The Printer Working Group

Imaging Device Security

August 16, 2018

PWG August 2018 Face-to-Face

Agenda

When	What
9:00 – 9:05	Introductions, Agenda review
9:05 – 10:20	Review status of HCD PP v1.1 and HCD iTC
10:20 – 10:30	Wrap Up / Next Steps

Intellectual Property Policy

"This meeting is conducted under the rules of the PWG IP policy".

- Refer to the IP statements in the plenary slides

Officers

- Chair:
  - Alan Sukert (Xerox)
- Vice-Chair:
  - Currently Vacant
- Secretary:
  - Alan Sukert (Xerox)
- Document Editors:
  - Ira McDonald (High North): HCD-TNC

Status of HCD PP Version 1.1

- Draft 1 (Version 1.0.1) posted in May 2018
  - Incorporated Errata #1 and all NIAP Technical Decisions
  - Baseline for proposing further updates
- Draft 2 (Version 1.0.2) prepared in Jun 2018
  - Implemented changes for Version 1.1 approved at Apr 25 and May 8 HCD Technical Committee Meetings
  - Currently under review

Status of HCD PP Version 1.1 Changes Incoporated in Drafts 1 & 2

- Seven NIAP Technical Decisions
  - **TD0299:** Update FCS_CKM.4 Assurance Activities (Test 2) to properly address when a TOE replaces a key with another valid key
  - **TD0261:** Replace FCS_CKM.4 in its entirety (including Assurance Activities) to include destruction of keys stored in flash memory.
  - **TD0253:** Provide an Assurance Activity for FCS_COP.1(i) since there were none before
  - **TD0219:** NIAP endorsement of the errata contained in *Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017*
  - **TD0176:** Modified the App Note and Assurance Activities for this SFR so they now applied to Self-Encrypting Drives

Status of HCD PP Version 1.1 Changes Incoporated in Drafts 1 & 2

- Seven Technical Decisions (cont)
  - **TD0157:** Added a new App Note and modified the Assurance Activity to reflect that fact that for some HCDs administrators are not permitted to manually configure or edit the IPsec Security Policy Database (SPD) and that BYPASS operations are not supported.
  - **TD0074:** Makes FCS_CKM.1(a) an optional rather than a mandatory requirement and moves the description of that requirement to Appendix C Optional Requirements.

Status of HCD PP Version 1.1 Changes Incoporated in Drafts 1 & 2

Errata #1

- Notation error corrections
- Extended Components Definition (ECD) Changes
- Fix SFR Dependencies

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Eliminated the requirement to support TLS 1.0 in FSC_TLS_EXT_1.1 in both sections A.9.12 and D.2.2.

  Rationale: TLS 1.0 is being dropped industry-wide as being an insecure TLS version, so it should no longer be required.

- Made all cipher suites optional in FSC_TLS_EXT_1.1 in both sections A.9.12 and D.2.2 – that meant eliminating the 'None' option under Optional Cipher Suites so that at least one had to be supported.

  Rationale: Consistency with NDcPP v2.0.

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Added to the last selection in FCS_COP.1.1(e) in section D.1.2 so the SFR now reads **FCS_COP.1.1(e) Refinement:** The TSF shall perform **key wrapping** in accordance with a specified cryptographic algorithm **AES in the following modes [selection: *KW, KWP, GCM, CCM*]** and the cryptographic key size **[selection: *128 bits, 256 bits***] that meet the following: [**ISO/IEC 18033-3 (AES), [selection: *NIST SP 800-38F, ISO/IEC 19772, no other standards***]].

  Rationale: Consistency with NDcPP v2.0.

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Added to FCS_COP.1.1(i) in section D.1.14 so the SFR now reads as follows: **FCS_COP.1.1(i) Refinement:** The TSF shall perform **key transport** in accordance with a specified cryptographic algorithm **RSA in the following modes [selection: *KTS-OAEP, KTS-KEM-KWS*]** and the cryptographic key size **[selection: *2048, 3072*]** bits that meet the following**: NIST SP 800-56B, Revision 1**.

  Rationale: Completeness and to clarify what the key sizes should be

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Added to FCS_PCC_EXT.1.1 in section D.4.1 so it now reads as follows: **FCS_PCC_EXT.1.1** A password used by the TSF to generate a password authorization factor shall enable up to [assignment: *positive integer of 64 or more*] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: *other supported special characters*]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [HMAC-[selection: *SHA-256, SHA-384, SHA-512*]], with [assignment: *positive integer of 1000 or more*] iterations, and output cryptographic key sizes [selection: *128, 256*] bits that meet the following: [**NIST SP 800-132**].

  Rationale: Consistency with NDcPP v2.0 and to clarify what the key sizes should be.

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Changed the TSS Assurance Activity for SFR FTP_ITC.1 in section 4.13.1 to read as follows: The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

  Rationale: Consistency with NDcPP v2.0.

