems to be a new NIAP policy that will focus only on those products that have a certified Protection Profile. [This policy seems to fit well with the P2600 activity.]

A description of the new NIAP CCEVS Strategy for FY10 is posted at: <http://www.niap-ccevs.org/>

11. Review of Action Items from Previous Meeting

Don Wright led a review of the 2009-04-29 Action Item spreadsheet, which was updated during the meeting to reflect the latest status.

All items except 492 (“work with Harry Lewis to get a core group established and then look at getting a PAR for a new project”) were closed. It was marked as partially complete.

The end-of-meeting Action Item spreadsheet is available at:
<http://grouper.ieee.org/groups/2600/actionitems/P2600-action-items-20090430.xls>

12. Protection Profiles Status

Don provided the following status:

- P2600.1
 - * On May 1, P2600.1 was unanimously recommended for approval by RevCom
- P2600.2
 - * Awaiting feedback from atsec & BSI before starting recirculation ballot #2
- P2600 .3, .4
 - * Will be edited to include whatever is learned from BSI validation of .2
 - * Recirculation ballot will then be run

13. PP Evaluation Financial Issues

Ron Nevo reported that negotiation with the IEEE and atsec have been fairly successful in terms of getting PP-A and PP-B evaluated, certified, and made available for public access. The existing funds will also be sufficient to expedite the IEEE publishing of PP-A.

- PP Evaluation Financial Issues
 - * Will use \$3300 to expedite PP-A
 - * Will use \$3300 to pay BSI
 - @tsec will cover any shortfall

- Evaluation Status (Smithson/atsec)
 - * Have copies of the evaluation report for PP-A been sent out to the companies who paid?
 - * Copies of the evaluation report for PP-B will go out when available

IEEE 2600.1 should be available in June. IEEE 2600.2 will be available later in the year.

14. Other issues raised on e-mail

Carmen Aubry has raised an issue on PP-B:

Hello all,

I was reviewing P2600.2 PP and thinking on possible implementations when I realized some disturbing facts.

I have always thought that, for a P2600.2 compliant product, we can avoid implementing a trusted path for the entire communication for print job submission and scan to remote destination.

Unfortunately, due to trusted path requirement for D.PROT and D.CONF, I'm afraid that whenever D.CONF or D.PROT data are present in scan or print jobs, it will not be possible to avoid using a trusted path for the entire communication. Let me explain my concerns with some use cases.

Scan to remote scan destination:

1. Defining the remote scan destination

In the table with D.PROT we suggested that the "remote scan destination" is an example of D.PROT. Given the trusted path requirement for this data (assured identification of its end points and protection of the communicated data from modification or disclosure) we can no longer do scan to a remote file server outside a trusted path (IPSec or HTTPS).

In my opinion, without changing the PP, the only way to overcome the problem is to not define the remote scan destination as D.PROT in our STs.

- a) Do you think that we may run into problems with the CC lab or CC scheme given the fact that this has explicitly been provided as an example of D.PROT in the PP?
- b) Do you see other solutions than providing a trusted path for the entire channel or saying it is not D.PROT?

2. Defining the password for the remote scan destination

In the table with D.CONF we suggested that the password for remote scan destination is an example of D.CONF. Given the trusted path requirement for this data (assured identification of its end points and protection of the communicated data from modification or disclosure) we can no longer do a scan to a remote file server outside a trusted path (IPSec or HTTPS).

I know that, for instance, in case of scan by SMB the password is not transferred in clear text on the line (NTLM or Kerberos) but I don't think that we provide: "assured identification of its end points" => How is the HCD assured of the identification of the remote file server? (the remote server is assured of user identification because he provides a password).

Which are our options to deal with this problem?

- a) Are we forced to exclude user password for the remote destination from D.CONF in our ST?
- b) Do you see other solutions than providing a trusted path for the entire channel or saying it is not D.CONF?

Printing

3. Submit a print job that contains a pin code that can be used to release the job. The pin code will be D.CONF. This pin code is encrypted (protection for disclosure). The problems arrive with the other requirements associated to the trusted path:

i) assured identification of its end points: The HCD is assured of user's identity (because it checked the credentials) but the user is not assured of printer identity (without using HTTPs or IPsec)

ii) I'm not sure that we can say that we satisfy the requirement for protection against modification by performing encryption only

Which are our options to deal with this problem?

a) Are we forced to exclude the pin code that is used to release the job from D.CONF in our ST?

b) Do you see other solutions than providing a trusted path for the entire channel or saying it is not D.CONF?

