IDS Face-to-Face Minutes
November 17, 2022

Meeting was called to order at approximately 10:15 am ET November 17, 2022.

Attendees –

Graydon Dodson	Lexmark
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Anthony Suarez	Kyocera
Alan Sukert	
Michael Sweet	Lakeside Robotics
Brian Volkoff	Ricoh
Bill Wagner	TIC
Uli Wehner	Ricoh
Steve Young	Canon

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2022-11-17-IDS-F2F v3.pdf.

- Minute Taker
  - Alan Sukert taking the minutes

  Note: Because Al was in Toledo Spain for the International Common Criteria Conference at the time of this meeting, the notes for this meeting will be less detailed than they typically are. If anyone has questions or comments on any of the meeting slides, please contact Al t ansukert49@outlook.com and he will gladly address your question or comment.

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
   - ASTM ICAM 2022 Presentation Summary
   - 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:
   - The biggest news was that HCD PP v1.0 and HCD SD v1.0 were both published with an official date of October 31, 2022. This brings fruition to over 2-1/2 years of work by the HCD iTC and is a major milestone.

     The final tally of the comments against the HCD cPP in developing HCD cPP v1.0 was:

     - 19 comments – all accepted – against the Security Problem Definition for HCDs that becomes part of the HCD cPP.
     - 339 comments were ‘Accepted’ to be fixed
     - 4 comments were ‘Accepted in Principle’ to be fixed eventually in the HCD cPP by the time HCD cPP v1.0 is published

  - 29 comments were ‘Deferred’ to be addressed a later time, possibly in a later version of the HCD cPP
  - 45 comments were either not accepted or rejected
  - Total comments - 436

  The final tally of the comments against the HCD SD in developing HCD SD v1.0 was:

  - 140 comments were ‘Accepted’ to be fixed
  - 3 comments were ‘Accepted in Principle’ to be fixed eventually in the HCD cPP by the time HCD SD v1.0 is published
  - 18 comment was ‘Deferred’ to be addressed a later time, possibly in a later version of the HCD cPP
  - 8 comments were either not accepted or rejected

- Al then went thru the key issues resolved in the published versions of both the HCD cPP and HCD SD since the Final Drafts of both documents. The two lists are shown at the end of these minutes. Some key points on each list:
- For the HCD cPP, the majority of the changes in the Final Draft were relatively straightforward. The major change from the Final Draft was several modifications to the **FPT_KYP_EXT.1 Extended: Protection of Key and Key Material** to address issues raised by JISEC and JBMIA regarding when to store encryption keys and key material in the case where the key is used to either wrap a key as specified in FCS_COP.1/KeyWrap or used to encrypt a key as specified in FCS_COP.1/KeyEnc or FCS_COP.1/KeyTransport] that is already either wrapped as specified in FCS_COP.1/KeyWrap or encrypted as specified in FCS_COP.1/KeyEnc or FCS_COP.1/KeyTransport
- For the HCD SD, the major issues involved (1) the associated KMD, TSS and Guidance Assurance Activities changes for the **FPT_KYP_EXT.1 Extended: Protection of Key and Key Material** and **FDP_DSK_EXT.1 Extended: Protection of Data on Disk** SFRs to reflect the changes to **FPT_KYP_EXT.1** made in the HCD cPP, (2) moving some Assurance Activities to their proper category for some SFRs and (3) modifying or addressing clarifications to some specific Assurance Activities for multiple SFRs.
- For the “schedule” discussion Al first showed an earlier schedule from February 2021 that had the HCD cPP v1.0 and HCD SD v1.0 published by 2/14/22. He compared that with the final planned schedule from July 2022 that had the HCD cPP v1.0 and HCD SD v1.0 that had both documents published by 9/7/22, and it was still off by 1-1/2 months.
- Al showed the list of current “Parking Lot” issues against both the HCD cPP and HCD SD now that version 1.0 of both documents has been published.