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Changed old paragraph 1451 in Appendix F to read "A description of the data encryption engine, its components, and details about its implementation (e.g. for hardware: integrated within the device's main SOC or separate co-processor, for software: initialization of the product, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions associated with the Master Boot Record (MBRs), partition tables, etc.)). The description should also include the data flow from the device's host interface to the device's persistent media storing the data, information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted Master Boot Record area). The description should be detailed enough to verify all platforms to ensure that when the user enables encryption, the product encrypts all Field-Replaceable nonvolatile storage devices. It should also describe the platform's boot initialization, the encryption initialization process, and at what moment the product enables the encryption.

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Changed old paragraph 987 in the KMD Assurance Activity in FDP_DSK_EXT.1 in section B.1.3 to read "The evaluator shall verify the KMD provides sufficient instructions to ensure that when the encryption is enabled, the TOE encrypts all Field-Replaceable Nonvolatile Storage Devices. The evaluator shall verify that the KMD describes the data flow from the interface to the Device's persistent media storing the data. The evaluator shall verify that the KMD provides information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted area)."

  Rationale – Inconsistency in KMD requirements between Appendix F and the KMD Assurance Activity for FDP_DSK_EXT.1 as to what storage devices should be encrypted, and to be consistent with the rest of the HCD PP.

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Changed the last sentence in Test Assurance Activity 5. for FPT_TUD.EXT.1 to read: (The evaluator shall also check those cases where digital signature verification mechanism, and if only selected in **FPT_TUD_EXT.1.3** the hash verification mechanism**,** fail.)

  Rationale: The hash verification failure test should only be required if hash verification is selected in FPT_TUD_EXT.1.3

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Changed two instances in the Assurance Activity for FAU_SAR.1 to read as follows:

  TSS:

  The evaluator shall check to ensure that the TSS contains a description that audit records can be viewed only by an Administrator and functions to view audit records.

  Test:

  - The evaluator shall also perform the following tests:
    1. The evaluator shall check to ensure that the forms of audit records are provided as specified in the operational guidance by retrieving audit records in accordance with the operational guidance.
    2. The evaluator shall check to ensure that no users other than an Administrator can retrieve audit records.

  Rationale: Consistency with the requirement as stated in FAU_SAR.1.1

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Added the following test to the Test Assurance Activity in FAU_STG.4:

  3. The evaluator shall check that the actions specified in FAU_STG.4.1 are performed when the audit log is full.

  Rationale: The Test Assurance Activity for this SFR never checks that the actions specified in the SFR are actually performed when the audit log is full.

Status of HCD PP Version 1.1 Changes Included in Drafts 1 and 2

- Added the following Test Assurance Activity to FMT_SMF.1:

  Test:

  The evaluator shall also perform the following test:

  The evaluator shall check to ensure that U.NORMAL is not permitted to operate the management functions.
  Note: This test can be partially or completely fulfilled by performing the Test Assurance Activity in FMT_MOF.1 depending on the list of management functions in FMT_MOF.1 and FMT_SMF.1.

  Rationale: Address the fact that FMT_SMF.1 has the implicit requirement that only U.ADMN can perform the indicated management functions.

Status of HCD PP Version 1.1

Additional changes that might be considered for Version 1.1:

- Eliminating the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite from FCS_TLS_EXT.1.
- In Appendix F, paragraph 1452, should that paragraph be revised to read "The process for destroying keys when they are no longer needed by describing the storage location of all keys and the protection of all keys stored in Field-Replaceable nonvolatile memory." (see #7 and #8 above)?
- Should FAU_STG.1 be a mandatory rather than an optional SFR. I think from both TC Meetings the consensus was that it should be, but not sure this falls into the "minor change" category so I didn't make the change yet.

Status of HCD PP Version 1.1

Additional changes that might be considered for Version 1.1:

- "Purge Data" may need to change to "Clear Data" to be consistent with terms and requirements from SP 800-88 (and equivalent ISO standard)
- See if any of the SFR dependencies have to be changed
- The issue brought up by JBMIA about the inconsistency between FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)] and FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication) over specification of the required key sizes because, to be honest, not sure how to address it
- The parking lot issues from the creation of Version 1.0 to see if any of them should go into v1.1

Status of HCD PP Version 1.1

Additional changes that might be considered for Version 1.1:

- Updates to SFR Dependencies to include:
  - FCS_COP.1(g) being dependent on FCS_COP.1(c)
  - For FCS_PCC_EXT.1, should FCS_COP.1(h) be a dependency and not also (or instead of) FCS_COP.1(g)
  - FCS_KYP_EXT.1 being dependent on FCS_KYC_EXT.1
  - Should FCS_CKM.1(b) be dependent on FCS_COP.1(e) and FCS_COP.1(g)

