IDS Face-to-Face Minutes
Aug 6-7, 2013

Meeting was called to order at approximately 9:00 am local Aug 6, 2013 and reconvened at approximately 9:00 am local Aug 07, 2013.

Attendees – Aug 6, 2013 and Aug 7, 2013

Carmen Aubry*	Oce - Canon
Nancy Chen*	
Richard Huelbig*	Sharp
Gyaneshwar Gupta	Oki Tokyo
Akisa Matsuda*	Sharp
Ira McDonald*	High North
Joe Murdock	Sharp
Ron Nevo	Samsung
Glen Petrie*	Epson
Brian Smithson	Ricoh
Alan Sukert*	Xerox
Michael Sweet*	Apple
Bill Wagner	TIC
Rick Yardumian	Canon
Bill Wagner	TIC
Rick Yardumian	Canon

*Dial-in

Agenda Items

Note: Meeting slides are available at ftp://ftp.pwg.org/home/pwg/pub/pwg/ids/Presentation/2013-08-06-IDS_F2F.pdf.

1. Minute Taker
   a. Alan Sukert taking the minutes
2. The main purpose of these two ½-day meetings was to participate in a meeting of the MFP Technical Committee (TC) and jointly review the latest draft (Version 0.6.1) of the new MFP Protection Profile.(PP). The goal is to give PWG IDS members a forum to review drafts of the MFP PP and make any comments.
   a. Brian Smithson led the MFP PP discussion. The plan for the two ½-day meetings is the following:
      - Do a walkthrough of the whole document,
      - Discuss any comments that have been posted to the TC,
      - Discuss a few other "known issues", and
      - Take new comments.
   b. The key points discussed at the two ½-day sessions were:
      - The new MFP PP will be based on exact compliance, meaning that no additional SFRs will be allowed in any Security Targets.
      - The new MFP PP will only cover MFPs, where an MFP is defined as a device with printing, copying and scanning and optional embedded fax; it will not cover networked printers.

- This new PP is being developed to meet the new approach of making the CC process align with procurements in the CCRA member nations, so that a CC certification will mean something to procurement personnel besides a checkbox.
- Wi-Fi is out of scope in the MFP PP; the PP assumes a wired connection.
- On Embedded (PSTN) fax – both sending and receiving faxes - is covered in the new MFP PP. Question was asked about devices that only send faxes – the TC will have to determine if/how to address such devices.
- The TC is struggling with how much of the Security Functional Requirements (SFRs) from the approved Network Device PP (NDPP) need to be incorporated into the MFP PP to address the divergent opinions (from all of them to none of them). It's a key issue the TC will have to get agreement on between NIAP (the US Scheme) and IPA (the Japanese Scheme).
- There was a discussion on USBs and similar interfaces and whether they are/should be part of the Target of Evaluation (TOE). The TC will have to address this issue, although it is likely any requirements related to USBs in the MFP PP will be optional ones.
- The PP needs to be consistent (it isn't now) with respect to what scanning is allowed (e.g., scan to USB?). Right now it only addresses scanning to an external IT entity.
- There were comments provided that the MFP PP needs to address customer engineers/serviced as a role in addition to normal users and admins, and the service role has to be inserted where applicable in the PP.
- There was a lengthy discussion on software updates and what requirements should be in the PP with respect to verifying the source of a software update.
- Brian pointed out that NIAP will not be evaluating this new PP directly. Instead, it will be evaluated by the applicable CCTL as part of the first evaluation of an MFP using the new MFP PP.
- IDS members suggested that the TC look at the PWG Common Log Spec to determine what audit log events should be required in the MFP PP. IDS members were given the action to compare the PWG Common Log Spec against the audit log requirements in the MFP PP and make any comments.
- The new MFP PP, unlike 2600.1 and 2600.2, will allow for network authorization to be permissible.
- There was a lengthy discussion on the access control policy in the MFP PP. It was suggested that this policy should agree with the IPP and Semantic Model PWG specs. It was also suggested that the MFP PP should make sure that the default position is that if the site access control policies break down or fail, no one except the admin should be allowed to do anything.

  The current User Access Control Policy in the MFP PP needs to be updated to explicitly allow admins to delete User Document Data and add access for admins to delete and modify job data (i.e., job instructions).
- For the TSF_FAU (Audit) SFRs it was suggested that we add job submission and job identifier as required items to log in addition to job completion status.
- It was suggested that the PP should explicitly indicate that the audit log requirements only apply to security management functions (defined as those management functions that affect the operation of the TOE Security Functions (TSFs)) and that the PP define the minimal set of security management functions that are required.
- The PP should probably define what is meant by external storage for the FAU_STG.1 SFR.
- The FDP_IFC.1 and FDP_IFF.1 flow control SFRs need to be refined to address network-fax separation. Also, the PP should better define and clarify what is meant by "non-fax data".

- The PP may need to use the extended component proposed by NIAP to address software upgrades with respect to FDP_ITC.2 (Import of user data with security attributes).
- The MFP PP will be including the FIA_AFL.1 (Authentication failure handling) SFR, meaning devices will have to have some type of locking mechanism after a certain number of incorrect login attempts. There was a lengthy discussion as to whether this should apply only to logins local to the device as opposed to logins via some type of network or smart card authentication – those should be a function of the remote authentication server or smart card and outside the TOE. While there was no consensus reached, it was agreed that the TC will have to address if and how this SFR applies to network and smart card authentication.
- Currently the MFP PP is making the SFRs for image overwrite "optional optional", meaning that the vendor has the option whether to include them in an ST or not. Note – if they were "mandatory optional" that would mean that if the vendor did do the overwrite function they would have to include the overwrite SFRs in an ST.
- The FIA_UAU.1 and FIA_UID.1 (timing of authentication and identification, respectively) SFRs will allow some actions to occur before identification and authentication of the user has occurred as long as they don't conflict with the User Access Control Policy. That is different from 2600.1 and 2600.2 which don't allow any actions until the user has been identified and authenticated.
- We will create a table in the MFP PP for the actions allowed for management of TSF data similar to the table created for the User Access Control Policy.
- For the FPT_TST.1 (self-test) SFR the TC will have to define in the MFP PP the minimum required to meet this SFR, with the important proviso that whatever is defined must be testable by an evaluation lab, and also what gets logged in the audit log if there is a failure in self-test. Since power on self-test is used to meet many of this SFR requirements this could have some implications on what error messages may be required to meet the SFR intent.

There were many smaller corrections suggested at the meeting that Brian recorded and which isn't recorded in these minutes. Brian plans to update this draft and have the update available for the next TC Meeting which is scheduled for Sep 9th in Orlando FL.

The IDS members present were asked if they wanted to continue to do this type of review and the response was in the affirmative. Given that we agreed to review any updates to the MFP PP at our next Conference call and have another walk-through session like this one at the October IDS Face-to-Face Meeting in Cupertino CA.

Next Steps

- Next Conference Call Aug 19, 2013 at 11am PT/ 2 pm ET.
- Next Face-to-Face Meeting will be October 22-24, 2013 in Cupertino CA (hosted by Ricoh).
- Actions:
  - IDS Members: Compare the auditable events between those defined in MFP PP Version 0.6.1 and the approved PWG Common Log Spec and provide comments to the MFP PP Technical Committee.

The meeting was adjourned at approximately Noon local on Aug 7, 2013.