IDS Face-to-Face Minutes
May 19, 2022

Meeting was called to order at approximately 12:45 pm ET May 19, 2022.

Attendees –

Amitha	Konica Minolta
Graydon Dodson	Lexmark
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Anthony Suarez	Kyocera
Alan Sukert	
Michael Sweet	Lakeside Robotics
Uli Wehner	Ricoh
Steve Young	Canon

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2022-05-19-IDS-F2F.pdf.

- Minute Taker
  - Alan Sukert taking the minutes

2. Agenda:
   - Introductions, Agenda Review
   - Discuss results of latest Hardcopy Device international Technical Community (HCD iTC) Meetings and HCD collaborative Protection Profile (cPP)/Supporting Document (SD) v1.0 status
   - IPP Encrypted Jobs and Documents
   - HCD Security Guidelines v1.0 Status
   - Trusted Computing Group (TCG) / Internet Engineering Task Force (IETF) Liaison Reports
   - Wrap-Up / Next Steps
3. Alan went quickly through the PWG Antitrust and Intellectual Property and Patent policies.
4. Alan went through the current status of the HCD iTC and its efforts to develop HCD cPP v1.0 and HCD SD v1.0. Some of the key points from this discussion were:

   - Al presented a new way of showing comments for this Face to Face. He showed all the comments received to date across all the drafts to date. Specifically for the 2nd Public Draft, there have been 83 total comments submitted against the 2nd Public Draft of the HCD cPP, all of which have been adjudicated (the slide in the presentation showed there was 1 that had not been adjudicated, but that comment was moved to the be reviewed under the cPP Final Draft comments). The tally for the 83 comments was:

     - 56 comments were ‘Accepted’ to be fixed for the Final Draft of the HCD cPP
     - 0 comments were ‘Accepted in Principle’ to be fixed eventually in the HCD cPP by the time the HCD cPP v1.0 is published
     - 10 comment was ‘Deferred’ to be addressed a later time, possibly in a later version of the HCD cPP
     - 17 comments were either not accepted or rejected

     Overall, for all the HCD cPP drafts to date the total comment tally has been:

     - 282 comments were ‘Accepted’ to be fixed for the Final Draft of the HCD cPP

- 5 comments were 'Accepted in Principle' to be fixed eventually in the HCD cPP by the time the HCD cPP v1.0 is published
- 44 comment was 'Deferred' to be addressed a later time, possibly in a later version of the HCD cPP
- 41 comments were either not accepted or rejected

Ira noted that there was a positive trend for the HCD cPP of total comments going down for each successive draft.

- The 2nd Public Draft of the HCD SD (Version 0.98 dated 2/24/2022) was release for public review on 2/24/2022. Al showed the same type of total comment chart for the HCD SD as he did for the HCD cPP. Specifically for the 2nd Public Draft of the HCD SD, there were 28 total comments submitted, all of which have been adjudicated. The tally for the 28 comments was:
  - 25 comments were 'Accepted' to be fixed for the Final Draft of the HCD cPP
  - 1 comment was 'Accepted in Principle' to be fixed eventually in the HCD cPP by the time the HCD cPP v1.0 is published
  - 0 comments were 'Deferred' to be addressed a later time, possibly in a later version of the HCD cPP
  - 3 comments were either not accepted or rejected

  Overall, for all the HCD SD drafts to date the total comment tally has been:

  - 106 comments were 'Accepted' to be fixed for the Final Draft of the HCD cPP
  - 2 comments were 'Accepted in Principle' to be fixed eventually in the HCD cPP by the time the HCD cPP v1.0 is published
  - 17 comment was 'Deferred' to be addressed a later time, possibly in a later version of the HCD cPP
  - 6 comments were either not accepted or rejected

  Al noted that the number of HCD SD comments was about a 1/3 of the HCD cPP comments. Ira asked if that might be because the type of comments was different – the HCD cPP comments were more editorial while the HCD SD comments were more technical. Al didn't think that was the case, but he said he would do some look at the comments because he was responsible for maintaining the Master Comment Spreadsheet for the HCD iTC.

