IDS Face to Face Minutes
October 23-24, 2013

Tuesday, Oct 23, 2013

Attendees

Ira McDonald	High North	(by phone)
Joe Murdock	Sharp	
Michael Sweet	Apple	
Brian Smithson	Ricoh	
Ashlee Holbrook	Lexmark	
Bill Wagner	TIC	
Rick Yardumian	Canon	
Russell Brudnicki	Kyocera	
Roarke Randall	Toshiba	
Gyaneshwar Gupta	Oki Data	
Tak Shiozaki	Epson	

Agenda

1. Introductions/Agenda Review
2. Action Item Review
3. Document Review
   a. IDS Attributes errata
   b. IDS Model
   c. TNC Binding Specification
4. ITU-T X.series standards
5. System Control Service Integration
6. MFP Technical Community vendor face-to-face meeting
   a. Recap of the F2F meeting in Orlando
   b. Discussion of currently open issues and proposed resolutions
   c. Updates from NIAP and IPA (if any)
   d. Plans and schedules
   e. Open discussion

Action Item review

AI #144 (Compare auditable events in the PP draft to the proposed PWG Common Log Spec)

- Will be discussed during the MFP TC session

Document Review

Active Documents

- HCD-TNC Binding (Prototype) ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idstnc10-20130910-rev.pdf
- IDS-Model (Interim) ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20120806-rev.pdf
- IDS-IAA (Interim) ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20111005-rev.pdf
- IDS-Remediation (Interim) ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-remediation10-20100930.pdf

Errata for 5110.1 (IDS Attributes)

- **ftp://ftp.pwg.org//pub/pwg/ids/wd/wd-idsattributes10-20131015.pdf**
- **ftp://ftp.pwg.org//pub/pwg/ids/wd/wd-idsattributes10-20131015.doc**
- **ftp://ftp.pwg.org//pub/pwg/ids/wd/wd-idsattributes10-20131015-rev.pdf**

Needed to accommodate different patches for different firmware components, different resident applications, and different user applications. It was correct in the NAP and TNC Binding specifications, but was not correct in the IDS Attributes document.

IDS Model

- **ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020.pdf**
- **ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020.docx**
- **ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020-rev.pdf**

Reviewed new definitions for Endpoint, Visible, and Securely Visible. These will be refined and where possible will bring in reference definitions, for discussion at the next conference call.

Reviewed and discussed User, Organization, Device, and Service Roles:

- Some detailed users roles were simplified by using a more general role name with attributes to specialize that role.
- Specific Organizational Roles will be replaced by “customer defined”.

HCD-TNC Binding (Health Assessment)

- **ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idstnc10-20130910.pdf**
- **ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idstnc10-20130910.docx**
- **ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idstnc10-20130910-rev.pdf**

Reviewed terminology sections, reference changes, and new sections and revisions in chapter 4.

ITU-T X.1254 Entity Authentication Assurance Framework

Ira gave an overview of this framework and its potential applicability to PWG IA&A specifications.

- Scope – managing entity authentication assurance
    - Specifies four levels of entity authentication assurance

  - Specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance
  - Provides guidance for mapping other authentication assurance schemes to the four LoAs;
  - Provides guidance for exchanging the results of authentication that are based on the four LoAs
  - Provides guidance concerning controls that should be used to mitigate authentication threats

- Terms

  - Assertion, Authentication, Claim, Context, Credential, Entity
  - Identity, Multifactor Authentication, Non-Repudiation
  - Identity Proofing, Mutual Authentication, Transaction
  - Trust Framework, Verification

- Levels of Assurance (LoAs)

  - 1 (Low) – little or no confidence in claimed or asserted identity
  - 2 (Medium) – some confidence in claimed or asserted identity
  - 3 (High) – high confidence in claimed or asserted identity
  - 4 (Very High) – very high confidence in claimed or asserted identity

- Actors

  - Entity – device, service, user, application, etc.
  - Credential Service Provider (CSP)
  - Registration Authority (RA)
  - Relying Party (RP)
  - Verifier
  - Trusted Third Party (TTP)

- Entity Authentication Assurance Framework Phases

  - Enrollment Phase
    – application and initiation (websites, badges, forms, etc.)
    – identity proofing and verification (entity identity attributes)
    – record-keeping (identity, verification, accept/deny/referral)
    – registration (during enrollment or later at first access)

  - Credential Management Phase
    – creation, binding to entity, issuance, activation
    – storage (secure handling, according to target LoA)
    – suspension, revocation, and/or destruction (CRLs, etc.)

