IDS WG Meeting Minutes
May 12, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on May 12, 2022.

Attendees

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Smith Kennedy	HP
Jeremy Leber	Lexmark
Alan Sukert	
Bill Wagner	TIC
Brian Volkoff	Ricoh
Steve Young	Canon

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
   - Preparation for the upcoming IDS Face-to-Face Meeting on May 19th
   - 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. Al then provided a summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 4/28/22.
   - 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.
     a. As stated in the minutes for the 4/28/22 IDS WG Meeting, the NIAP comments centered on four issues:
        - Concern that the "*[**assignment:** media-specific method(s)]*" selection entry in the FPT_WIPE_EXT SFR was too broad and needed to be more specific in terms of the methods specified
        - Whether the FDP_RIP.1/Overwrite SFR applied to wear-leveling devices or not (i.e., was overwrite only allowed for non-wear-leveling devices)
        - Making sure the FPT_WIPE_EXT SFR aligned with FCS_CKM.4
        - Documentation of data on the device should specify encrypted documents

        To address the NIAP comments the following changes were made to the FPT_WIPE_EXT SFR and AAs (changed wording is in bolded text):
        - Removed the sentence "This objective may only be included in STs for TOEs that do not store any D.USER.DOC data on wear-leveling storage devices (e.g., SSDs)." In the Application Note based on a comment Bill made at the 4/28/22 meeting.

- Changed the "*[**assignment:** media-specific method(s)]*" selection entry in the FPT_WIPE_EXT SFR to three new specific method entries:
  - ***media specific eMMC method,***
  - ***media specific ATA erase method***
  - ***media specific NVMe method*** (Note – this was added at the request of JBMIA)
- Modified AA Test 3 to be consistent with the above change as follows:

  Test 3: [*Conditional: If a **media-specific method** or block erase is selected*] Using a debug log or special tooling that the developer shall provide, the evaluator shall verify that the **media-specific method** or block erase command is executed.

  This test verifies the execution of the **media-specific method** or block erase command.
- Added the following to the TSS AA:

  The evaluator shall ensure the storage medium(s) subject to overwrite are identified and the storage medium(s) leverage functionality that matches the selection on wear-leveling.

  The evaluator shall examine the TSS to ensure that the TSS describes the type(s) of overwrite (e.g., single overwrite with zeros) of D.USER.DOC that the TOE performs.
- Add the following to the Guidance AA:

  The evaluator shall check to ensure that the operational guidance describes the type(s) of overwrite (e.g., single overwrite with zeros) of user document data that the TOE performs.
- Removed the following from the TSS AA:

  The evaluator shall review the types of storage devices and determine that all wear-leveling types of storage (e.g., SSDs) are not cleared solely by an "overwrite" method, the TSS documents that D.USER or D.TSF could remain on the device.

b. The ITSCC comments resolved around two issues:

- Whether or not cryptographic erase applies to the FDP_RIP.1/Overwrite SFR. They think that the cryptographic erase is already covered by SFR FPT_WIPE_EXT, and from a technical point of view the cryptographic erase is not a kind of overwrite since the data to be overwritten remained undeleted. So, they are not sure if it would be appropriate to use cryptographic erase as an overwrite method
- In SFR FDP_RIP.1.1/Overwrite, it seems that the option "by destroying its cryptographic key" seems to be for "wear-leveled storage device", while the other option "by overwriting data" seems to be for "non-wear-leveled storage device". Is it possible to select "by overwriting data" for "wear-leveled storage device"? Is it possible to overwrite data on a wear-leveled storage device such as SSDs?

We got into a good discussion on the second issue. The question of whether it is possible to perform overwrite on a wear-leveling device like an SSD is that currently technically it is possible but impractical. For a wear-leveling device, what it would entail is to have every temporary image file created by a job have its own unique key that can be destroyed rather than have a common key for all temporary image files created and stored on the wear-leveling device.