- Al then reviewed the key issues that were resolved in the 2nd Public Draft of the HCD SD:
  - Added a Test Assurance Activity for SFR **FPT_TST_EXT: TSF testing** where one was not present in previous drafts
  - Moved the Assurance Activities for the following:
    - All of the Audit Log related SFRs to under "Security Audit (FAU)" rather than because they are all mandatory SFRs
    - SFR **FCS_CKM.1/AKG Cryptographic Key Generation (for asymmetric keys)** to **Chapter 3. Evaluation Activities for Conditionally Mandatory Requirements** as required by NIAP Technical Decision TD 0074
    - SFR **FCS_CKM.2 Cryptographic Key Establishment** to **Chapter 3. Evaluation Activities for Conditionally Mandatory Requirements** because it refers to the conditional requirement SFR **FCS_CKM.1.1/AKG Cryptographic Key Generation (for asymmetric keys)**
  - Added ISO/IEC 11770-6:2016 to the list of references an evaluator shall verify the approved derivation mode and key expansion algorithm for in the TSS Assurance Activity for SFR **FCS_KDF_EXT.1: Cryptographic Key Derivation**

- Corrected an incorrect CEM paragraph reference in **Section 6.2.1. Basic Functional Specification (ADV_FSP.1)** *Table 2. Mapping of ADV_FSP.1 CEM Work Units to Evaluation Activities*
- Corrected several unreachable URLs in Appendix C: Public Vulnerability Sources.
- Removed redundant Operator User Guidance Evaluation Activities related to the evaluator ensuring that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE and providing a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE
- Corrected two incorrect paragraph references in **Section 6.6.1. Vulnerability Survey (AVA_VAN.1)** *Table 3. Mapping of AVA_VAN.1 CEM Work Units to Evaluation Activities*
- Added the missing content of the Evaluation Activity (Documentation) and Evaluation Activity sections under **Section 6.6.1. Vulnerability Survey (AVA_VAN.1)**
- Implemented the significant updates to the Assurance Activities (mostly in the Test Assurance Activities) requested by ITSCC (the Korean Common Criteria Scheme) for the following SFRs:
  - **FCS_CKM.1/SKG Cryptographic key generation (Symmetric Keys)**
  - **FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)**
  - **FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)**
  - **FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)**
  - **FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)**
  - **FCS_COP.1/KeyWrap Cryptographic operation (Key Wrapping)**
  - **FCS_CKM.1/AKG Cryptographic Key Generation (for asymmetric keys)**
  - **FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation**

  This last set of changes was very significant and could have a big impact on vendors who certify HCDs against the HCD cPP/SD once they are published. The reason is that the Test Assurance Activities added because of the ITSCC comments in most cases were extensive and go beyond the standard tests performed for these cryptographic SFRs.

  The reason that is important is because with the current HCD PP, since it was sponsored by NIAP Policy 5 was applicable. NIAP Policy 5 stated that if the Vendor sponsoring the certification could produce a valid CAVP certificate, testing of many of the cryptographic SFRs listed above could be waived.

  However, since NIAP isn't a sponsor of the HCD iTC and neither JISEC or ITSCC recognizes NIAP Policy 5, the Vendor will be responsible for performing all the necessary testing for these cryptographic SFRs. Most vendors don't have the capability to do this type of testing so they have to contract it out to either the evaluation lab doing the certification or another lab that has the necessary tools to do this type of testing. Cryptographic testing is expensive, and the extra testing added because of the ITSSC comments will add extra costs to any certification against the HCD cPP. In addition, there is no guarantee NIAP will accept these additional tests ITSSC added.

  Ira asked whether additional ITSSC tests are compatible with CAVP; Al indicated he didn't know but suspected they probably aren't.

- Al provided an update on the issue facing the HCD iTC on how to handle Cryptographic Erase (CE)- see the minutes from the November 4, 2021 and February 9, 2022 IDS Face-to-Face Meetings for the background on this issue.

The proposal to add the Data Wiping SFR FPT_WIPE_EXT that was discussed at the February 9th Face to Face has been modified multiple times by the Secure Erase Subgroup and the full HCD iTC since February 9th. At the beginning of May, the HCD iTC finally received comments against the proposal from NIAP, ITSSC and JISEC. In summary, the comments were:

NIAP

- Not clear whether this proposal is related to cryptographic erase, overwrite in general on SSDs, or both
- Inclusion "[assignment: media-specific method(s)]" in the SFR seemed overly broad
- Wanted some wording changes in the Application Note to the FPT_WIPE_EXT SFR

ITSCC

- Unclear whether the FDP_RIP.1/Overwrite SFR applies to cryptographic erase or not – this really meant did the FDP_RIP.1/Overwrite SFR itself apply to just the traditional overwrite function or did it also apply to cryptographic erase.
- In SFR FDP_RIP.1.1/Overwrite, 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"? It is possible to overwrite data on a wear-leveled storage device such as SSDs?