Can you please give me your opinion on this issues?

Carmen explained her impression that in PP-B, scan to file and print submission can be done without a trusted path. However, if D.PROT and D.CONF data are present, it does not seem possible to do without a trusted path.

Whenever there is a mix of user data with authentication data, there seems to be a requirement for a trusted path.

There was some discussion—and disagreement—about whether a Kerberos environment achieves adequate endpoint assurance.

It was suggested that Helmut (atsec) should be contacted and asked about this issue. It relates to one of the differentiators between PP-A and PP-B. Hopefully, we can identify a use case scenario that doesn't require a trusted path.

Carmen will write up the question to be sent to atsec.

15. Evaluation Status

It was noted that atsec still needs to provide a "FINAL" [and non-confidential] evaluation report to each of the Sponsor companies.

16. Guide to P2600 PPs ad hoc status

Don Wright led the review of the 497 comments received on the Protection Profile Guide document.

Alan Sukert had examined all of the comments prior to the meeting. Don explained that most of them were only editorial in nature, and that Alan proposes to accept them as written. As such, they do not merit spending [much] time reviewing in the meeting. In spite of this, the comment review occupied the remainder of the day. The resolutions to all the comments were captured by Don and are available on the website: http://grouper.ieee.org/groups/2600/comment-tracking/P2600-Guide_2009_04_v03.pdf

During the review, it was agreed that the terms "Should", "Shall", and "Must Not" will be changed to lower case.

Because the Application Note numbers vary (for the same textual content) in the different Protection Profiles, the Guide should note that all Application Note numbers referenced refer to PP-A only.

Comment #7

This comment concerns PP Guideline 43a: "In this case the ST Author should be able to argue that such fully encrypted disks do meet the requirements of FPT_CIP_EXP.1.2 because they do detect gross modification such as degaussing of the disk and, more importantly, they exceed the "detection" requirement by preventing modification."

Suggested Remedy

Please check with Helmut Kurth or someone else from ATSEC in order to double check this statement.

→ Will ask atsec and modify as necessary.

16.1 JBMIA Comments on Guide

The JBMIA had submitted six comments, but in most cases the attendees of the P2600 group were not sure about exactly what was requested in terms of what text should be added to the Guide. However, attempts were made to interpret the desired request, and a proposed resolution was generated for each. The JBMIA members are encouraged to review the proposed resolutions and determine whether they adequately address their issues.

Comment #1

Specification of TOE boundary. [Regarding clauses 5 and 12.3 in PP-A (pages 6 & 39)]

Physical and logical boundary of TOE and its method of specification.

From Table 22 of Section 5, physical object is seen as physical boundary and logical boundary is seen as aspect of functional specification of physical object.

We would like to get agreement that each vendor can specify its own TOE boundary. For example:

- we would like to be granted that each vendor specifies firmware version that is necessary
- in the case hardware (for example IC chip) will be included in addition to firmware, we would like to be granted that hardware boundary is specified in terms of IC chip, not the whole hardware.

→ It is the intent of the PP that, generally, the entire HCD is the TOE.

[Note that the PP does not talk about the TOE "boundary."]

Add to the international section text that reminds the ST Author that some schemes have different rules on defining the TOE boundaries. **However, any security relevant component addressed in the PP or ST must be included in the TOE.**

If a feature, such as COPY, FAX, SCAN, etc. is a part of the HCD, then the feature must be included in the TOE boundary.

Comment #2

Interpretation of FIA_UID.1/FIA_UAU.1 [Regarding 10.5 in PP-A page 27]

FIA_UID.1/FIA_UAU.1 is applicable in the case that TOE uses external user authentication server in the IT environment.

FIA_UID.1/FIA_UAU.1 states "require" , but not "provide". Therefore FIA_UID.1/FIA_UAU.1 is applicable as the TOE SFR in the case that TOE uses external user authentication server in the IT environment.

[Referring the Meeting Minutes on the MEETING #42, the ATSEC recognized it.

