IDS WG Meeting Minutes
December 16, 2021

This IDS WG Meeting was started at approximately 3:00 pm ET on December 16, 2021.

Attendees

Erin Huber	Xerox
Ira McDonald	High North
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 Hardcopy Device international Technical Community (HCD iTC) Meetings since the last IDS Workgroup Meeting on 10/28/21.
   - Latest status on the HCD Security Guidelines
   - Thoughts on IDS Workgroup activities in 2021
   - A look ahead to 2022
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 began with a summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 10/28/21.
   - For the most past the main items covered at these meetings was addressing comments against the 1st Public Draft of the HCD collaborative Protection Profile (cPP). The big news was that necessary comments were addressed and the 2nd Public Draft of the HCD cPP – Version 0.11 dated 12/14/21 – was released for public review on 12/15/21. Al indicated that because of the Christmas and New Year holidays, the review period for this 2nd Public Draft of the HCD cPP will last until January 31, 2022.

     Al then went through the list of the key areas that were addressed in this 2nd Public Draft of the HCD cPP:
     - Added the Extended Component Definition for SFR **FIA_X509_EXT.1 X.509 Certificate Validation**
     - Added a note for the optional Organizational Security Policy Purge in Section 3.5.7 indicating that Cryptographic Erase is not included in this optional requirement because it is covered in the mandatory requirement of FCS_CKM_EXT.4 and FCS_CKM.4.
     - Replaced the text of the Application Note for SFR **FPT_KYP_EXT.1 Extended: Protection of Key and Key Material** in the 1st Public Draft to add clarity to what the Application Note was trying to convey.
     - Removed the part of the sentence in the application note in SFR **FCS_KYC_EXT.1.1** (**Key Chaining**) that talks about "keys in areas of protected storage" because keys in areas of protected storage are already discussed in SFR **FPT_KYP_EXT.1 Protection of Key and Key Material** in a superior way.
     - Removed references to SFRs such as FPT_ITT that were not in the HCD cPP.
     - Clarified via an addition to the Application Note that the scope of TST Testing for SFR **FPT_TST_EXT.1 TSF testing** is focused on correct operation of the cryptographic function and detection of malfunctions, since the integrity of the executable code can be guaranteed by SFR **FPT_SBT_EXT Secure Boot.**

  - Corrected the Extended Component Definition for SFR **FPT_KYP_EXT.1 Extended: Protection of Key and Key Material.**
  - Clarified that the requirement in SFR **FPT_SBT_EXT Secure Boot** to use the chain(s) of trust to confirm integrity of its firmware/software using one or more of the selected methods applies only at boot time.
  - Clarified that support for TLS Mutual Authentication and DTLS Mutual Authentication, whether as a client or as a server, are optional in all cases.
  - Corrected numerous incorrect references to Section and Table numbers and SFR names within the document.
    - Corrected the header information for many of the SFRs in the HCD cPP:
    - Security Objective(s) met
    - “selected in” for Selection-Based SFRs
    - Components “Hierarchical to”
    - SFR “Dependencies”
  - Clarified that SFRs **FIA_X509_EXT.1 X.509 Certificate Validation and FIA_X509_EXT.2 X.509 Certificate Authentication** must be selected (they are both Selection-Based Requirements) if ‘X,509 Certificate’ is selected in **FPT_TUD_EXT.1.3 (Trusted Update).**
  - Corrected the publication dates for the ISO/IEC Standard references in several of the cryptographic SFRs.
  - Added AES bit selection option to **SFR FCS_COP.1.1/StorageEncryption**

  Al noted that none of these key areas were major technical issues.

- Al then reviewed the “Cryptographic Erase” issue that had been discussed at the 10/28/21 IDS Workgroup meeting. As a reminder, the issue revolves around the following statement in the Security Problem Definition (SPD) portion of the HCD cPP in the Organizational Security Policies section under the Image Overwrite (Optional) section:

  Such customers desire that the image data be made unavailable by overwriting it with other data or by destroying its cryptographic key.

