IDS Face-to-Face Minutes
August 24, 2016

Meeting was called to order at approximately 9:00 am local August 24, 2016.

Attendees –

Shivaun Albright*	HP Inc.
Tom Benkart*	
Jeff Binford*	Lexmark
Gerardo Colunga*	HP Inc.
Graydon Dodson	HP
Gyaneshwar Gupta*	Oki Data
Katuya Katayama	Intel
Smith Kennedy	HP Inc.
Jeremy Leber*	Lexmark
Brian Smithson	Ricoh
Alan Sukert*	Xerox
Michael Sweet*	Apple
Bill Wagner*	TIC
Craig Whittle	Sharp
Rick Yardumian	Canon

*Attended by phone

Agenda Items

Note: Meeting slides are available at http://ftp.pwg.org/pub/pwg/ids/Presentation/2016-08-24-IDS-F2F.pdf.

1. Minute Taker
   - Alan Sukert taking the minutes
2. Agenda:
   - Introductions, Agenda Review, Status
   - Review Issues/Concerns on new HCD PP
   - Review issue resolution process
   - Common Criteria/ICCC Update
   - Wrap-Up
3. Went through the PWG Intellectual Property policy.
4. Review Issues/Concerns on new HCD Protection Profile (PP)

   The following points were made as part of the discussion:

   - Brian noted that the Korean Scheme requires conformance to both the IEEE 2600.2 PP and the new HCD PP.
   - The Key Transport Security Functional Requirement (SFR) (FCS_COP.1 (i)) has no assurance activities associated with it. Means if we include that SFR we either have to get an interpretation from NIAP (the US Scheme) / JISEC (the Japanese Scheme) as to what the assurance activities for this SFR are or propose something ourselves.

- The use of Solid State Drives (SSDs) and how some of the SFRs like Key Destruction (FCS_CKM.4) apply when you cannot do overwrite was discussed. It was pointed out that the Application Note with the FCS_CKM.4 SFR does indicate that the overwrite requirement would not apply if an SSD was used; the question arose whether NIAP concurred with that position. Alan indicated that he raised this issue with NIAP via the format Technical Rapid Response Team (TRRP) process in February 2016 and still has not received a formal reply from NIAP to it. It was pointed out the Full Disk Encryption (FDE) collaborative PP (cPP) "punted" on the use of SSDs but they did put something about SSDs in the supporting documents that accompanied this cPP.
- Someone also brought up the concern about what to do with full chip erase.
- It was indicated that with the new HCD PP the creation of the Key Management Description, TOE Summary Spec and Entropy documents would be challenging because of the detailed content/format requirements for these three documents in the new HCD PP.
- Brian pointed out he is having an issue with how to handle "true random number generators" (TRNGs). He asked for an interpretation from NIAP and did not get a clear answer but what he did get from NIAP was sufficient to proceed.
- Concern was expressed about the potential for differences between the interpretations on the SFRs, assurance activities, etc. in the new HCD PP we get from our respective evaluation labs and the corresponding interpretations we might get from NIAP. If they are different it puts us vendors in a difficult position and could significantly delay completion of certifications against the new HCD PP. Our best hope is that the evaluation labs are in continuing contact with NIAP so the possibility of differing interpretations is minimized.
- There was also a concern expressed that NIAP has not given specific direction on which crypto-related SFRs we can skip full testing for if we use FIPS-certified algorithms/modules. Right now, there is only general guidance provided by NIAP on this subject. It was suggested that we look for precedence in other STs such as for the Network Device PP (NDPP) that have been accepted by NIAP. It was also pointed out that NIAP is more interested in crypto algorithm FIPS-compliance than in crypto module FIPS-compliance. Finally, it was pointed out that the current process does not adequately address SFRs that do not explicitly cover crypto algorithms as to which of them may have their assurance activities "waived" by using FIPS-certified algorithms/modules.

