IDS Face-to-Face Minutes
August 29, 2019

Meeting was called to order at approximately 9:05 am local August 29, 2019.

Attendees –

Smith Kennedy	HP Inc.
Cihan Colakoglu	Kyocera
Sean Kau	Google
Jeremy Leber	Lexmark
Ira McDonald	High North
Alan Sukert	Xerox
Michael Sweet	Apple
Bill Wagner	TIC
Rick Yardumian	Canon

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2019-08-29-IDS-F2F.pdf.

1. Minute Taker
   - Alan Sukert taking the minutes
2. Agenda:
   - Introductions, Agenda Review, Status
   - Discuss results of latest HCD TC Meetings and potential HCD cPP content
   - HCD Security Guide 1.0 Status
   - Wrap-Up / Next Steps
3. Went through the PWG Intellectual Property policy.
4. The status of proposed Version 1.1 of the Hardcopy Device (HCD) Protection Profile (PP) was discussed. NIAP has indicated that it will not accept any changes to HCD PP version 1.0; it is waiting for HCD collaborative PP (cPP) version 1.0. So that means that HCD PP v1.1 will not be approved or published. However, the work we did on it is not totally wasted in that the draft HCD PP 1.1 will be the basis for HCD cPP 1.0.
5. We then discussed the status of the HCD Technical Community (TC) transition towards becoming an HCD international TC (iTC). The latest status was that the Common Criteria Development Board (CCDB) has approved both the Essential Security Requirements (ESR) and Terms of Reference (ToR) documents submitted to the CCDB by the HCD Working Group (WG) (which consists of the Japanese and Korean Schemes) at the April 2019 CCDB Meeting in Rome. Both the ESR and ToR were then submitted to the CC Management Committee (CCMC) for its approval; once the CCMC approves both documents we can officially form an HCD iTC.

   The HCD WG is working very closely with the CCMC to obtain CCMC approval before the upcoming HCD TC Face-to-Face Meeting which will be held Sep 26th in Singapore.

6. We then discussed issues associated with the transition from an HCD TC to an HCD iTC and what the content of an HCD cPP version 1.0 might be. Some of the key points from this discussion were:

   - Given that the old "IEEE 2600" HCD PPs are set to expire at the end of 2019, many Schemes who are certifying HCDs against these old HCD PPs may no longer be able to do that. The reason these older "IEEE 2600" HCD PPs will expire at the end of 2019 is that the IEEE has a 10 year

expiration date on all IEEE standards unless there is an effort to update or resubmit the standard to the IEEE. Since these "IEEE 2600" HCD PPs were approved by the IEEE in 2009 and because of the new HCD PP v1.0 there was no desire to form an IEEE subgroup to resubmit or revise these 10-year old PPs to the IEEE, the "IEEE 2600" HCD PPs will expire at the end of 2019. That means that as of Jan 1, 2020 no one will be able to obtain any of the "IEEE 2600" HCD PPs from the IEEE. What this will mean to any Schemes that are certifying products against the "IEEE 2600" HCD PPs is unknown, but it puts an increased emphasis on getting on HCD cPP v1.0 out as quickly as possible, given the fact that the current HCD PP is a bi-national PP of the US and Japan and is only recognized by the US, Japan, Canada and Sweden for certification of HCDs.

- The upcoming HCD TC Face-to-Face on Sep 26th will be divided into two parts: the first 4 hours will be devoted to technical issues regarding the HCD TC and cPP and the last 4 hours will be devoted to issues in setting up the HCD iTC.

- There will be multiple issues in forming the HCD TC which are listed on the meeting slides. Some additional issues we discussed at this meeting were:

    o Timing of HCD iTC Conference Calls. Since the iTC will have representatives from North America and Asia finding a common time to hold Conference Calls will be difficult. Right now they are being held at 8PM ET which is 9AM in Korea. We'll have to look at whether we continue that or have meetings where times are rotated to be good for North America / Europe one time and good for Asia another time. Just one of the many issues you face when forming an iTC.

    o Much like what is now being done with the Network Device (ND) iTC, Ira suggested that we split up the technical work of creating the cPP into subgroups with each subgroup looking into the requirements in a different area (like crypto or authentication/authorization or secure protocols). I will bring that idea up at the HCD TC Face-to-Face meeting.