  JISEC, the Japanese Scheme, submitted a comment against the 1st Public Draft of the HCD cPP to remove this sentence. JISEC does not want Cryptographic Erase (CE) to be included in any of the discussions of Image Overwrite in either the SPD or in the FDP_RIP.1/Overwrite SFR that is the SFR addressing image overwrite. JISEC’s rationale is that CE, which is what self-encrypting nonvolatile storage devices like Self-Encrypting Drives (SEDs) use to make data on the drive irretrievable, is already adequately covered in the HCD cPP via the two “key destruction” SFRs – FCS_CKM_EXT.4 which requires that the encryption keys in these drives be destroyed when no longer required and FCS_CKM.4 which provides the requirements as to how these encryption keys are to be destroyed.

  Essentially the position of the Japanese and Korean Schemes was that the FDP_RIP.1/PURGE SFR was not acceptable for wear-levelling devices because with CE there was a chance that user data could still be left after the CE was done. Both Schemes, however, would support the HCD iTC’s development of a new SFR that could address the issue that didn’t involve a “Purge” function.

  The HCD iTC set up a CE subgroup which after several weeks of work finally came up with a solution. JISEC had wanted to eliminate Image Overwrite, but the HCD iTC convinced JISEC that US customers wanted Image Overwrite and were willing to pay extra for devices with HDD options that had Image Overwrite function.

  The solution was the following new extended SFR **FDP_WIPE_EXT** Data Wiping:

  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): [**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, fixed value(s)],*
- *block erase,*
- *Cryptographic Erase,*
- *[**assignment:** media-specific method(s)]*

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

Application Notes

In this context, “Cryptographic Erase” encompasses any method that destroys 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.

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 perform the Assurance Activities accordingly.

The CE Subgroup also generated a set of Assurance Activities (AAs) that are included in Attachment 1. There were also some proposed additions to the TSS and Guidance Documentation Assurance Activities for **FDP_RIP.1/Overwrite** to clarify that this SFR did not apply to TOEs that store user or TSF data on wear-levelling storage devices.

Bill noted that in the proposal presented to the HCD iTC there was explanatory paragraphs explaining the rationale for the changes to the **FDP_RIP.1/Overwrite** AAs and the new **FDP_WIPE_EXT** Data Wiping SFR. He thought that explanatory text might be useful if it was included in the HCD cPP with each SFR. Al indicated he would bring that up with Kwangwoo Lee when he gets back after Jan 1st.

- Next Al went over some comments from ITSCC (the Korean Scheme) against the HCD Supporting Document that the HCD iTC had not yet reviewed. The important aspect of these ITSCC comments was that they were all against many of the cryptographic SFRs in the HCD cPP and they all requested additional testing of these SFRs, in many cases extensive additional testing.

  Where this is a concern dates back to the current approved HCD PP that HCDs currently are certified against. That PP was a bi-national PP sponsored by the US and Japanese Schemes. The importance of that was that since NIAP (the US Scheme) sponsored the HCD PP, NIAP Policies applied to products certified against the HCD PP. Where that became an important advantage was NIAP Policy 5, which stated that if a Product had a current valid CAVP (NIST Cryptographic Algorithm Validation Program) certificate, testing a many of the cryptographic SFRs could be waived. Since cryptographic SFR testing in vey difficult, costly and time-consuming, the ability to waive much if not all of that testing was a big advantage.

  However, the HCD cPP effort is sponsored by the Japanese and Korean Schemes and not by NIAP. The question that the HCD iTC will need to get answered before the Final Draft gets released for public review is whether both Schemes will allow vendors the same latitude with respect to cryptographic SFR testing and CAVP certificates as was the case for the HCD PP. This is especially true given the additional testing ITSCC wants added to many of the cryptographic SFRs. If such latitude is not allowed vendors and evaluation labs will have to come up with the tools and resources to do the difficult cryptographic testing that formerly was waived.
- Lastly Al went through the current “official” schedule and gave his assessment of where the HCD iTC is against that schedule:

    - Release of the 2nd Public Drafts was scheduled for 12/1. The HCD cPP 2nd Public Draft was released on 12/15 so it is two weeks behind schedule. The HCD SD 2nd Public Draft is not nearly as ready for release because the HCD iTC is still reviewing comments against the 1st Public Draft of the HCD SD and the HCD iTC does not meet again until Jan 10th. Al's best guess is that the HCD SD 2nd Public Draft will be released around the end of January 2022, so it is running around 6 weeks behind the HCD cPP.
    - Comments for the HCD cPP 2nd Public Draft are due by Jan 31st, against 2 weeks after the planned 1/15/22 date. Al felt that 2-week delay would probably remain, so he expected the Final Draft HCD cPP should be released around the end of March 2022.
    - Assuming there will be a one-month review period for the HCD SD 2nd Public Draft, comments against that draft would be due around the end of February or 1st week of March 2022, around 6 weeks after the planned date. Assuming the 6-weeks lag Al would expect the Final Draft of the HCD SD to be released around the end of April 2022.
    - Assuming both the HCD cPP and HCD SD will be published together, Al felt that based on the above his best guess was that both documents would be published sometime in June 2022.