  The key issues for the HCD cPP (in Al’s view) are

  - Addressing the Roots of Trust issues
  - 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
  - Support for NTP

  The key issues for the HCD SD (in Al’s view) are

  - Correcting TSS Assurance Activities for SFR FCS_CKM.4 Key Destruction

  - Correcting Test 2 for SFR FCS_CKM.4 Key Destruction to provide a valid test for where the data read operation would fail
- There are two big remaining issues, now that both documents have been published.
  - One is setting up the HCD Interpretation Team (HIT) – finalizing the HIT operating procedures, determining the membership (both in terms of how many and the actual members), determining who will fill the Chair and Deputy Chair roles, and then actually begin HIT activities. This becomes increasing time critical because Brian indicated he was told by the Canadian Scheme that they are ready right now to start accepting HCD certifications against the new HCD cPP and SD.
  - The other is determining a release plan for the HCD cPP and HCD SD for future updates of both documents. The HCD iTC has determined that there will be both major (x.0) and minor (x.y) releases; the questions the HCD iTC must now determine the answers to are:
    - What is the time frame between minor releases (e.g., the ND iTC has minor releases of the ND cPP once a year on average)
    - What is the time frame between major releases and how is that determined
    - What goes into a major or minor release
- Al then listed these items that might be considered for inclusion in the HCD cPP/SD Post-v1.0. The major items Al feels will almost certainly be in next version (v1.1) of the HCD cPP and SD are:
  - Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
  - Inclusion of NTP
  - Inclusion of AVA_VAN and ALC_FLR.* to be consistent to the upcoming EUCC. Al noted that coordination between the CC and EUCC and the issue of mutual recognition between the two schemes is going to become a big issue in 2023. Ira mentioned that the EU has recently issued the Cyber Resiliency Act (CSA); a link to the CSA is at https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.
  - Incorporate NIAP SSH Package
  - Address the changes to comply with Commercial National Security Algorithm (CNSA) Suite 2.0 that addresses cryptanalytically relevant quantum computers (CRQCs). CNSA 2.0 will have a large impact on any IT or IOT product that does hashing, for example, because it will limit allowable SHA values to only SHA-384 or SHA-512.
  - Update to address the new CC 2022 versions of ISO/IEC 15408/18045 that was just published on November14th.

  The items for potential in V1.1 or later versions of the HCD cPP/SD are basically the same as they were from the August IDS Face to Face. The one addition is the possibility of expanding the scope to include 3D printers.
- Next steps are pretty straightforward:
  - Implement the HIT for maintaining HCD cPP/SD v1.0
  - Agree on the HCD cPP/HCD SD release plan
  - Determine the content for and then create the next HCD cPP/SD release (v1.1)
  - Ensure that the HCD iTC continues to be fully engaged now that HCD cPP v1.0 and HCD SD v1.0 have been published
- Al finished the HCD iTC discussion with the last of his HCD iTC lessons learned:

- I have said this before, but developing v1.0 of the HCD cPP and HCD SD in 2 years, 8 months is an accomplishment worth celebrating
- Input and support from Stakeholders (meaning the Schemes that sponsor the iTC) are critical for success
- Feedback and buy-in from all vendor communities is also critical for success The HCD iTC was lucky that it had active participants from both the Japanese and American HCD vendors all through the process of creating the HCD cPP and HCD SD.
- Setting an initial aggressive schedule is not advisable because it will never be met. Better to set a realistic schedule, and even that one will likely not be met. Kwangwoo Lee, the HCD iTC Chair, admitted he was young and naïve when he developed his initial aggressive schedule for our iTC.

5. Al then went through the presentation he gave on November 4th to the ASTM International Conference on Additive Manufacturing (ICAM) 2022 entitled "**Developing Common Criteria Based 3D Printing Equipment Cybersecurity Certification**". This was based on a briefing Al and Paul Tykodi gave to Insights in Sep 2020.

   The main point of the presentation was that the work done in developing the HCD cPP can be leveraged to eventually develop a PP for the Digital Path for Additive Manufacturing (Note: Additive Manufacturing is just another term for "3D Printing) because at the 10,000 foot level HCDs and the Digital Path/3D printers are not that dissimilar in terms of assets that need to be protected, the security threats against those assets that need to be mitigated and the security objects that are needed to mitigate those threats.

   A few words on what the Digital Path for Additive Manufacturing (aka the Digital Path) is. Slide 31 shows pictorially the Digital Path as a data flow diagram. The phases of the Digital Thread are as follows:

   1. **Product Inception** which involves requirements definition and concept generation/evaluation of the object to be printed
   2. **Design/Scan and Analyze** – This is where the initial translation of the object to be printed to digital form occurs in the form of a CAD model that is created. Traditional analysis using tools such as Finite Element Analysis and advanced multi-physics modeling and simulation of 3D printing process for object to be printed is also done during this phase.
   3. **Build and Monitor** – This is where machine instructions to control printer and build the printed 3D object are created. This phase includes (1) simulation of build process, (2) creating of a 2.5D model in .STL format created from the CAD model (which is stored in plain text), (3) detailed Build Planning and collecting of Machine Data, and (4) Part Fabrication (this includes Slicer software that created the layers upon which the printed 3D object is actually created).
   4. **Post Processing and Finishing** – This phase involves testing and inspection to determine the printed 3D object is correct and meets its design. This phase Includes collection of data generated during the Digital Thread to update CAD model.