- In discussion as to what should potentially go into HCD cPP v1.0, there was a general agreement that our goal should be that HCD cPP v1.0 is a "modest update" to HCD PP v1.1 that is issued as quickly as possible (to bridge the gap for vendors that certify HCDs in Schemes that do not recognize the current HCD PP) and then we follow that up with an HCD cPP v1.1 update 6 months after v1.0 is issued. The obvious question is what constitutes a "modest update" and what new requirements should go into HCD cPP v1.0. It was also pointed out that the HCD iTC has to be flexible enough to address the continuing and often quick change in the HCD industry and in technology that can drive new requirements that HCDs will have to meet and that need to be reflected in the HCD cPP.

- We then got into a good discussion of what requirements could go into HCD cPP v1.0 beyond those shown in the meeting slides. We did some brainstorming and some of the issues we came up with were:

    o Distributed security model with block chains

    o Wireless (Wi-Fi, Bluetooth, NFC, Cellular 3G/4G/5G)

    o Advanced cryptographic techniques like hash-based signatures

    o Mobile (e.g., guest authentication, printing, scanning)

    o Integrating differences among national cryptographic requirements – cryptographic agility

- o Secure software/firmware and trusted updates for companies with sites in multiple countries

  Ira mentioned that the ND iTC was updating the ND cPP to sunset any TLS cipher suites with RSA key generation that have keys less than 3072 bits; that goes beyond the new NIST SP 800-56B requirement that sunsets any TLS cipher suites with RSA key generation that have keys less than 2048 bits. We'll have to see if that is something the HCD iTC wants to tackle in HCD cPP v1.0.

- Alan gave an idea of an aggressive schedule that he will discuss at the HCD TC Face-to-Face that will get us an HCD cPP v1.0 in 18 months to help close the gap mentioned above because of the archiving of the IEEE 2600 HCD PPs. The schedule is as follows:

  - CCMC approval of creation of HCD iTC – Sep 2019
  - First HCD iTC F2F Meeting – Sep 2019
  - First draft of HCD cPP v1.0 – Jun 2020
  - Updated draft of HCD cPP v1.0 – Sep 2020
  - HCD cPP v1.0 submitted for approval by HCD iTC membership – Jan 2021
  - HCD cPP v1.0 submitted to CCDB for approval – Mar 2021
  - HCD cPP v1.0 published – Jul 2021

- Ira went through the status of the PWG Hardcopy Device Security Guidelines he is preparing. There has been no update since the April IDS Face-to-Face meeting, but he hopes to be able to work on it again starting in October. Ira indicated that the Security Guide will mainly have guidance on current security technology being implemented in HCDs, but there will also be a brief chapter on advanced cryptographic techniques being looked at now.

- Finally, Alan mentioned that there is a major update to the ISO 15408 Common Criteria standard. He had thought that maybe he could get copies of the proposed changes for the IDS WG to look at, but that is not likely. Instead, he was asked if there were slides that indicate what the changes are. Al said that there were, and he would provide them to the IDS WG.

Wrap Up

- Next steps will be to:
  - Implement the transition from the HCD TC → HCD iTC
    - Determine and install "officers"
    - Set up meeting cadence, iTC membership, etc.
    - Have the first iTC meeting
  - Start work on HCD cPP v1.0
    - Develop plan for development, review and release of HCD cPP v1.0
    - Determine content scope
    - Initiate "transition" of HCD PP v1.1 into first draft of HCD cPP v1.0
    - Update and review drafts as necessary to create "final" version
    - Get iTC review and approval for "final" version
    - Release HCD cPP v1.0

- Next IDS Conference Call will be on Sep 19, 2019 to help Al prepare for the Sep 26th HCD TC Face-to-Face.

- Next IDS Face-to-Face Meeting will be at the Nov 13-14, 2019 PWG Virtual Face-to-Face.

Actions:

- Al Sukert to send the IDS WG slides on the proposed changes to ISO 15408.

The meeting was adjourned at approximately 10:55 am local on August 29, 2019.