4. Ira had to leave the meeting unexpectedly because of a power outage, but before he left he indicated he will have some free time in early 2022 so he expects to be able to work on the HCD Security Guidelines. So hopefully sometime towards the end of 1Q 2022 we might have an updated draft of the guidelines for the IDS Workgroup to review.
5. Since this is the last meeting of 2021, Al wanted to end the meeting with two things – looking backwards at 2021 and looking forward to 2022 both from an IDS perspective.

   Regarding 2021:

   - Those present felt the IDS WG did a good job of tracking what was happening in the HCD iTC and the status of the HCD cPP/SD. They felt the meetings provided a good overview of what was happening at the HCD iTC meetings.
   - Those present liked the extra topics that Al covered at the meetings like the ENISA Cryptographic Certification (EUCC) or the White House Cybersecurity Executive Order.
   - Al was concerned about lack of attendance especially later in 2021. He even had to cancel a meeting because only 3 persons showed up. Steve mentioned he was the only one from Canon that attended IDS WG Meetings; we have sporadically had attendance at IDS WG meetings from representatives from Xerox, Lexmark and Ricoh.
   - Al felt he was not getting enough support from the PWG SC in terms of attendance at IDS WG meetings.
   - Overall, everyone felt it was a good year.

   Regarding 2022:

   - Bill and others are looking forward to Ira completing (or at least significantly updating) the HCD Security Guidelines.
   - There was a suggestion that in addition to more special topics at the IDS Meetings that Al provide follow-up to the special topics from 2021 such as EUCC and the Cybersecurity Executive Order.
   - Everyone felt there was a need for a Vice-Chair for the IDS WG so Al had a back-up. Al reinforced that idea since, being a retiree, there will come a time in the future – not in the near future – that he will decide to actually retire – and there will need to be someone to take over the IDS WG.
   - IDS WG needs to continue to follow the HCD iTC and the status of the HCD cPP/SD, but Al still wants to start following other HCD standards activities that may be of interest to IDS members.

6. **Actions:** None

Next Steps

- The next IDS WG Meeting will be January 20, 2022 at 3:00P ET / 12:00N PT. Main topics will be review of the 1/10/22 and 1/18/22 HCD iTC Meetings and initial preparation for the February IDS Face-to-Face Meeting on February 10, 2022.

Attachment 1
FDP_WIPE_EXT ASSURANCE ACTIVITIES

The following AAs will be included in the HCD SD for SFR FDP_WIPE_EXT:

TSS
The evaluator shall examine the TSS to ensure that the description is comprehensive in describing what customer-supplied data is to be wiped, where it is stored, and how it is made unavailable.

If the assignment for “media-specific methods” is selected, the evaluator shall ensure that the TSS describes the method in sufficient detail to determine whether any encrypted D.USER or D.TSF remains on the storage media.

If multiple methods are specified, the evaluator shall ensure that the description clearly states what methods are used for each type of storage and/or customer-supplied data.

Regardless of whether Cryptographic erase is implemented or not, the functional requirements FCS_CKM.4 and FCS_CKM_EXT.4 are provided by the TOE. Thus, the evaluator shall check to ensure that this is clearly described in the TSS and the operational guidance.

Guidance
The evaluator shall check to ensure that the operational guidance contains instructions for initiating the Wipe function.

The evaluator shall check to ensure that the operational guidance describes the type(s) of information that is wiped, and the method(s) used.

The evaluator shall check to ensure that the operational guidance describes the indication to administrators that the wipe is in progress (optional) and that the wipe completes.

If a wipe method is used that leaves any encrypted D.USER or D.TSF on the storage media, the evaluator shall check to ensure that the operational guidance includes a statement cautioning the user about that condition.