Issues to be considered for HCD PP Version 2.0 or HCD cPP Version 1.0

- Outputs of new TLS Technical Committee and inclusion of TLS 1.3
- Changes to NIST SP 800-131A and NIST SP 800-56B related to disallowance of TLS cipher suites using RSA Key Generation
- NDcPP Version 2.0 – Alignment with SFRs common with the HCD PP
- FDE AA and EE cPP Version 2.0 – Alignment with SFRs common with the HCD PP
- New NIAP Policies and new NIAP Technical Decisions against HCD PP, NDcPP, FDE AA cPP and FDE EE cPP
- Areas where the HCD PP Assurance Activities may have provided unintended functional requirements
- Internationalization (i.e., replace or augment NIST standards with ISO standards)

Issues to be considered for HCD PP Version 2.0 or HCD cPP Version 1.0

New or Modified SFRs:

- Management of Crypto keys
- Additional IPSec requirements
- Separate TLS requirements for TLS acting as a server vs. TLS acting as a client (dependent on what TLS Technical Committee creates)
- Protection of authentication passwords
- Inclusion of Wi-Fi (especially with development of WPA3)
- Addition of requirements for support of SNMPv3
- Audit Log Server Requirements

Issues to be considered for HCD PP Version 2.0 or HCD cPP Version 1.0

New or Modified SFRs (cont'd):

- Key Destruction SFR
- TPMs used in the TOE
- EAL Claim for HCD PP
- Password Policies
- Password Policy Applicability (normal vs. admin users)
- Kerberos Support
- S/MIME Support
- SMBv3 Support
- Others?

JISEC Comments Related to HCD PP/cPP

- JISEC would like to be one of the initiators for an ESR (Essential Security Requirements) for an HCD cPP. They will ask US, Korean, Swedish and Canadian schemes to be initiators with them.
- JISEC thinks the HCD TC should create and present a draft ESR to the initiators.
- JISEC approve all NIAP TDs as long as the reason of the decision is described clearly and the decision does not introduce inconsistency. They do not approve TD0074 as is because it does not have a described reason and because simply omitting it introduces an inconsistency of dependency. They approve the other TDs on HCD PP so far.
- JISEC advises the HCD TC, vendors and CCTLs to review Assurance Activities (AAs) carefully. They will interpret AAs literally.
- They think HCD TC should propose TDs to NIAP and JISEC.
- JISEC may consider to evaluated HCD PP version 1.1 separately, but they have currently no plan and no budget to do so.

Formation of an iTC to Generate an HCD cPP

- HDP cPP is needed to address the fact that European countries are requiring "EAL" CC certifications which is forcing some vendors to certify the same MFP twice – once against the HCD PP which has no EAL and once against 2600.2 which is at EAL2
- iTC formation has to be approved by the CCDB (Common Criteria Development Board) which requires two artifacts:
  - An ESR (Essential Security Requirements) document
  - Terms of References which addresses how the iTC will function
- Will need to establish at some point a "NIT" process for HCDs
  - Means we will set up a subgroup within the TC to address requests for interpretations of the HCD PP.
- Complicating the issue is that the IEEE 2600 PPs will be archived and no longer available from the IEEE after 2019 because of IEEE rules on how they were created
  - This is the PP used in place of the HCD PP by most of the vendors who certify HCDs in Japan, Sweden, Germany, etc.

HCD iTC Status

- Goal is still to move to an HCD iTC and create an HCD cPP
- Looking for two of the following Schemes to sponsor this activity – Korea, Sweden, Japan and maybe Canada
  - Was discussed with ITSCC (Korean scheme). ITSCC confirmed that they will gladly support iTC process for developing a collaborative Protection Profile (cPP) and related Supporting Documents (SD) under the CCRA with goal of getting HCD iTC approval during Oct 2018 CCDB Meeting or later.
  - Contacted Swedish Scheme about this; still waiting for a response

HCD iTC Status

- First step is to create draft ESR (Essential Security Requirement) document and distribute for comment in time to discuss at October 2018 HCD TC Meeting and then gather members for an iTC
  - Use existing ESR documents (Status, Background and Purpose, Use Cases, Resource to be protected, Attacker access, Attacker Resources, Boundary of Component, Essential Security Requirements, Assumptions, Optional Extensions, Objective Requirements, Outside the Scope of Evaluation) and material from HCD PP Version 1.0

Wrap Up/ Next Steps

- Submit "Final" HCD PP Version 1.1 for review at October 2018 HCD TC Meeting
- Submit ESR to CCDB as soon as possible
  - Initial HCD TC review of draft ESR by end of August 2018
  - HCD TC review of ESR Draft by end of Sep 2018
  - Will try to submit for consideration at October 2018 CCDB Meeting
- Get agreement with NIAP and JISEC on process for getting HCD PP Version 1.1 approved as soon as possible after October 2018 HCD TC Meeting and get this process started. Goal should be to get Version 1.1 approved by 1Q 2019
- Generate membership and draft Terms of Reference for a proposed HCD iTC by EOY 2018