JISEC

- 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. Note – the HCD iTC didn't understand this comment and NIAP didn't agree with it either because in CC Part 2 FDP_RIP.1 only requires that the data be "unavailable" which FDP_RIP.1.1/Overwrite essentially states.
- We are not sure why NIAP and HCD iTC want to include a mandatory requirement, cryptographic erase (destroying cryptographic key), as an optional requirement (i.e., cryptographic erase should be a mandatory requirement) – this was interpreted to mean that JISEC wanted cryptographic erase to be a mandatory option within FPT_WIPE_EXT rather than FPT_WIPE_EXT being a mandatory SFR.

After discussion of these comments the Secure Erase Subgroup and the full HCD iTC agreed to make the following changes to address the comments from the three Schemes:

- Replace FDP_RIP.1/Overwrite with a new Extended User.Doc Unavailability SFR FDP_UDU_EXT with the following text:

  FDP_UDU_EXT.1.1/Overwrite 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

- Update FPT_WIPE_EXT to make cryptographic erase a mandatory method for making data unavailable and to delineate specific allowable media-methods to select from. New text is

  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*].

- Added additional TSS and Guidance elements to ensure types of overwrite and medium being overwritten are identified
- Make the requested changes to the FPT_WIPE_EXT Application Notes

- Some of the other issues facing the HCD cPP are:
  - There are some new NIAP TDs written by the Network Device Interpretation Team (NIT) against SFRs and Assurance Activities (AAs) that the HCD iTC inserted into the HCD cPP and HCD SD. The HCD iTC has to determine if these changes should be inserted into the corresponding SFRs and AAs in the HCD cPP/SD in Version 1.0 or what until the next version.
  - There are still several "Deferred" comments against both the HCD cPP and HCD SD the full iTC has to determine how to disposition – put in a "Parking Lot" for a future version, put in the Final Draft for Version 1.0 or just Reject.
  - Still need some type of answer on whether to include removal of support for Cipher suites with RSA Key Generation with keys < 2048 bits as required by NIST SP 800-56B and NIST SP 800-131A as well as for SHA-1 and all RSA and DHE Key Exchange.
  - Finally, the HCD iTC needs to make a final decision on whether or not to include NTP in Version 1.0 or put in in the "Parking Lot" for the next release.
- Al indicated that right now with the exception of what was mentioned above there is no new content planned for the HCD cPP. The only things that might change that would be requests from NIAP, the Japanese and Korean Schemes, NIAP Technical Decisions against the HCD PP or possible comments against the Final Drafts of the HCD cPP and SD.

  Al noted that the current "Parking Lot" issues that have been pushed to the next release of the HCD cPP/SD are:
  - Addressing hardware-based Roots of Trust stored in mutable memory as well as immutable memory
  - Clarification that the Secure Boot SFR only requires verification of firmware/software that is stored in mutable memory at boot time and does not require verification of firmware/software stored in immutable memory
  - Comments that require implementation of TLS 1.3 to resolve
- Al provided a status update on schedule that was just revised on May 16th to reflect the work to resolve the Cryptographic Erase proposal. The new schedule is as follows:
  - Publishing of Final Drafts of HCD cPP and HCD SD: 6/13/22
  - Review Final Public Drafts of HCD cPP and HCD SD: 6/14/ – 7/17
  - Review comments and update both documents: 7/18/22 – 8/1/22
  - Publish HCD cPP and HCD SD Version 1.0: 8/2/22

  Al indicated that the two weeks to review the comments and update the documents might be optimistic because, as Ira has stated on more than one occasion, the final drafts is when most people (especially Schemes) read the documents for the first time. So, the expectation is that you'll get a lot of comments and some very technical comments that will require changes to the final drafts. So, Al felt it was more realistic that the documents would be published closer to the end of August.