The real impetus for wanting this capability for a wear-leveling device has to do with the reason why customers want HDDs with the classic overwrite function (more on this later) even if an HDD is an extra option. Most vendors implement (and customers want) an overwrite function that is generally denoted as "Immediate Image Overwrite (IIO)". What IIO does is that after every print, scan, copy or fax job is finished processing by the HCD, any

temporary image files created during processing of that job are immediately overwritten by whatever overwrite algorithm that vendor uses (e.g., all zeros).That way, no matter what happens the customer is sure that no temporary image files will be retained at the end of the day, at decommissioning, etc. Currently, because of how Cryptographic Erase currently works there is no equivalent to IIO for wear-leveling devices and customers would like to have it. But, as stated above, that would require that each job have a unique key assigned to the image file created and currently that is not practical.

To address the ITSCC issues, the following change was made:

- The wording of the FDP_RIP.1/Overwrite SFR was modified as follows to clarify that it applied to both wear-leveling and non-wear-leveling devices -- FDP_RIP.1.1/Overwrite Refinement: 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.

c. JISEC had two issues but they were significant:

- The proposal of FDP_RIP.1.1/Overwrite does not meet the requirements of original FDP_RIP.1 defined in the CC part2, nor the allowed refinement operation defined in the CC part1. This is because there are residual data that cannot be erased by overwriting data for wear-leveled storage device. Therefore, it does not meet the requirements of original FDP_RIP.1.

- We are not sure why NIAP and HCD iTC want to include a mandatory requirement, cryptographic erase (destroying cryptographic key), as an optional requirement.
  Why is the following method not good?
  - Exclude cryptographic erase from the optional requirements, Overwrite and Purge.
  - Clarify that cryptographic erase is included as a mandatory requirement.

The first JISEC comment was surprising. The actual text of FDP_RIP.1 from ISO/IEC 15408 Part 2 is:

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].

which only requires that the data be made “unavailable”. The modified SFR in the latest version of the HCD cPP is:

FDP_RIP.1.1/Overwrite Refinement: The TSF shall ensure that any previous information content 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**.

Both overwrite and cryptographic erase will make the user document data unavailable. In discussing this first comment, the Secure Wipe Subgroup finally decided that the only real way to address this comment was to eliminate the use of FDP_RIP.1. So, the Subgroup created a new Extended User Document Unavailability SFR FDP_UDA_EXT with the same content as the updated content of FDP_RIP.1/Overwrite to address the ITSCC comments:

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 hope is that this will address this particular JISEC concern.

As a side note, during this discussion we got into a conversation about “overwrite” and the fact that the term seems today to get overloaded in terms of its meaning. There is the overwrite function itself that actually writes a pattern over the user document data file, and there is the overwrite method as defined in NIST SP 800-88r1 as a means of sanitizing a hard disk drive “by using organizationally approved and validated overwriting technologies/methods/tools”. The problem is that both meanings get used interchangeably and that causes confusion, which the Subgroup believed was part of JISEC’s issue here.

Regarding the second JISEC comment, the Secure Erase Subgroup agreed that this comment was essentially asking that Cryptograph Erase has to be a mandatory requirement, whereas in the latest version of the HCD cPP both FDP_RIP.1/Overwrite and FDP_RIP.1/PURGE) which FPT_WIPE_EXT is replacing) are optional requirements. This particular issue really has two components – whether the FPT_WIPE_EXT SFR itself should be a mandatory SFR or whether the Cryptograph Erase option within the FPT_WIPE_EXT SFR should be a mandatory option.

The Secure Erase Subgroup reached consensus that as a minimum we should make the Cryptograph Erase option within the FPT_WIPE_EXT SFR a mandatory option; we couldn’t reach consensus whether to make the SFR itself a mandatory SFR so we left that decision to the full HCD iTC at its next meeting. We did feel that if the FPT_WIPE_EXT SFR was to be mandatory it should probably be a Conditionally Mandatory SFR based on the type of storage media the HCD has.

