IDS WG Meeting Minutes
May 26, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on May 26, 2022.

Attendees

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Smith Kennedy	HP
Jeremy Leber	Lexmark
Alan Sukert	

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the HCD iTC Meetings since our last IDS WG Meeting on 4/28/22
   - Presentation by Smith Kennedy on IPP Authentication
   - Round Table
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. Before starting the discussions Al talked about the change in when IDS Meetings will occur in the future. IDS and IPP share the Thursday 3PM time slot on alternate weeks. However, because of conflicts and other issues IDS was asked, and agreed, to switch alternate weeks with IPP starting in June. So, our next IDS WG Meeting will be on Jun 16th and then future IDS WG Meetings will be every two weeks after June 16th.
4. Al then provided a summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 5/12/22.
   - The vast majority of the time spent at the HCD iTC meetings since the last IDS WG Meeting was spent continuing work on finalizing the new FPT_WIPE_EXT SFR and its associated Assurance Activities (AAs). Specifically, the HCD iTC work to address comments to the FPT_WIPE_EXT SFR and AAs from the Korean Scheme, from NIAP and now from JISEC. It is important that the HCD iTC get buy-in from NIAP for the HCD cPP and for this SFR because the HCD iTC wants any HCD that is certified against the HCD cPP/SD to be accepted by NIAP so it can be included on the NIAP Product Compliant List (PCL). That will allow that HCD to be sold to the US Government.
     - As stated in the minutes for the 5/19/22 IDS Face to Face Meeting and 5/12/22 IDS WG Meeting, the Secure Erase Subgroup and full HCD iTC came up with a hopefully final proposal to address the NIAP, ITSCC and JISEC comments that were detailed in the above two sets of meeting minutes. This “final” proposal basically included:
       - Replacing FDP_RIP.1/Overwrite with

         FDP_UDA_EXT.1 EXTENDED: The TSF shall ensure that any previous information content stored on a [selection: wear-leveled storage device, non-wear-leveled storage device] of a resource is made unavailable [selection: by overwriting data, by destroying its cryptographic key] upon the deallocation of the resource from the following objects: D.USER.DOC.

       - The Updating FPT_WIPE_EXT to be:

         FPT_WIPE_EXT.1.1 The TSF shall ensure that any previous customer-supplied information content of a resource in non-volatile storage is made unavailable upon the

request of an Administrator to the following objects: [*D.USER, D.TSF*] using the following method(s): *cryptographic erase and* [**selection:**

- *logically addresses the storage location of the data and performs a [**selection:** single, [**assignment:** ST author defined multi-pass]] overwrite consisting of [**selection:** zeroes, ones, pseudo-random pattern, any value that does not contain any CSPs],*
  - *block erase,*
  - *media specific eMMC method,*
  - *media specific ATA erase method,*
  - *media specific NVMe method,*
  - *no other method*

] that meets the following: [*no standard*].

Application Notes
In this context, "cryptographic erase" encompasses any method that destroys the decryption key or the key that protects the decryption key while leaving encrypted D.USER and/or D.TSF on the storage media. This would include, for example, some ATA commands that only destroy the key. Note that key destruction is a mandatory requirement covered by FCS_CKM.4 and FCS_CKM_EXT.4. cryptographic erase also uses the method described in FCS_CKM.4 and FCS_CKM_EXT.4 for key destruction.

If the "overwrite" method is applied to any wear-leveling storage media, the ST author must assume that some encrypted D.USER and/or D.TSF remains on that storage media and document this condition in the TSS.

If a single magnetic drive is partitioned, and one or more of the partitions do not contain D.USER or D.TSF, the ST author should clarify whether the partitions not containing the data are included in the wipe function.

Wear-leveling storage media is characterized by differentiating between logical and internal physical addressing to enable longevity enhancements via erasures and re-writes being distributed across the physical media.

- Updating the Assurance Activities as indicated in the previous meeting minutes.