5. We discussed in some length our experiences with the NIAP TRRT process.

   The following points were made as part of the discussion:

   - The TRRT process is designed to provide solutions to issues raised by vendors and evaluation labs in a timely manner. The view of the attendees was that the TRRT process is somewhat "opaque" and there are issues with what happens if someone from NIAP leaves (Alan indicated that that was one of the reasons the NIAP response to his SSD question has taken so long), how anyone can check the status of their requests and whether NIAP publishes a list of all the feedback and responses they provide via the TRRT process.
   - Consensus was that the TRRT process as currently being implemented by NIAP took either very fast (few days to get a response) or very long (months to get a response) – nothing in between.
   - A serious concern expressed was, since the new HCD PP is a bi-national PP between the US and Japan, whether the guidance being published by NIAP against this PP was being coordinated with the corresponding guidance from JISEC. So far, the limited evidence is that NIAP is coordinating responses with the Japanese Scheme.

6. Discuss the next steps after the HCD PP

   - No plans now to update the HCD PP.
   - Japan and Korea may be willing to sponsor the effort to eventually create an HCD cPP and write the Essential Requirements, which is the first step in this process. However, nothing has actively been done yet by either scheme towards that end (nor will it be done anytime soon) because both schemes are working on higher priority issues now.

7. Some other items discussed:

   - Someone asked when the next NDPP update would occur. No one attending the meeting knew the answer.
   - Someone asked about the status of version 2.0 of the FDE cPP. The response was that that update had not been started yet and was not slated for completion until at least a year from now.
   - Brian mentioned that the NDPP has a "NIT". This is a group of industry and government people who are a subset of the full NDPP international Technical Committee (iTC) and who work NDPP issue with NIAP cooperatively, with NIAP taking the lead. It was suggested that maybe we should have something like that for the HCD PP so we can cooperatively work with NIAP to resolve issues, or at the least establish a working relationship with the HCD PP TRRT. This would be especially helpful to resolve printer-specific issues.

     It was mentioned that the Common Criteria Users Forum (CCUF) has established a set of "cohorts" that provide communication lines between the CCUF and NIAP to discuss issues. It was suggested that since at least two of the members of the IDS WG (Alan and Brian) are members of the current cohort that is to start in Sep 2016 that they bring up the idea of establishing an HDP PP at the next CCUF-NIAP cohort meeting. Alan took the action to bring the topic up at that meeting.
   - We have to find a way to 'internationalize" the HCD PP more. Right now there are many references in the HCD PP to FIPS documentation, but not all countries (e.g., Korea) recognize FIPS - Korea only recognizes its own crypto standards for example.
   - Need to formally replace Scheme recognition of the old IEEE 2600.2 PP for HCDs (for example, earlier it was stated that Korea recognizes both IEEE 2600.2 and the new HCD PP).
   - Someone asked about the status of FIPS 140-3. This version will recognize ISO standards instead of FIPS standards so it will be more internationally accepted, Looks like this update is at least a year away, and maybe even longer.
   - It was mentioned that the new HCD PP is not recognized yet in Europe, Not sure that is true; may want to see if we can confirm that statement.
   - There was discussion of whether something more formal could be done with the HCD PP under the auspices of the PWG. It was suggested that maybe the HCD PP could be made a PWG standard to give it some more formal industry status. We discussed briefly how that might be done under the auspices of the PWG IDS Working group – it would require a charter update, generation of a white paper and then go through the PWG standards process. Alan agreed to look into this further but no commitment was made to do anything.

Wrap Up

- No future IDS Conference Calls are scheduled at this time. However, Alan did propose that we set up at least a month conference call to just keep in touch and provide a forum for discussing issues, status and anything related to the HCD PP. Alan took the action to set up a conference call sometime in September.
- No future IDS Face-to-Face Meetings are planned at this time.
- Actions:
  a. Al Sukert: Bring up the issue of an HCD PP "NIT" at the next CCUF-NIAP Cohort Meeting on Sep 8th.
  b. Al Sukert: Set up an IDS Conference Call sometime in September (probably towards the end of the month).

The meeting was adjourned at approximately 10:35 am local on August 24, 2016.