<http://grouper.ieee.org/groups/2600/minutes/P2600-minutes-Mar2009.pdf>

Also the sample ST exists at http://www.commoncriteriaportal.org/files/epfiles/st_vid10242-st.pdf]

➔ It is not clear what is being requested. Comment rejected due to lack of understanding of the issue. The group requests that JBMIA members provide specific suggested changes to the Guide text. Note that use of external authentication is discussed in the Guide in 4.3.5.2 and elsewhere.

Comment #3

Consistency between O.AUDIT.LOGGED and corresponding SFRs [Regarding class 8.1 of PP-A (page 14)]

The O.AUDIT.LOGGED security objective states that “The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration”, while the corresponding SFRs are FAU_GEN.1 and FAU_GEN.2 . It seems to be inconsistent.

The ST that claims SFRs and rationale corresponding to O.AUDIT.LOGGED as it is in [PP] should be permissible to fulfill the security objective.

➔ “TOE use” seems to be the item of inconsistency that is being referenced in the above comment. However, TOE usage (e.g., job initiation, job completion) *can* be security relevant and are included in the table of auditable events in FAU_GEN.1 in PP-A—and therefore the inclusion of “use” is appropriate. In PP-C and PP-D, an ST Author may choose not to audit job initiation and job completion.

Text will be added to the Guide (in 5.2.2.3.1) to explain this.

Later, Brian made the following comment:

Audit for job completion is required in PP-A. Audit for job initiation is recommended. Therefore, the ST Author cannot choose to not audit job completion (for PP-A, at least...).
--

Comment #4

Requirement of ALC_FLR.2

1. About ALC_FLR.2, let us clarify that this SAR focus on only TSF? In other word, could we recognize that non TSF software is out of scope of this SAR?
2. We would like to know how level of actual process is allowed as ALC_FLR.2. For example, ,about "remediation procedures issued to TOE users" , is it allowed that service engineer update FW by visiting users? And about "flaw reporting" is it allowed that service engineer notify this by email or displaying only on web site?

➔ Add text in the Guide to address the questions:

- 1) Applies to any security flaw in the software/firmware in the TOE

2) The group does not think that there is any requirement about “automated” flaw remediation. Only a procedure is needed. Automated methods to fix flaws is not a requirement at FLR.2.

Comment #5

Difference in contents of requirements between CC and [PP] in audit log.

Which should be correct to handle that are not specified to audit in a [PP] out of all SFRs specified in the [PP]?

- it is not necessary to claim in ST since there is no description in the [PP].
- although there is no specification in the [PP], if the SFRs that are specified to be audited in CC part 2 will not be audited, the rationale for not auditing must be described in ST.

We request that it is not necessary to claim in ST since there is no description in the [PP].

For example, we would like to get agreement that the contents of requirements is to generate the log only for 5 items in Table 15 in the case we claim Minimum as audit level, not to generate the Minimum level of log that is described as audit for the other SFRs.

➔ Text will be added to 5.2.2.7.1 (d) (1) (iv) explaining how to specify auditing only the events required by the PP.

If the ST Author selects "Not Specified", then the product must only generate audit data for the five items in Table 15.

If they ST Author selects "Minimum", then the product must generate whatever is required by CC for "Minimum" audit level for all SFRs in the ST, and they must also generate audit data for the five items in Table 15. For example (in PP-A), Table 15 requires logging of Job Completion which is not part of any of the CC-defined audit requirements, and it requires logging of successful/unsuccessful use of authentication and identification mechanisms which are part of the CC-defined Basic audit level.

Comment #6

Sufficiency that some SFRs rationale meets the corresponding security objectives.

CC require the ST author to describe the security requirements rationale that demonstrate the SFRs meet all security objectives for the TOE. (ASE_REQ.2.7C)

These rationale demonstrate correspondence between SFRs and all security objectives of [PP] in subclause 10.12 Table 20, page 34.

These rationale are written as high level statements (shown as bellow).

Is the same statement as [PP] enough because [PP] is validated?

Or is ST author required more detail statements how the refined SFRs meet to all security objectives for the TOE ?

In Table 20, "Purpose" state that how the SFRs meet to each security objectives.

1. FDP_ACC.1(a) Enforces protection by establishing an access control policy.
2. FDP_ACF.1(a) Su[PP]orts access control policy by providing access control function.
3. FIA_UID.1 Su[PP]orts access control and security roles by requiring user identification.

Same statement as [PP] is enough for ST because [PP] has already been approved.

