IDS Face-to-Face Minutes
November 5, 2014

Meeting was called to order at approximately 1:00 pm local November 5, 2014.

Attendees –

Carmen Aubry*	Oce Canon
Tom Benkart*	
Jerry Colunga*	
Graydon Dodson*	Lexmark
Mike Green	Conexant
G. Gupta	Oki Data
Lonnie Higgs*	NSA/IAD
Dan Manchala	Xerox
Ira McDonald*	High North
Soma Meiyappan	Conexant
Joe Murdock	Sharp
Brian Smithson*	Ricoh
Alan Sukert*	Xerox
Michael Sweet*	Apple
Bill Wagner	TIC
Rick Yardumian	Canon

Agenda Items

Note: Meeting slides are available at http://ftp.pwg.org/pub/pwg/ids/Presentation/2014-11-05-IDS_F2F.pdf .

1. Minute Taker
   1. Alan Sukert taking the minutes
2. Agenda:
   - Introductions, Agenda Review
   - Common Criteria Update
   - Document Status
   - Document Review
     - IDS Model Spec (Interim)
     - IDS IAA Spec (Interim)
   - Future Activities
   - Wrap Up
3. Went through the PWG Intellectual Property policy.
4. There was no action item review at the meeting.
5. Brian Smithson reviewed the latest status of the new MFP Protection Profile (PP) Technical Committee (TC); slides are available at http://ftp.pwg.org/pub/pwg/ids/Presentation/2014-11-05-MFPTC-F2F.pdf . The key comments were:
   - We posed several questions to Lonnie Higgs (see slides 9-11). He will take these back to his team at NSA and get us answers next week. One point that was made was that IPA feels that any

requirements in the MFP PP that are extracted from the Network Device PP (NDPP) should match the requirements in NDPP Errata #2, so any differences from NDPP Errata #2 should be consciously made. Brian will look at the current differences in the MFP PP from NDPP Errata #2 and provide them to Lonnie to get clarification on whether the differences were intentional or not.

Another point is that the current requirements in the MFP PP for exporting the audit log to an external IT entity are based on a “push” model from the TOE to the external entity; the question is whether a “pull” model from the external entity is allowable (because a “pull” model could imply that the TOE needs to store the audit log until it is “pulled”). Lonnie will try to get clarification on whether a “pull” model is allowed.

- We spent most of this part of the meeting discussing the issues the MFP PP TC is having trying to define the disk encryption requirements for the MFP PP based on the new Full Drive Encryption (FDE) AA and EE collaborative PPs (cPP). Right now the MFP PP states that there is a choice of one of three options that can be selected:

  ✓ Conform to the NIAP Software Full Disk Encryption (SWFDE) PP

  ✓ Conform to the FDE cPP (not clear if both the AA and EE parts would be required)

  ✓ Conform to SFRs in the current draft MFP PP that are based on the SWFDE PP.

  We are looking at redefining the SFRs for disk encryption by extracting the applicable SFRs from the FDE cPP AA and EE cPPs, especially the FDE AA cPP.

- The problem with the two FDE cPPs and SWFDE PP as they now stand is that they are based on the “lost laptop” model where the full Target of Evaluation (TOE) is in the hands of the attacker; that type of model does not apply to an MFP, hence the problem in just apply the SWFDE PP or the FDE cPPs as is. Unlike a laptop where a user has to do some type of authentication to unlock the device, an MFP will unlock the device and perform the disk encryption without any type of user intervention.

- There is a newer draft of the two FDE cPPs available that apparently relaxes some of the requirements (for example, passwords may no longer be required to enable encryption/decryption). We may be able to use these relaxed requirements in the latest FDE cPP drafts to help define the disk encryption requirements for the MFP PP. However, it was pointed out that NIAP (or any other Scheme for that matter) could put constraints as part of its endorsement of the FDE cPPs that would require some requirement that the FDE cPPs make optional.

- What might help the MFP PP TC is a document from the FDE TC that describes how to do a single evaluation that meets both the FDE AA PP and FDE EE PP.

- It was noted that there is a planned revision to the FDE cPPs in the spring of 2015. The MFP PP TC should make sure that any issues we find that are needed to make the FDE cPPs applicable to MFPs should be given to the FDE iTC in time to make this revision.

- Brian then led the group through the threats, assumptions, objectives and SFRs from the FDE AA CPP and which ones applied to MFPs, which ones didn’t apply and which ones we weren’t sure about (see slides 12-18). The group agreed in almost all cases with Brian’s assessment as indicated on the slides. The group did think we should remove the assumptions about secure state (doesn’t make any sense for MFPs) and strong cryptography (is redundant with requirements already in the MFP PP), and the requirements for submask combining (it applies to the authentication factor that MFPs don't have in the first place) and for FCS_CKM.2 (because the FDE CPP only references them but doesn't include the actual SFRs).

- Our current planned approach for addressing disk encryption in the MFP PP is to extract the applicable requirements from the FDE AA cPP and then modify them as necessary. The goal is to make sure that the disk encryption requirements in the MFP PP are ones that all vendors can meet; we don't want the case of having requirements here that no one or only a small handful of vendors can meet. We are looking at both NIAP and IPA to approve this approach.
- Next steps for the MFP PP TC are to work on extracting into the MFP PP the applicable SFRs from the FDE AA cPP and then modify the SFRs that require modification (see slides 15-18).