- Al then listed these items as ones to consider for inclusion in the HCD cPP/SD Post-v1.0. A couple of areas he emphasized this time were:
  - Coordination with EUCC (the new EU equivalent of the CC)
  - Inclusion of AVA_VAN and ALC_FLR.* because EUCC mandates that ALC_FLR be included in any a EU certified product under EUCC and the CCDB has indicated that the CC will have to include ALC_FLR into the CC for compatibility with EUCC
  - May require a PP Module to avoid duplicate certifications in EU
  - Changes due to HCD Integration Team responses to comments/questions
  - Incorporation of CCDB and CCUF Crypto WG Packages
  - Syncing with upcoming ND CPP Version 3.0 planned for Oct 2022. For example, the new version will include the CCUF Crypto WH SSH Package; the HCD cPP may have to consider changing to that package to sync with ND
- Next steps were that same as before. Keys are following the new schedule and setting up the Interpretation Team.
- Al finished the HCD iTC discussion with some more additions to the HCD iTC lessons learned he presented at the previous IDS Face-to-Face Meetings. These additional lessons learned were:
  - The end game is always the hardest part, because every time you think you're close to the end you're not
  - It's never too early to start planning for what comes after initial release because you always think you have more time to plan for what comes next than you actually do
  - It is critical that you avoid "reinventing the wheel" whenever possible – or in other words leverage what others have done before you whenever you can
  - Considering we started in February 2020, getting a new iTC established and creating/publishing a major cPP and SD within 2-1/2 years is still quite a feat

5. Mike Sweet then gave a presentation on IPP Encrypted Jobs and Documents. This is part of a series of presentations to familiar the IDS WG on the security aspects of IPP. The key points in Mike's presentation were:
   - The current prototype draft (needs prototyping) can be found at https://ftp.pwg.org/pub/pwg/ipp/wd/wd-ipptrustnoone10-20210519.pdf
   - The goal is to define new encrypted IPP message formats that provide IPP with end-to-end encryption of IPP Job attributes, Document attributes, and Document data. The encrypted formats use public key cryptography with an optional password to effectively protect the IPP message/Document data payload from intermediaries and when the data is at rest in the destination Output Device. The new message format reuses the existing S/MIME 4.0 [RFC8551] message format to protect the combination of IPP message and Document data normally sent in the clear as part of a Job Creation Request.
   - In summary:
     - Implements an S/MIME container for Print Jobs and Job Receipts (attributes containing accounting info)
     - PGP container was also proposed but ultimately was shelved due to lack of interest
     - Works for both direct and cloud/local server printing solutions
     - One new Client operation to query encrypted Job attributes/receipts
     - Two new Proxy operations to return encrypted Job attributes/receipt

     The key is to maintain confidentiality.

- For an Encrypted Print Job:
  - Printer/Proxy advertises an X.509 certificate and public key to use for encrypted printing
  - Client encrypts an IPP Print-Job request with document data in an S/MIME container using the Printer's X.509 certificate, signed using the Client's X.509 certificate
  - Job ticket and document data are both protected and signed to prevent modification
  - An additional password/passcode can be set for release at the printer's console
  - Printer/Proxy decrypts the S/MIME message, validates the Client signature, and processes the Print-Job request and document data

  The basis for this encryption is that the printer can't be trusted to store the job securely. This works for X.509 certificates for either a signed client or an end user. The only negative is that this requires that the printer accept and spool the job, so this will not work on printers that just stream the print job.
- The Get-Encrypted-Job-Attributes operation allows a Client to query Encrypted Job attributes from a Printer. 526 Once authorized, the attributes are encrypted using the Public Key supplied by the Client 527 and returned as data following the IPP response. It works as follows:
  - Client send a Get-Encrypted-Job-Attributes request with its own X.509 certificate and public key
  - Client certificate must match Print-Job request's signature
  - An ordinary Get-Job-Attributes request will only return basic state information
  - Printer/Proxy encrypts a Get-Encrypted-Job-Attributes response in an S/MIME container using the Client's X.509 certificate, signed using the Printer's X.509 certificate
  - Client decrypts the S/MIME message, verifies the Printer's signature, and processes the response attributes as needed
- Mike ended the presentation with a couple of questions:
  - Should we talk about using separate certificates and keys for signing and encryption?
    - Separate certificates sometimes used in email, where any validation seems to be limited to matching the common names of the certificates and "are the CAs that issued the certificates trusted?"

    The consensus of those present was that it is bad practice to use separate certificates in this case, but the use of separate certificates shouldn't be precluded. In short – "allow it but don't require it"
  - What should the common name be for Printer certificates?
    - Should be something the Client can use for validation
    - "printer-uuid" value?

    There was general agreement this can and should be done, and the specifics of what the name should be would be handled outside this meeting.

