The Printer Working Group

Imaging Device Security

February 14, 2019

PWG February 2019 Virtual Face-to-Face

Agenda

When	What
9:00 – 9:05	Introductions, Agenda review
9:05 – 10:25	Review HCD PP v1.1/ HCD ESR / HCD ToR
10:25 – 10:45	PWG HCD Security Guidelines
10:50 – 11:00	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:
  - Brian Smithson (Ricoh)
- Secretary:
  - Alan Sukert (Xerox)

Status of HCD PP Version 1.1

- Final draft HCD PP Version 1.1 created.
  - Incorporates Errata #1, all NIAP Technical Decisions and the changes approved by HCD Technical Committee
- Draft provided for review and comment by Feb 8th
  - 10 Comments Received
  - None of these comments reviewed at Feb 11 HCD TC Teleconference
- After all comments have been resolved, will submit to NIAP and JISEC for their review and approval
  - Need to get agreement with NIAP and JISEC on process for approving HCD PP Version 1.1 approved as soon as possible.
  - Goal is to get Version 1.1 approved by 2Q 2019

Comments to Final HCD PP Version 1.1 Draft

- Minor wording modification needed to the change made to the FAU_SAR.1 Audit review SFR

  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

  Change to read

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

- Minor wording correction needed to the implementation of NIAP TD0299

  Test 2: Applied to each key **help** in non-volatile memory and subject to destruction by the TOE… help → held

Comments to Final HCD PP Version 1.1 Draft

- Dependency List for FCS_COP.1(g) is incorrect as stated.

  Should be:

  Dependencies:

  [~~FDP_ITC.1 Import of user data without security attributes, or~~

  ~~FDP_ITC.2 Import of user data with security attributes, or~~

  FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

  FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

  FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

Comments to Final HCD PP Version 1.1 Draft

- FCS_KYC_EXT.1 is a dependency fo **FPT_KYP_EXT.1 Extended**.
- Dependency list should be:

  Dependencies:

  FCS_KYC_EXT.1 Extended: Key Chaining

Comments to Final HCD PP Version 1.1 Draft

- Expand on implementation of NIAP TD0074 which made FCS_CKM.1(a) an optional SFR
  - Explicitly allow the operational environment (OE) to satisfy FCS_CKM.1(a)
  - Add specification text to a new security objective for the OE, requiring the same crypto strength as FCS_CKM.1(a) and administrative protection for the keys in the OE
  - Add a new Optional Use Case for this configuration
- No specific text proposed

Comments to Final HCD PP Version 1.1 Draft

- Correct incorrect Appendix references in Security Assurance Activities for ADV: Development
  - Correct reference

    The Assurance Activities contained in Section 4, Appendix B , Appendix C , and **C.4.1** should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

    should be

    The Assurance Activities contained in Section 4, Appendix B , Appendix C , and **Appendix D** should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

Comments to Final HCD PP Version 1.1 Draft

- Correct Dependencies in FPT_TUD_EXT to be mandatory as follows:

  Dependencies:

  [FCS_COP.1(b) Cryptographic Operation (for signature generation/verification),

  FCS_COP.1(c) Cryptographic operation (Hash Algorithm)]

  should be

  Dependencies:

  FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)

  FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

Comments to Final HCD PP Version 1.1 Draft

- The TRRT query below has been submitted. NIAP has a proposed solution and is in discussion with IPA on the proposed solution. After NIAP issues a TD in response to the TRRT query, the TD should be brought into HCDPPv1.1:

  HCDPP FTP_TRP.1(b) should be selection-based, not mandatory, based on the supported device functionality.

  Rationale:

  HCDPP allows for one or more of the following functions defined in section 1.3.1.1: printing, scanning, copying. HCDPP also contains FTP_TRP.1(b) which requires the existence of a remote, non-administrative interface to the device regardless of the devices functionality. FTP_TRP.1(b) is an issue for department-level copy-only and scan-only devices, which don't have a need for a remote, non-administrative interface.

  Consider making FTP_TRP.1(b) required for printing, but optional for devices without "Printing" functionality.