   The comparison to HCDs is based on the fact there are two computers – one containing the CAD model, and simulations from the **Design/Scan and Analyze** phase as well as the .STL file and the actual 3D printer itself. There are threats around unauthorized access to the CAD model, .STL file, etc. stored on the first computer as well as threats related to transferring the .STL file to the 3D printer. There are files and software stored on the 3D computer that need to be protected from unauthorized access and software on both computers that need to be protected from unauthorized firmware/software updates.

   When you put that all together the presentation tries to make a case that the similarities are sufficient that a PP for the Digital Thread/3D Printers can be developed based on the Security Problem Definition from the HCD cPP.

   The last slide in the presentation indicates the steps that should be done to develop such a PP.

6. Ira then covered the latest status on the HCD Security Guidelines. Essentially nothing has changed since the February or August IDS Face to Faces – 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).
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 mentioned were:
    - Next TCG Members Meetings will be Feb 22, 2023 in Vancouver BC
    - Regarding **Trusted Mobility Solutions (TMS)**, it is developing a Mobile Ecosystem Security Guidelines consisting of best practices.
    - For **Mobile Platform (MPWG)**:
        - ***TCG Mobile Reference Architecture v2*** and ***TCG TPM 2.0 Mobile Common Profile*** are both under review to be completed by Jan 23rd. Both standards affect any device that supports Wi-Fi.
    - For **Recent Specs**:
        - ***TCG Measurement and Attestation RootS Library*** will be published sometime in Q4 2022. It took so long because the previous version had errors in it that needed to be addressed. This standard is important because it supports network utility and provides for high quality secure boot by attesting to the integrity.
        - ***TCG Component Class Registry*** supports PCs and servers
        - ***TCG Storage Component Class Registry*** involves pieces of storage
- Regarding IETF standards activities, some key items Ira stressed were:
    - For TLS:
        - **IETF Exported Authenticators in TLS – RFC 9261**, **IETF Importing External Pre-Shared Keys (PSKs) for TLS 1.3 – RFC 9258**, and **IETF Guidance for External Pre-Shared Key (PSK) Usage in TLS – RFC 9257** allow strong binding between the App layer and the TLS layer
        - **IETF TLS Ticket Requests – RFC 9149** is about resuming sessions
        - **IETF DTLS Protocol Version 1.3 – RFC 9147** was published in Apr 2022
        - **IETF TLS 1.3 (errata update)** is supposed to be published in Jan 2023.
        - **IETF Using Attestation in TLS and DTLS** is new work to use embedded services; will add to TLS vis the TLS handshake. There will be no export protocol for attestation, so attestation will be built into the app layer.
        - **IETF Secure Element for TLS Version 1.3** involves SIM cards for TLS 1.3
    - For **Security Automation and Continuous Monitoring (SACM)** the **IETF Concise Software Identifiers** will improve compression by using post-swids.
    - Regarding **Concise Binary Object Representation (CBOR)**, CDDL (Concise Data Definition Language) 2.0 will add import/export, versioning, name spaces and features similar to how IPP uses them. This is important in many areas such as Global Platform.

      Other specs of note:

        - **IETF Feature Freezer for CDDL** is a "parking lot" for new features not yet standardized

    - **IETF CBOR Tags for Time, Duration, and Period** is being developed jointly with other IETF Working Groups
    - **IETF Using CDDL for CSVs** will allow generated CDL schema to be exported as a CSV file
    - **IETF Notable CBOR Tags** is the "parking lot" for new tags
    - **IETF Storing CBOR on Stable Storage** involves canonical file storage and is needed by RATs and other WGs. Had been in RFC status for 6 months.

  - Regarding **Remote ATtestation ProcedureS (RATS)**:

    There is lots of work being done; the information on Slide 41 is only part of it. Other specs of note:

    - **IETF Entity Attestation Token (EAT)** is in IETF Last Call; should be published in Jan 2023.
    - **IETF EAT-based Key Attestation Token** is a new spec.
    - **IETF Concise TA Stores (CoTS)** has generated a lot of interest
    - **IETF RATS Architecture** has been around for a while
    - There is a new "Message Envelop" spec under development.