The next step was to give the full HCD iTC membership one week (which was the week of May 16th) to comment on the "final" proposal. During that week we received two sets of comments. One was against Test 5 of the Assurance Activities that stated that since cryptographic erase was now a mandatory option that test case was no longer a conditional test, so we removed the fact that Test 5 was conditional of cryptographic erase being selected. The other comment was to remove "cryptographic" from a key destruction reference in the FPT_WIPE_EXT Application Note because it was unnecessary.

The WIPE proposal now goes to JISEC and ITSCC for their comments due June 6th so the two new SFRs and AAs can be folded into the HCD cPP and HCD SD in time to meet the Jun 13 date for publishing the Final Drafts.

- Al then brought up again the issue of NTP. The HCD iTC has still not decided whether or not to include NTP in v1.0 because of the "secure NTP" requirements in the ND cPP version that would be used. More specifically, the NTP requirement from the ND cPP that is of concern is:

  FCS_NTP_EXT.1.2 The TSF shall update its system time using [selection:
  - Authentication using [selection: *SHA1, SHA256, SHA384, SHA512, AES-CBC-128, AES-CBC-256*] as the message digest algorithm(s);
  - [selection: *IPsec, DTLS*] to provide trusted communication between itself and an NTP time source.

  ].

  The hope is that this will be resolved once and for all at the next HCD iTC Meeting on May 16th.

What was different this time was that the NIAP representative was at the meeting, and he indicated that NIAP's position is that it would favor that HCD cPP v1.0 include NTP. The HCD iTC agreed to give JBMIA and HCD iTC members one more week until 5/30 to discuss the issue, and then it would decide once and for all whether NTP would be in v1.0 at the next HCD iTC Meeting on 6/1.

5. While we were waiting for Smith to attend we got into a wide ranging but good discussion on several issues related to Common Criteria. The key points of these discussions were:

   - Matt asked whether NIAP Policy 5 would apply to the HCD cPP. Unfortunately, since NIAP is not a sponsor of the HCD ITC it would not apply to the HCD cPP, so the vendors (or more correctly the labs who do the evaluations) would have to do all of the cryptographic testing required in the HCD SD. However, it was mentioned that each country could issue Position Statements on the published HCD CPP and HCD SD. So, it is possible that NIAP could issue a Position Statement that could state that for purposes of being placed on the PCL a valid CAVP certificate could be accepted in lieu of some of the cryptographic testing for HCDs certified against the HCD cPP.

   - Another question was asked about the transition period from the current HCD PP to the HCD cPP once the HCD cPP and HCD SD are published. Al indicated that it will probably be Scheme-dependent. From his past experience with NIAP and JISEC, NIAP will probably make the new HCD cPP effective immediately and archive the HCD PP as soon as the HCD cPP is approved by NIAP; JISEC, on the other hand, will most likely have some type of transition period between 18 months and two years where certifications against both the HCD PP and HCD cPP will be allowed before archiving the HCD PP. Al has no experience with ITSCC so he doesn't know what Korea will do but he suspects they will do some type of transition like JISEC.

   - A question from Smith opened a discussion into the whole process of how testing works within a certification of a product under Common Criteria (CC). The process can be described as follows:

     a. The evaluation of a product that is being certified under Common Criteria is done by an evaluation lab - in the US it is called a CCTL (Common Criteria Test Lab). Only labs that are accredited by each country's Scheme[1] are allowed to perform evaluation of products for Common Criteria certifications for approval by that Scheme.

     b. The Security Target (ST) defines the Security Functional Requirements (SFRs) that the product must meet to be approved by the Scheme for certification as well as the Security Assurance Requirements (SARs) that the evaluation lab must assure are also met for the product to be approved for certification.

     c. In the current CC methodology, every product must show Exact Conformance with an approved Protection Profile (PP) or Collaborative PP (cPP); that means it must meet exactly all the SFRs and SARs in the ST or it does not get certified. From a testing perspective that also means that the product must meet all the applicable Assurance Activities (AAs) (both documentation and test) for the SFRs in the ST that are documented in the Supporting Document for the cPP the product is claiming Exact Conformance to.