    – renewal and/or replacement
    – record-keeping (creator, identity, entity, status)

  - Entity Authentication Phase
    – authentication (including LoA of each identity attribute)
    – record-keeping (service provision, compliance, accountability and/or legal requirements)

- Management and Organizational Considerations

  - Service establishment
  - Legal and contractual compliance
  - Financial provisions
  - Information security management and audit
  - External service components (i.e., third parties)
  - Operational infrastructure (i.e., trust frameworks)
  - Measuring operational capabilities

- Threats and Controls

  - Enrollment Phase – impersonation
  - Credential Management Phase – tampering, unauthorized creation, disclosure, unauthorized possession, unavailability, duplication, delayed revocation, repudiation
  - Authentication Phase – keystroke loggers, social engineering, guessing, duplication, phishing, eavesdropping, replay, session hijack, man-in-the-middle, theft, spoofing, masquerade

System Control Service Integration

(We covered this in an earlier session)

- Updated tables in IDS-Model

  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020.pdf
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020.docx
  - ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20131020-rev.pdf

IDS Face to Face Minutes
October 23-24, 2013

Wednesday, Oct 24, 2013

Attendees

Carmen Aubry*	Oce Canon
Tom Benkart*	CC Consulting LLC
Russell Brudnicki	Kyocera
Graydon Dodson*	Lexmark
Gyaneshwar Gupta	Oki Data
Ashlee Holbrook	Lexmark
Ira McDonald*	High North
Joe Murdock	Sharp
Kathy Reese*	Corsec
Brian Smithson	Ricoh
Alan Sukert*	Xerox
Roarke Randall	Toshiba
Michael Sweet	Apple
Lachlan Turner*	CSC
Bill Wagner	TIC
Lida Wang	Kyocera
Rick Yardumian	Canon

*By Phone

Agenda

1. MFP Technical Community vendor face-to-face meeting
   a. Recap of the F2F meeting in Orlando
   b. Discussion of currently open issues and proposed resolutions
   c. Updates from NIAP and IPA (if any)
   d. Plans and schedules
   e. Open discussion
2. Slides for this session are posted either on ftp://ftp.pwg.org/pub/pwg/ids/Presentation/2013-10-24-MFP-TC_F2F.ppt or http://ftp.pwg.org/pub/pwg/ids/Presentation/2013-10-24-MFP-TC_F2F.ppt.
3. Brian discussed the current open issues against Draft 0.6.3 of the Protection Profile for Multifunction Printers as follows:
   a. Issue 1. **User authorization is defined too narrowly** – The MFP Protection Profile (PP) Technical Committee (TC) at its last Face-to-Face in Orlando FL decided that the way to address this issue was to remove the part of the affected sentence that dealt with access control, since it really has nothing to do with user authorization for PSTN fax. The attendees at this session agreed with the TC's resolution.
   b. Issue 2. **Discussion on I&A&A failure including external authentication** – The issue here is whether we should include requirements around what the TOE should do if an external

authentication server such as Kerberos or LDAP times out or fails to authenticate multiple times in succession. The TC had proposed that the MFP PP should not state anything about this particular case, but did agree to look and see what other PPs such as NDPP or ESM had done about this case; turns out that Brian did look and neither PP addressed this case at all.

Those present at this session agreed that if network authentication fails the device should automatically fallback to local authentication, but this shouldn't be stated as a requirement. It was suggested that maybe this should be included in the MFP PP as a App Note, but Brian indicated this may not be a good idea because the Japanese scheme takes App Notes as being requirements. At the end of this discussion all present agreed with the TC proposal.

c. Issue 3. **Audit Log (FAU_GEN.1) Requirements** ***"For "Modification to the group…" -- what additional info should be collected in the audit log?"*** – The TC in discussing this issue decided that we would look at what the other PPs are doing. As was the case for Issue #2 Brian did a search and found that NDPP and ESM either don't include this item at all or don't collect any additional information. Ira suggested that this type of information should be placed in a "best practices" document similar to the PP Guide the P2600 Working Group created for the 2600.x PPs. At the end of this discussion all present agreed that the MFP PP should not include any additional audit log information in this case as a requirement.

d. Issue 4. **Use of the Term "non-fax data" for information flow control SFR** – This issue involves the use of the term "non-fax data" in the flow control requirements for PSTN fax that address network-fax separation, and whether some other approach/term would be better to use. The TC's proposal here was to use the FDP_IFF.1/FDP_IFC.1 requirements from the Common Criteria and specify that they apply specifically to user document and user job data. Brian pointed out that if we use FDP_IFF and FDP_IFC we will need something active to control the flow for these two requirements, or we may need to have an Assurance Component dealing with architecture (since network-fax separation is principally addressed via the system architecture) to evaluate that these two sets of requirements are met.

