IDS WG Meeting Minutes
September 30, 2021

This IDS WG Meeting was started at approximately 3:00 pm ET on September 30, 2021.

Attendees

Matt Glockner	Lexmark
Erin Huber	Xerox
Alan Sukert	
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the discussions at the HCD iTC Meetings since the IDS Face-to-Face Meeting on 8/19/21.
   - Status of the HCD Security Guidelines
   - Proposed changes to the iTC Development Process
   - Round Table Discussion
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust- policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al reviewed what was discussed at the Hardcopy Device international Technical Community (HCD iTC) Meetings since the last IDS Face-to-Face Meeting on 8/19/21. The main topics discussed at these meetings were:
   - Most of the work done by the HCD iTC since the August IDS Face-to-Face Meeting was in addressing comments against the HCB cPP and HCD cPP 3rd internal drafts so that the 1st Public Drafts of both documents could be published.

     The HCD iTC was able to address all submitted comments against the HCD cPP 3rd internal draft and the 1st Public Draft of the HCD cPP was created on 08/30/21. After a short internal review to make sure all comments were integrated into the draft properly the HCD cPP 1st Public Draft was released for public review on 9/2/21. The 1st Public Draft of the HCD cPP has been posted on the Common Criteria Portal at https://www.commoncriteriaportal.org/communities/hardcopy_devices.cfm; the "HCD cPP draft for public review draft 1" link takes you to https://github.com/HCD-iTC/HCD-iTC-Template/blob/Review/HCD_cPP_DRAFT_v0.10_2021-08-30.pdf where you can see the PDF version of this draft. The comment period for this 1st Public Draft goes through October 8th, so if anyone seeing these minutes wants to review and comment on this draft there still is time – just follow the directions in the Common Criteria Portal link for the HCD iTC on how to report any comments to the HCD iTC.
   - There was a review of a final updated JBMIA proposal for the **FPT_KYP_EXT.1 Protection of Key and Key Material** SFR. This update was to amend the proposed application note to add examples to clarify when a key is not part of a key chain. The HCD iTC agreed on a reworded Application Note that made the newly added text by JBMIA clearer and more understandable. Al went quickly through the slides of the full JBMIA final proposal for this SFR that the HCD iTC finally accepted and that was implemented in the 1st Public Draft of the HCD cPP.
   - JBMIA also introduced a proposal to update the SFR FDP_RIP.1/Overwrite that addresses Image Overwrite and its accompanying Assurance Activities in the HCD SD. The crux of the issue is that as currently stated this SFR only allows for the use of the image overwrite method to make residual image data stored on non-volatile storage on an HCD irretrievable. However, with the

advent of Self Encrypting Drives (SEDs) where the image overwrite method will not work, some type of cryptographic erase method will be necessary. The JBMIA proposal is to modify the FDP_RIP.1/Overwrite SFR to allow cryptographic erase as an option in addition to image overwrite to accommodate the use of SEDs, TPMs, etc. This also required modification of the associated Test Assurance Activities for this SFR to point to FCS_CKM.1 for verification of key destruction, since cryptographic erase involves destruction of the key used to encrypt the residual image data in question.

The HCD iTC discussed but deferred this proposal to after the 1st Public Draft of the HCD cPP was published. This becomes important because of the next topic.

- Al then discussed a comment from JISEC (the Japanese Scheme) against the 1st Public Draft of the HCD cPP that was discussed for most of the 9/27/21 Meeting. The comment was against wording the Security Problem Definition (SPD) portion of the HCD cPP – specifically, the Organization Security Policies section dealing with Image Overwrite. In that section it states "Such customers desire that the image data be made unavailable by overwriting it with other data or by destroying its cryptographic key." JISEC wanted the "or by destroying its cryptographic key" portion removed because destruction of cryptographic keys is already addressed by the two key destruction SFRs FCS_CKM_EXT.1 which says that the keys must be destroyed when no longer needed and FCS_CKM.1 which states how they will be destroyed.

  Most agreed that the two key destruction SFRs do cover destroying the cryptographic key used to encrypt the residual image data on an SED, and therefore the phrase could be eliminated on that basis. However, the discussion at the HCD iTC Meeting then got back to the very issue that was the basis of the JBMIA proposal mentioned above – if we remove this phrase, we are in essence saying that the HCD cPP will only support the image overwrite method and not support cryptographic erase for making residual image data unavailable. It was clear the HCD iTC was split on that point and agreed to continue the discussion at its next meeting.