    Ira noted that RAYS will not specify a transport protocol to send attestation.

  - Finally, for the **IRTF Crypto Forum Research Group (CFRG):**

    There are several RFCs that were published as noted on Slide 43. Many of these specs use NIST primitives. Other specs of interest:

    - **IRTF NTRU Key Encapsulation** involves Open Source and has been around a while
    - **IRTF Ristretto255 and Decaf448 Groups** is a new group
    - **IRTF Properties of AEAD algorithms** is a utility for key parameters for AEAD. It collects 20 names properties for AEAD
    - **IRTF Verifiable Distributed Aggregation Functions** has been approved

8. **Wrap Up**

  - Next IDS Working Group Meeting will be on December 1, 2022. Main topic of the meeting will be Al's summary of the 22nd CCUF Workshop and the International Common Criteria Conference he recently attended in Toledo Spain.
  - Next IDS Face-to-Face Meeting will be during the February 2023 PWG Virtual Face-to-Face Meeting February 7-9, 2023.

  Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 11:58 am ET on November 17, 2022.

MAJOR CHANGES INCLUDED IN FINAL PUBLIC DRAFT HCD cPP

1. **To include Cryptographic Erase into the HCD cPP and address concerns about** the fact that the FDP_RIP.1/* SFRs suggested to users that residual data is permanently removed from wear-leveling storage devices (e.g., SSDs), when in fact FDP_RIP.* can't be used for operations involving Cryptographic Erase (CE) because the actual data is still present in encrypted form, and future technologies might be capable of breaking the encryption the following was done:

   - **Replaced SFR FDP_RIP.1/Overwrite** Subset residual information protection with a new SFR FDP_UDU_EXT.1 User.DOC Unavailable **that (1) provides the option for Overwrite for the SFR to apply to both wear-levelling and non-wear-levelling storage devices and (2) to include destruction of cryptographic keys as well as overwrite to make USER.DOC unavailable.**

   - **Replaced SFR** FDP_RIP.1/Purge Subset residual information protection with a new SFR FPT_WIPE_EXT.1 Data Wiping that requires that customer-supplied D.USER and D.TSF data stored in non-volatile storage be made unavailable using Cryptographic Erase as a mandatory method and optionally using none or one or more of five other methods – overwrite, block erase, media specific eMMC method, media specific ATA erase method, or media specific NVMe method.

   - **Added or modified wording addressing Cryptographic Erase or destruction of cryptographic keys in the following Sections:**

     a. **Section 1.4.2** USE CASE 2: Conditionally Mandatory Use Cases, Item 4. Nonvolatile Storage Devices

     b. Section 1.4.3 USE CASE 3: Optional Use Cases, Item 2. Redeploying or Decommissioning the HCD

   - Added the following statement to the definition of O.STORAGE_ENCRYPTION in Section 3.5.4 Storage Encryption: "…and the TOE shall provide a function that an authorized administrator may destroy encryption keys or keying material if the TOE supports a function for removing the TOE from its Operational Environment".

   - Added the following note to Section 3.5.7 Wipe Data (optional): Note: Cryptographic erase which is covered in the mandatory requirement of FCS_CKM_EXT.4 and FCS_CKM.4 can be used as a method to remove some parts of User Data and TSF Data, but it cannot be a single method to remove User Data and TSF Data unless all the data are encrypted.

   - Because of the new FDP_UDU_EXT.1 SFR, modified Section 3.5.6 Image Overwrite (optional) to remove the statement "or by destroying its cryptographic key" in the last sentence since it was no longer necessary.

   - Changed the title of Section 3.5.7 from Purge Data (optional) to Wipe Data (optional) reflect the new FPT_WIPE_EXT.12 Data Wiping SFR

   - Changed the title of Section 4.1.13 from Purge Data (optional) to Wipe Data (optional) reflect the new FPT_WIPE_EXT.12 Data Wiping SFR

   - Changed the Organizational Security Policy (OSP) O.PURGE_DATE to O.WIPE_DATA to reflect the new FPT_WIPE_EXT.12 Data Wiping SFR

   - Modified the Application Note for the SFR FDP_DSK_EXT.1 Protection of Data on Disk to state that if additional data other than D.USER.DOC and D.TSF.CONF are encrypted, it will be purged by the cryptographic erase process

2. Modified SFRs FPT_SBT_EXT.1.5 and FPT_SBT_EXT.1.6 for Secure Boot to clarify that they apply only to Hardware Roots of Trust.