We there updated the FPT_WIPE_EXT SFR as follows to address the second JISEC comment:

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.

- Al then brought up 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.

  As part of the preparation for the meeting was given a "homework assignment" to sample some ND certifications done by NIAP to see what how they addressed NTP requirements. Al sampled 20 different vendors that had products certified by NIAP against ND cPP v2.2e and a summary of what he found was that:

  - 18 of the 20 STs (one ST for each of the 20 products certified) did include the NTP SFR.
  - For the 18 STs that included the NTP SFR:
    - 16 STs chose the "Authentication" selection option and 2 STs chose the trusted communication selection option.
    - For the 2 STs that chose the trusted communication selection option, both chose the IPsec protocol
    - For the 16 STs chose the "Authentication" selection option, all but two chose just SHA1 as the message digest algorithm even though SHA1 is being deprecated. This is a very interesting result given that most of the certifications sampled were completed within the last 12 months, well after deprecation of SHA1 had been announced.

  It is hoped these results will help the NTP discussion at next Monday's HCD iTC Meeting.

- Al finally went briefly over the latest HCD iTC schedule status. As Al mentioned at the last IDS WG meeting, the current HCD iTC Workplan has the following key milestones
  - Submit Final Draft of HCD cPP and HCD SD: 5/16
  - Review HCD cPP/SD Final Drafts: 5/17 – 6/20
  - Review comments against HCD cPP/SD Final Drafts and update documents: 6/21 – 6/30
  - Publish HCD cPP v1.0 and HCD SD v1.0: 7/5/22

  The HCD iTC was on-track for the Final Drafts of both the HCD cPP and HCD SD to be submitted for public review on 7/16 subject to any last-minute issues. However, based on the lack of consensus to fully address the JISEC comments by the Secure Erase Subgroup, the publishing of the Final Drafts of the HCD cPP and HCD SD are going to be delayed at least a week and possibly more than that. Al's best guess is that the two documents are more likely to be published around the end of July or beginning of August 2022 at the earliest.

4. Al them showed the agenda for the IDS Face-to-Face Session at the May PWG Meetings on May 19th. The agenda is as follow:

When	What
12:45 – 12:55	Introductions, Agenda review
12:55 – 1:50	Discuss results of latest HCD iTC Meetings and HCD cPP/SD v1.0 status
1:50 – 2:10	IPP Encrypted Jobs and Documents
2:10 – 2:15	HCD Security Guidelines v1.0 Status
2:15 – 2:40	TCG/IETF Liaison Reports
2:40 – 2:45	Wrap Up / Next Steps

The IPP Encrypted Jobs and Documents discussion is part of an effort to educate IDS members on the security aspects of IPP.

Although the HCD Security Guidelines v1.0 Status and TCG/IETF Liaison Reports topics are on the agenda, there is a chance that Ira McDonald may not be able to present due to illness, so Al will be preparing a backup presentation based on one of the three special topics he presented at IDS WG Meetings since the last IDS Face-to-Face Session at the February PWG Face-to-Face Meetings - NIST Special Publication 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST Special Publication 800-213A IoT Device Cybersecurity Guidance for the Federal Government: *IoT Device Cybersecurity Requirement Catalog* and the NIST Cybersecurity Framework. At the meeting Al indicated he wasn't sure which of the three he would due, although he was leaning towards the SSDF presentation.

5. **Actions:** None

Next Steps

- The next IDS WG Meeting will be May 26, 2022 at 3:00P ET / 12:00N PT. Main topics will be review of the 5/16 and 5/23 HCD iTC Meetings, post-mortem on the IDS Face-to-Face Meeting on May 19th and a presentation by Smith Kennedy on IPP Authentication.
- The IDS Face-to-Face Meeting that is part of the May Virtual PWG/OpenPrinting Meeting will be on May 19th at 12:45 PM ET.