➔ Add text [somewhere in clause 5] which tells the ST Author that the sufficiency of the PP’s rationale for use in a specific ST should be negotiated during ST evaluation.

16.2 Status of the Guide

Don referenced the following question that was raised on the e-mail list:

From: Farrell, Lee
Sent: Wednesday, April 01, 2009 11:52 AM
To: STDS-2600@LISTSERV.IEEE.ORG
Subject: [2600] PP guide -- Official Document?

Hi,

I just received a question about the "official" status of the Guide. Would it be possible to include a reference (i.e., a durable link) in the 2600.x standards that points to the Guide? Or better yet, get NIAP to either publish it on or provide a link from their website? Basically, anything that would somehow elevate the status and purpose of the Guide?

Don/Brian, could you please add this discussion topic on the agenda for April?

Thanks,

lee

Don explained that the PP Guide is only an informative document written by the authors of the PPs. It is very unlikely that it will be endorsed by either NIAP or BSI—nor posted on their websites. The Guide will be posted on the P2600 website.

Given the current status of the IEEE standard for 2600.1 (PP-A), it is too late to modify the content of the document to include a reference to the Guide.

Don did suggest that it would be possible to process the Guide as an IEEE Guide, in which case it would be published and recognized by the IEEE. However, this would require additional effort by the P2600 Working Group to go through the standards development process. There did not seem to be much support for this from the group members.

17. Production Printing Protection Profile (PP-E)

Harry Lewis explained that Don's leadership has run its course with regard to his involvement with efforts on P2600 Protection Profiles. If there will be any activity on a Production Printing Profile, a new leader is required. However, Harry is not [yet] prepared to volunteer until he hears the answers to a few questions:

- What time involvement might be required?
- What are the necessary steps?
- What are the costs for evaluation and certification?

Don listed the following steps:

- Officers are needed
- An IEEE Project Authorization Request must be established

- A revision to IEEE 2600 (base specification) would be necessary to include a description of the new environment
- Threats and mitigation requirements analysis – in terms of the unique requirements for production printing
- Agreement on the “TOE boundary” for production printing systems must be established

Estimated cost elements:

- Evaluation and Certification: ~\$25-50K?
- Copyright from IEEE ~\$12K?

Alan noted that Xerox is seeing more customer awareness of security requirements for office and production equipment. These requirements are appearing in Request for Proposals, with a focus on network protection. It was noted that the security requirements do not seem to be specifically tied to production printing equipment, but appear more often as general security requirements.

The following questions were raised:

- Is a certified Protection Profile really required? Or would a separate IEEE standard be sufficient?
- Is there enough interest and commitment to move forward? If not today, how soon?

Don noted that a PAR would need to be submitted to the IEEE in the next four days, or it would be delayed until the end of July.

Harry, Alan, and Ron all indicated that their companies (InfoPrint, Xerox, and Sharp) are interested. Carmen and Nick said that Océ and Canon are interested enough to have them participate if any activity on this effort occurs.

18. Schedule Review

PP-B certification has been delayed beyond the date for the May 7 submission to RevCom. As a result, the next RevCom approval date will be in September. PP-C and PP-D will also be held off for IEEE submission until BSI completes their certification activity and feedback.

Brian’s latest schedule diagram was provided, and is available at:

<http://grouper.ieee.org/groups/2600/presentations/MtLaurel2009/schedule43a.pdf>

19. Posting and Comment deadlines for the July Meeting

Don reminded everyone of the following guidelines and deadlines for submitting comments on the PP Guide document and the Production Printing Protection Profile:

- Documents are under change control
- All comments must be in the tool
- The editor may not make changes EXCEPT based on submitted and accepted comments.
- PP-A, B, C & D are closed for commenting!!!

- Posting of Documents: June 26, 2009
- Posting of Comments: July 3, 2009

[NOTE: Because these dates were set for a July 10 meeting, they should be adjusted to June 8 and June 15 for the re-scheduled June 22 meeting.]

20. Next Meeting Details

Harry Lewis said that he cannot attend a July 10 meeting. However, there is a possibility that he could participate in a June 22-26 meeting co-located with the PWG—provided that the PWG could reschedule their meeting by one week.

This will be investigated over the next few days to confirm.

Otherwise, the P2600 group will plan to hold a meeting in the San Jose area on July 10. Details will be announced.

Hardcopy Device and System Security meeting adjourned.