  At the discussion at the IDS WG Meeting l mentioned that he favors implementing the JBMIA proposal and not removing the phrase from this section. Al also mentioned that the Security Objective for Image Overwrite in Section 4.1.12 does not mention cryptographic erase at all and needs to be modified also.

  At the meeting Bill made the point that Image Overwrite is a particular method for making the image data unavailable, so it was suggested that if cryptographic erase is included the sections on Image Overwrite might need to be renamed to something more general. It was not clear there was any consensus on the part of the members present at the IDS meeting what to do here either.

- Finally, Al quickly reviewed the latest HCD iTC schedule to give an update on where the HCD iTC was compared to the latest plan. Looking at the schedule, things were not as bad as they could be:

  - All 3rd Internal Draft activities were completed, albeit later than planned
  - 1st Public Draft of the HCD cPP was released on 9/2, only 3 days later than planned
  - The 1st Public Draft of the SD was finally made available for a final review on 9/29' should be released probably around 10/5. So, it is running roughly a month behind schedule.

  Depending on how many comments we get we may be able to get close to the 12/13 date for the HCD SD, but my guess is that it will be closer to the beginning of January for the 2nd Public Draft of the HCD SD.

4. Ira wasn't present at the meeting so there was no status presented on the HCD Security Guidelines.
5. For the last item Al reviewed results of an advisory group he was on to help NIAP and the Common Criteria Development Board update the process an iTC uses to create a cPP and an SD. The current process is 31 steps and is very cumbersome, bureaucratic and in some cases does not reflect what actually happens in developing and approving a cPP and an SD.

The major changes to the process that are being proposed are:

- Currently the process states that anyone (denoted as the 'Initiator') can initiate a request to the CCDB to startup an iTC to create a CPP and SD for a class of products for which no cPP/SD currently exists – could be an extension of a known technical area like 3D printing or some new technical area. Typically, the 'Initiator' is a Technical Committee or a member of the CCDB but it could be one or more Subject Matter Experts would want to form an iTC in their area of expertise.

  The process as it is documented now states that once the 'Initiator' makes a request to the CCDB to initiate an iTC and the CCDB agrees, the CCDB creates a Working Group (WG) that consists of at least two members of the CCDB (i.e., at least two Common Criteria Schemes) and the WG then creates and gets public review and approval of the Essential Security Requirements (ESR); the ESR basically contains the high-level requirements and threat environment for the class of products the iTC is to create the cPP for.

  The problem with the WG creating the ESR is that often the high-level requirements of the SMEs and vendors of the technologies involved don't get addressed adequately by the WG, and once an ESR is approved it is difficult to change.

  The revised process will now allow the 'Initiator' to create the ESR, which will mean that the person(s) who want to create the iTC and the cPP and who will likely have the technical knowledge of what requirements are needed and what threats a=have to be addressed will now be able to define the ESR.

- The second major change deals with the multiple steps involved in creating the cPP and SD. Currently there are 8 steps in the iTC process that involve creating, reviewing and approving the SPD, creating the requirements, reviewing comments and position statements and finally adjudicating comments that all lead up to publishing the cPP and SD for Public Review. In the updated process these 8 steps have been reduced to one simple step – iTC drafts the cPP and SD.

- The last major change deals with how the cPP and SD are finally published and approved. The 4 steps in the current process do not reflect how this is actually done in practice today. What is done today is that the cPP and SD are both published after they have been publicly reviewed and all comments have been adjudicated. Once the cPP and SD have been published, the first time the published cPP and SD are used to certify a product two important things happen:

  - The cPP will itself be certified against the criteria for evaluating cPPs per ISO 15409 and the CEM at the same time the product is being certified to ensure the product conforms to the cPP.

  - If the product is successfully certified by determining by the evaluation lab that it meets the Evaluation Criteria in the SD, that will constitute CCDB approval of the SD.

  The iTC process will be revised to reflect this current behavior in how the cPP is certified and the SD is approved by the CCDB.

6. Round Table:

   Conferences of Note:

   - Fall 2021 CCUF Workshop is October 13-14, 2021. Registration is currently underway – link is https://www.ccusersforum.org/event/the-20th-ccuf-workshop/. Sessions will be 9A – 12N ET on 10/13 and 9A – 11A ET on 10/14.

   - International Common Criteria Conference, Oct 19-20, 2021. Note: Early registration extended to Oct 8th.

7. **Actions:** None

Next Steps

- The next IDS WG Meeting will be October 14, 2021 at 3:00P ET / 12:00N PT. Main topics will be review of the recent HCD iTC Meetings, HCD Security Guidelines Status Update, review of the CCUF Workshop and Round Table.