6. Document Review

- IDS-Model spec for review was available at http://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20141101-rev.pdf. Joe indicated this was a revision to address comments from the last F2F, to fill in missing text and to update all the diagrams.

  Review Comments presented at the meeting were:

  a. Title: Change to read "Imaging System Security Model".

  b. General: Replace 'Imaging Device' with 'Imaging System' whenever applicable in the spec.

  c. Define the term 'Imaging System' in Section 2.

  d. Reconcile the applicable definitions in Section 2 with the corresponding definitions in the IPP Everywhere spec. Remove the definitions for 'Visible' and 'Securely Visible'.

  e. Define the term 'Service' in Section 2.

  f. General: Review capitalization and make sure that all terms that need to be capitalized are capitalized. Make sure to capitalize 'owner' in the spec.

  g. Page 11, Section 2.2: Modify the definition of 'Client' per the discussion at the meeting.

  h. Page 11, Section 2.2, Line 345: Change the definition of Delegated Resource to read "…a different actor to manage the resource…"

  i. Page 12, Section 2.2, Lines 377-385: Add 'Imaging Systems' and 'Imaging Services' to the applicable items in Section 3.1.

  j. Page 12, Section 3.1, Lines 383-385: Combine Items #4 and #5 together into a single item.

  k. Page 14, Section 3.4, Line 446: In Item #1 change 'Device' to 'Client Device'.

  l. Page 15, Section 4.1.2, Line 480: Change 'identification' to 'identity'.

  m. Page 15, Section 4.1.2, Line 483: Change 'biological scan' to 'biometric information'.

  n. Page 15, Section 4.1.2, Line 487: Rewrite the first sentence to state that access rights are being restricted.

  o. Page 15, Section 4.1.3, Line 489: Clarify the second sentence.

  p. Page 15, Section 4.1.3 Line 490: Capitalize 'authorization'.

  q. Page 15, Section 4.1.3, Line 495: Change the term 'database' here and elsewhere in Section 4 to be 'data store'.

r. Page 18, Table 1: Change 'Imaging Device' to 'Imaging Service' in the applicable definitions in Table 1.

s. Page 18, Table 1: Change 'Sevice' to 'Device' in the definition of Owner.

t. General: Reference definitions from other specs rather than creating new definitions for this spec whenever possible.

u. Page 18, Table 1: Make the definitions of 'Guest' and 'NormalUser' consistent.

v. General (Section 4): Use consistently the term 'Actor' or 'Security Actor' in the tables in Section 4 (it was decided to use the term 'Actor').

w. Page 18, Table 1: Define the term 'Security Actor' to be something like "an authenticated actor with rights to modify security policies or perform other security-related operations such as shutting down services."

x. Page 19, Table 4: Change 'HID Card' to 'smart card' in the definition of Identification Service.

y. Page 19, Table 4: Remove the definition of Resource Service.

z. Page 20, Table 5: Add to the definition of Embedded Device text extracted from the relevant RFC.

aa. Page 21, Section 5.1, Line 585: Use the RFC as the reference to the XML signature syntax.

bb. General (Section 5.3): Use 'UUID' instead of 'GUID' in the various security element definitions.

cc. Section 5.3: Define one general authorization type instead of one for each element type.

dd. General (Section 5.3): Think about Job and Document ID of users.

ee. Page 28, Section 6, Line 713: Add a sequence diagram to explain how this is supposed to work.

ff. Page 31, Section 11.1, Line 800: Change sentence to read "…controller by an Imaging Device…"

gg. Page 34, Section 13.3, Line 883: Remove the "W3C" reference here.

There was a question asked whether this spec could be applied to address key generation and key management. The response was that it could be, but the current spec doesn't reflect it and likely will not; we don't want the spec to be vendor-specific.

- IDS-AAA spec for review was available at http://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20141101-rev.pdf. Joe indicated this was a complete rewrite to eliminate unnecessary material, provide an updated model and address previous review comments.

  Review Comments presented at the meeting were:

  a. Title Page: Change title to read "Imaging System Security Identification, Authentication and Authorization".

  b. General: Make the corresponding changes in Section 3.4 that were made in the IDS Model spec.

  c. Page 14, Section 6.1.1.5, Line 341: Address the note added in the page here.

  d. General (Section 6): Change 'X509' to 'X.509' everywhere it occurs.

   e. Page 16, Section 6.2.1: Define the 'SSID' element shown in Figure 6.
   f. Page 22, Section 6.5.1: Define all the elements shown in Figure 14.
   g. Page 24, Section 10, Line 505: Address the note added in the page here.

7. There was a brief discussion on the suggestion from Joe that the IDS WG prepare some type of business case white paper around 3-D printing similar to the one created for Managed Print Services. The group decided that instead of a separate white paper we should provide text to go into the white paper the PWG is preparing around 3-D printing.

Next Steps

- Next Conference Call November 17, 2014 at 11am PT/ 2 pm ET. Main topic will be review of the PWG IDS charter.
- Next Face-to-Face Meeting will be Feb 3-5, 2015 at Xerox in El Segundo CA.
- Actions:
  a. Joe: Update the IDS-Model spec to address the comments presented at this meeting.
  b. Joe: Update the IDS-IAA spec to address the comments presented at this meeting.
  c. Joe/Ira: Provide text to go into the PWG 3-D Printing white paper.

The meeting was adjourned at approximately 4:30 PM local on November 5, 2014.