Alternately, an Extended Component could be used to describe these requirements, similar to the approach the P2600 Working Group took in the 2600.x PPs. It was pointed out that NIAP makes extensive use of extended components (even when sometimes they aren't needed) in the new PPs so we certainly have precedence set here. At the end of the discussion we agreed to continue to look at both approaches and see which one turns out to be the easiest to implement. Brian will assemble a small subgroup of the TC to look at the two approaches.

e. Issue 5. **Additions to required Audit Log entries for job submission and job completion** – The TC didn't finalize a proposal on this item; they wanted to see what vendors were logging for these two elements first. There was also the issue as to whether we could add additional information for job submittal and/or job completion beyond what is minimally specified and still meet the "exact compliance" requirement NIAP wants the MFP PP to meet.

We agreed that we need from NIAP a clear definition of what "exact compliance" is before we can answer the second question. It was noted that the 2600.x PPs only required job submission, not job completion. The consensus of those present at this session was that we should probably do what 2600.x did in this area in the MFP PP, but there was no firm resolution. This item remains open.

f. Issue 6. **Audit Log Specification Proposed by the PWG** – The PWG at our last Face-to-Face in August had recommended that the MFP PP TC look at the PWG Common Log Spec for audit log entries that should be required in the MFP PP (e.g., the PWG Common Log spec requires job completions to be logged). The MFP PP TC's position is that we are not looking for any additional audit requirements beyond the minimum required. The TC hasn't looked at the PWG Common Log Spec yet, so this issue remains open. It was suggested that some of these additional audit log requirements could be identified as "best practices" is a separate document and/or considered for implementation in a later update to the MFP PP after the initial MFP PP.

g. Issue 7. **Whether OSPs are necessary** – This issue was raised by Mario Tinto, one of the NIAP validators working on the MFP PP. Brian indicated he talked to Mario about this issue, and based on that discussion he feels Mario will withdraw his objection and no change will be needed.

4. Key other points raised in the session that are not on the session slides:

   a. Ira brought up that NIAP is developing a new Protection Profile for the Trusted Platform Module (TPM). NIAP may require that any network-connected device has to have a TPM.

   b. Wi-Fi is definitely out of scope as part of the evaluated configuration for the MFP PP. The reason is because the TC doesn't want the Wi-Fi PP to become applicable to MFPs since many of the requirements in the Wi0Fi PP don't apply to MFPs.

   c. We have not had any updates from either NIAP or the IPA (Japanese Scheme) since the Orlando Face-to-Face (F2F).

   d. The MFP PP for now is not being treated as a collaborative PP (cPP); it is being treated as a bi-lateral PP.

   e. There have been no changes in the MFP PP schedule communicated by either NIAP or IPA since the Orlando F2F. It was noted that NIAP is saying on its web site that the MFP PP will be completed by end of 2014. Our best guess is that we expect the TC to finalize PP by mid -2014 and then have the rest of 2014 for review and approval. After that there will likely be an 18-24 month transition period from the 2600.2 PP after approval of MFP PP until the MFP PP becomes mandatory.

   f. We suspect that the Common Criteria Development Board and NIAP want to align the MFP PP with what the USB Working Group is doing in developing the new USB Devices PP.

   g. Brian's goal in having these types of F2F meetings with the PWG IDS is to get more vendors involved in developing MFP PP.

Action items

1. Joe: Update IDS Model according to today's review.
2. Ira: Update the TNC Binding Specification according to today's review.
3. Michael, Ira, Joe: Look into how to make PWG specifications more visible, through a registry or repository, perhaps talk to Anne Price at TCG.

Next Steps / Future Activities

- Definition of core set of Policy Attributes
  - Addition to IAA specification
  - Harmonize with TCG TNC specifications

  - Define access control values
  - IDS model specification
  - IDS health remediation
    - Integrate with TCG TNC Work Group
- No conference call on November 4, 2013. Next Conference Call is December 2, 2013.
- Next Face-to-Face Meeting is February 4-6, 2014 in Irvine CA (Samsung)