     d. With the above as a background, the vendor may (but is not required to do so) do its own internal testing to verify that all the SFRs are met. The evaluation lab is required to develop an Independent Test Plan that is reviewed and approved by the Scheme that will approve the certification. This test plan will indicate how the evaluation lab will test the applicable test AAs from the SD, evaluate any SARs in the ST, evaluate the appliable TSS and Guidance AAs in the SD and document any additional tests that the evaluation lab plans to run beyond what is in the SD. This evaluation activity is done in accordance with the Common Methodology for Information Technology Security Evaluation (CEM), which defines the minimum actions to be performed by an evaluator in order to conduct a CC evaluation, using the criteria and

[1]The "Scheme" is the government body in each country which is a signatory of the Common Criteria Recognition Arrangement that is responsible for implementing the Common Criteria for that country. For example, in the US that is NIAP; in Japan it is JISEC and in Korea it is ITSCC

evaluation evidence defined in the CC. The purpose of the Test Plan is to show how the evaluation lab will demonstrate to the Scheme that the product meets the SFRs and SARs and AAs in the ST and SD.

e. Once the Scheme approves the Test Plan the evaluation lab will perform the evaluation activities according to the test plan. It does require that the evaluation lab record the results of each test including screen shots and all test outputs.

f. When the evaluation lab has completed all of its evaluation activities it will create an Evaluation Technical Report (ETR) summarizing the evaluation activities done, the results and the recommendation to the Scheme for either approval or disapproval of certification of the product. The content (and essentially the format) of the ETR is defined in the CEM.

g. The Scheme will review the submitted ETR and can do one of several things – they can accept it as is (that's what you hope for as a vendor); they can send back comments to be addressed (which from experience can sometimes be simple fixes to the report or sometimes can require actual changes to the product and retesting) or they can reject the ETR and require a "go back to Square 1" type of action.

h. Assuming the Scheme either accepts the ETR or only requires changes to the ETR itself, the Scheme (or more specifically the lead individual from the Scheme responsible for that certification) will write an evaluators report, create the certificate, and then post the ST, the Evaluator's Report and the Certificate on the Scheme's certified product list.

Note that steps g. and h. can takes anywhere from a couple of days to several weeks.

- There was a question about what happens after a cPP and SD gets published. The process as it is currently done is as follows:

a. After a cPP and SD gets published, the first time they are used in an actual certification three things happen somewhat in a combination of both sequentially and in parallel:

- The cPP itself will get certified typically by the lab performing the certification of the first product against that cPP. cPPs do get certified against criteria in Part 1 of the CC (ISO/IEC 15408). In response to a question, typically once a cPP is certified against its initial version it is not recertified when subsequent versions are published.

- Per the current iTC Process the SD is supposed to be approved by the Common Criteria Development Board (CCDB). In the current process that approval is done via the first certification of a product using that SD rather than via a separate CCDB approval.

- When the cPP is published Schemes can issue Position Statements concerning that cPP. The Schemes that sponsor the development of the cPP will,certainly issue Position Statements, but any other Scheme is free (but not required) to do so. These Position Statements state that country's position regarding that cPP - e.g., whether or not it will accept certification of products conforming to that cPP; are there any caveats or conditions that accompany that acceptance, etc.

6. Smith indicated he wasn't ready to do his presentation on IPP Authentication at this meeting, but would do it at the next IDS WG Meeting. He did give a brief idea of what he would cover – a survey of the http authentication methods like Kerberos and OAUTH2 that apply to IPP. Smith did say that OAUTH2 was the most difficult one to address.

7. **Actions:** None

Next Steps

- The next IDS WG Meeting will be June 16, 2022 at 3:00P ET / 12:00N PT. Main topics will be review of the HCD iTC Meetings since this meeting and the presentation by Smith Kennedy on IPP Authentication.