3. Removed the previous Software Functional Requirements table that was in Appendix H: SFR List, as well as the entire appendix, that mapped SFRs to OSPs. Replaced this table with a new table in Section 5.12 TOE Security Functional Requirements Rationale that maps OSPs to SFRs and provides the rationale for that mapping.
4. Moved SFR FCS_CKM.1/AKG Cryptographic Key Generation (for asymmetric keys) from a Conditionally Mandatory to an Optional requirement.
5. Added missing or incorrect SFR Mapping Information for several SFRs.
6. Removed the Consistency Rationale Appendix as being repetitive and no longer needed.
7. The term File Encryption Key (FEK) was incorrectly used in several places in the document; it was replaced by "BEV or DEK". Also, is some instances "DEK" was missing when it should have been included, so in those instances "BEV" was changed to "BEV or DEK" also.
8. Corrected a typo in Section 5.4.2. FDP_ACF.1 Security attribute based access control, Table 5. D.USER.JOB Access Control SFP, where "log' should have been "job".
9. Addressed the following NIAP Technical Decisions:
   - TD0642: FCS_CKM.1(a) Requirement; P-384 keysize moved to selection
   - TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH
   - TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server
10. Fixed several grammatical and typographical errors in the document.

IDS Face-to-Face Minutes
November 17, 2022

MAJOR CHANGES INCLUDED IN FINAL DRAFT OF HCD SD

1. Added the Assurance Activities for the new SFRs **FDP_UDU_EXT.1 User.Doc Unavailable** and **FPT_WIPE_EXT.1 Data Wiping** that replaced the previous SFRs **FDP_RIP.1/Overwrite** and **FDP_RIP.1/Purge**, respectively.

2. Because of the inclusion of Cryptographic Erase due to the new SFRs **FDP_UDU_EXT.1 User.Doc Unavailable** and **FPT_WIPE_EXT.1 Data Wiping**, made the following changes to the Assurance Activities for SFR **FDP_DSK_EXT.1 Extended: Protection of Data on Disk**:

- Added the following paragraph to the TSS Assurance Activities:

  If data (e.g., D.USER.JOB, D.TSF.PROT) other than D.USER.DOC and D.TSF.CONF are encrypted, the evaluator shall verify that TSS identifies all such data and states that no other customer-supplied data are encrypted

- Added the following new tests to the Test Assurance Activities:

  Test 3. (If data other than D.USER.DOC and D.TSF.CONF are encrypted,) write the data to the storage device with operating TSFI which enforce write process of the data.

  Test 4. (If data other than D.USER.DOC and D.TSF.CONF are encrypted,) verify that the data written in Test 3 is not in plaintext form; and verify that the data can be decrypted by proper key and key material.

3. Updated the discussion in **Section 1.1. Technology Area and Scope of Supporting Document** to indicate that certifiers/certification bodies are users of this document.

4. Removed wording in **Section 1.2 Structure of the Document** that implied that Certifying Bodies (CB) could modify Evaluation Activities in the SD.

5. Removed wording in the preliminary paragraph in **Chapter 2. Evaluation Activities for SFRs** that suggested witnessing developer-generated tests vs. independently performing tests, because that would require CB approval.

6. Revised the Test Assurance Activities for both SFR **FCS_COP.1/DataEncryption** and SFR **FCS_COP.1/StorageEncryption** to add testing of the key size of 192 bits.

7. Broke up the Test Assurance Activities for SFR **FIA_PMG_EXT.1 Extended: Password Management** into two separate test cases to avoid confusion.

8. Revised **Section A.1.1. Type 1 Hypotheses - Public-Vulnerability-based** to add the missing information and to clarify the text from the previous versions of this document.

9. Revised Section **A.1.2. Type 2 Hypotheses - iTC-sourced** to indicate that there are currently are no iTC-sourced flaw hypotheses, but that a future revision of the HCD cPP may update this section for relevant findings made by evaluation laboratories.

10. Corrected and/or updated the Evaluation Activities for the following areas in **Chapter 6 Evaluation Activities for SARs:**
    - **ADV_FSP.1-5 Evaluation Activity**
    - **Operational User Guidance (AGD_OPE.1)**
    - **Vulnerability Survey (AVA_VAN.1)**
11. Fixed some incorrect section references in the document as well as some typographical and grammatical errors.