6. Ira then covered the latest status on the HCD Security Guidelines. Essentially nothing has changes since the February IDS Face to Face – the version of the HCD Security Guidelines (Version 13.1 dated 8 February 2022) that can be found at https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20220208-rev.docx (Note: a "clean" version of the update can be found at https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20220208.docx) has not been updated.
7. For the final topic Ira presented his Liaison report on current standards developments for the Trusted Computing Group (TCG) and Internet Engineering Task Force (IETF). The key points from Ira's Liaison Report were:

   - Regarding TCG standards activities, some key items Ira stressed were:

- Next TCG Members Meetings
  - **TCG Hybrid F2F (Chevy Chase, MD) – 18-22 July 2022 – Ira to call in**
  - **TCG Hybrid F2F (New Orleans, LA) – 24-28 October 2022 – Ira to call in**
- **TCG MARS 1.0 Mobile Profile** – will be published 4Q 2022
- For **Trusted Platform Services (TPG)** – there are 3 APIs (***Global Platform (GP) TPS Client API / Entity Attestation Protocol / COSE Keystore)*** that are being worked on.
- ***TCG DICE Endorsement Architecture for Devices –*** this is needed to boot TPMs and will be reviewed this month
- ***TCG EK Credential Profile for TPM 2.0 –*** will be review published this summer
- **TCG Canonical Event Log Format – published February 2022** This spec is for log formats for TPM operations

- Regarding IETF standards activities, some key items Ira stressed were:
  - IETF 114 Hybrid F2F (Philadelphia, US) – 25-29 July 2022
  - IETF 115 Hybrid F2F (London, UK) 7-11 November 2022
  - Key TLS-related specs that have been recently published were:
    - **IETF Connection Identifier for DTLS 1.2 – RFC 9146**
    - **IETF DTLS Protocol Version 1.3 – RFC 9147**
    - **IETF TLS Ticket Requests – RFC 9149**
  - Other TLS-related specs of note:
    - **IETF Importing External PSKs for TLS – draft-08** is going to IETF editor so is close to final draft
    - **IETF IANA Registry Updates for TLS/DTLS – draft-00** – latest draft only has small changes
    - **IETF Secure Element for TLS 1.3 – draft-04** deals with secure elements for GP
    - **IETF Compact TLS 1.3 – draft-05** – this is important because for compact TLS is 50% of full TLS
    - **IETF TLS 1.3 – draft-04** – this spec only contains errata only (~64 items)
    - **IETF Exported Authenticators in TLS – draft-15** - provides a way to authenticate one party of a TLS or DTLS connection to its peer using authentication messages created after the session has been established; prevents man-in-the-middle and related attacks
  - Security Automation and Continuous Monitoring (SACM) wrapped up in December 2021. However, the **IETF Concise Software Identifiers** spec is important to Remote ATtestation ProcedureS (RATS)
  - Regarding Concise Binary Object Representation **(**CBOR), some specs of note:
    - **IETF Storing CBOR Items on Stable Storage** – that was approved on May 18th and is now a STABLE Standard
    - **IETF Packed CBOR** – this packs large CBOR structures further
    - **IETF Using CDDL for CSVs** – hasn't made much progress on this document
  - Regarding Remote ATtestation ProcedureS (RATS):

- Several of the specs are either in IETF Last Call or close to publication
- **IETF RATS Architecture** – this will be published later this summer- this spec hooks up with the **TCG Canonical Event Log Format** for Global Platforms

- Finally, for the **IRTF Crypto Forum Research Group (CFRG):**
  - This is where the IETF does all its cryptographic work
  - **IRTF Hybrid Public Key Encryption – RFC 9180** was published in February 2022. Address both pre-quantum and post-quantum security
  - **IRTF Argon2 password hash and proof-of-work – RFC 9106** was published in Sep 2021.
  - **IRTF Verifiable Distributed Aggregation Functions** – this document addresses issues like “how can I do surveys and split apart the results and then combine them again later so that the original names are not known”

8. **Wrap Up**

- Next IDS Working Group Meeting will be on May 26, 2022. Main topics of the meeting will be latest HCD iTC status and an IPP Authentication presentation by Smith Kennedy.
- Next IDS Face-to-Face Meeting will be during the August 2022 PWG Virtual Face-to-Face Meeting August 16-18, 2022.

Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 2:55 PM ET on May 19, 2022.