Regardless of whether Cryptographic erase is implemented or not, the functional requirements FCS_CKM.4 and FCS_CKM_EXT.4 are provided by the TOE. Thus, the evaluator shall check to ensure that this is clearly described in the TSS and the operational guidance.

Tests
Test 1: The evaluator shall perform the following steps to verify that a wipe function can be initiated by an authorized administrator and that the TOE provides feedback about the status of the wipe operation.

1. Submit a print job containing known text strings to the TOE and ensure it is not printed.
2. Initiate a wipe.
3. If the guidance documentation indicates that status information about the wipe operation is provided during the process, the evaluator shall verify that the status information is provided as described.
4. The evaluator shall verify that the indication of completion of the wipe operation is provided as described in the guidance documentation.

All the following tests are dependent on Test 1 being performed.

Test 2: [*Conditional: If the device remains in an operational state after the device is wiped*] The evaluator shall perform the following steps to verify that previously configured administrator accounts no longer grant access.

1. Use a local administrator access mechanism on the HCD to verify that logging in using a previously valid administrator account and password is not successful. If the HCD grants access without prompting for a password, this step is considered successful provided that this behavior is consistent with the installation procedures described in the guidance documentation.

2. Attempt to establish a remote administrator session using the previously configured network interface information for the TOE (i.e., protocol, IP address and port). The HCD should not respond to incoming IP traffic on its network interface.

Test 3: [*Conditional: If the wipe method causes all addressable locations of storage media used to hold D.USER or D.TSF to be set to a fixed pattern*] The evaluator shall verify that locations on the storage media available for D.USER and/or D.TSF have been set to the pattern specified in the SFR. This test may require forensic tools to be installed on the HCD, or for the storage media to be moved to a separate system equipped with forensic tools. At minimum, the evaluator shall examine the storage locations specified in the following table for the specified storage types.

Storage Media Type	Locations Examined
Magnetic Media	1. First 2049 sectors of the disk 2. 129 sectors before and after the middle of the disk, including the middle sector 3. Last 1025 sectors of the disk 4. 10 separate sectors chosen by the tester at random in the remaining area of the disk 5. If the disk has over 268,435,456 sectors (28-bit Logical Block Addressing (LBA) limit) then sectors 268,435,327 to 268,435,585 sectors of the disk 6. If the disk has over 4,294,967,296 sectors (32-bit LBA limit) then sectors 4,294,967,167 to 4,294,967,425 sectors of the disk 7. Sectors that the tester believes should be tested, if any
Wear-Leveling Media (e.g., SSD)	1. First 2049 sectors of the disk 2. 129 sectors before and after the middle of the disk, including the middle sector 3. Last 1025 sectors of the disk 4. 10 separate sectors chosen by the tester at random in the remaining area of the disk 5. If the disk has over 268,435,456 sectors (28-bit Logical Block Addressing (LBA) limit) then sectors 268,435,327 to 268,435,585 sectors of the disk 6. If the disk has over 4,294,967,296 sectors (32-bit LBA limit) then sectors 4,294,967,167 to 4,294,967,425 sectors of the disk 7. Sectors that the tester believes should be tested, if any

Test 4: [*Conditional: If the wipe method leaves encrypted D.USER and/or D.TSF on the storage media*] The evaluator shall verify that the appropriate keys according to the KMD description required by FCS_CKM_EXT.4 has been destructed in the method described in Tests Assurance Activity of FCS_CKM.4.

Test 5: The evaluator shall verify that known text strings for D.USER and D.TSF are not found on the storage media. This test may require special tools to be installed on the TOE, or for the storage media to be moved to a separate system equipped with special tools, provided by the TOE developer if necessary. The evaluator shall examine the storage media specified in the following table for the specified data.

Data Type	Search Patterns
D.USER	Known text from the print job that was submitted to the TOE prior to the wipe being performed
D.TSF	1. The ASCII representation of the IP address assigned to the TOE when it was in operation 2. The hexadecimal representation of the IP address assigned to the TOE when it was in operation 3. The ASCII representation of an administrator account that was configured for the TOE when it was in operation

Data Type	Search Patterns
	4. The ASCII representation of the password for an administrator account that was configured for the TOE when it was in operation