Comments to Final HCD PP Version 1.1 Draft

Additional Comments from the IDS WG:

Potential Topics for Next Update to HCD PP Beyond v1.1

- Backlog of comments that need addressing (parking lot from v1.1)
- Remove cipher suites with RSA Key Assignment – when NIST approves and NIAP enforces the new updates to NIST SP 800-131A and NIST SP 800-56B
- Integrate new NIAP TLS Package
  - Based on NDcPP
  - Separates TLS as a client SFRs from TLS as a server SFRs
- Removal of support for SHA
- Key Destruction SFR
- Use of TPMs and SSDs/SEDs in the TOE
- Requirements around use of X.509 Certificates (included via reference in new TLS Package)
- Syncing with updates to NDcPP and three FDE cPPs

Potential Topics for Next Update to HCD PP Beyond v1.1

- Update Password Policies to meet NIST SP 800-171 and the new California Password Law
- Password Policy Applicability (normal vs. admin users)
- Wi-Fi Support
- SNMPv3 Support
- Kerberos Support
- S/MIME Support
- SMBv3 Support
- Incorporation of GDPR and privacy implications
- 3rd Party Entropy Sources
- Audit Log Server Requirements

Potential Topics for Next Update to HCD PP Beyond v1.1

- Consider Changes in NDcPP v2.1
  - Main substantive changes appear to be:
    - Deletion of support for 192-bit TLS cipher suites and addition of two new TLS_DHE_RSA cipher suites
    - New SFR for NTP
    - Addition of new encryption algorithms, authentication implementations and key exchange methods for SSH
    - **Audit Events.** All generation/import/change of long-term cryptographic keys (i.e. not session keys) need to be audited, including those that are automatically generated by the TOE
    - Added additional management functions for possible selection, some of which we might want to look at for inclusion in HCD PP

Status of HCD iTC and HCD cPP

- Draft of Essential Security Requirements (ESR) and Terms of Reference (ToR) documents provided to HCD TC for review and comment by Feb 8th
  - 27 Comments Received against ESR and ToR drafts
  - All 17 ESR Comments reviewed at Feb 11 HCD TC Conference Call
  - Will review all remaining comments at a Feb 25 HCD TC Conference Call
- After all comments have been resolved, will submit to CCDB for its review and approval
  - Need CCDB approval to form HCD iTC and create HCD cPP v1.0

Comments to ESR Draft

- Simplification of first draft ESR to make it more like the ND ESR
  - Simplified version is the one provided to IDS WG to review

  Comment Accepted by HCD TC
- PSTN and Document Storage are Conditionally Mandatory, which is different from Optional. The Conditionally Mandatory functions (according to HCD PP at least) are fax, document storage/retrieval, and field-replaceable nonvolatile storage.
  - Made several changes to ensure that Conditionally Mandatory and Optional requirements are listed appropriately

  Comment Accepted by HCD TC

Comments to ESR Draft

- All products should have a means for updating software. It should not be optional
  - Remove the notion that software updating is optional

  Comment Accepted by HCD TC
- Software integrity check is not limited to preventing malware distribution- there are other reasons for ensuring software integrity, not just to prevent malware distribution
  - Remove the discussion of malware.

  Comment Accepted by HCD TC

Comments to ESR Draft

- In addition to not checking User Data for malware, the ESR also does not require checking for other kinds of malicious User Data (for example, PostScript, JPEG)

  Anti-malware checks on User Data transferred to and from the HCD should be

  Resistance against malicious User Data transferred to or from the HCD.

  Comment Accepted by HCD TC

- Under 'Out of Scope for Evaluations' is anti-malware really out-of-scope and does it apply to just user data
  - Need for HCD TD to determine how to address
  - Use proposed wording in comment

  Comment Accepted "In Principle" by HCD TC; specific wording to be determined by HCD iTC

Comments to ESR Draft

- The statement “HCD shall provide mechanisms to verify the authenticity of software updates” needs to be expanded to address the case where a software update file containing malware or other “bad” software is properly digitally signed
  - Need for HCD TD to determine how to address

  Comment rejected by HCD TC
- An HCD has firmware (e.g. BIOS) in addition to software. The protection of HCD's firmware is critical to the security of the HCD.
  - Replace "software" with "firmware / software“

  Comment accepted by the HCD TC

Comments to ESR Draft

- Currently the following bulleted item in the "Attacker's Access" section covers firmware / software:
  "An attacker may cause the installation of unauthorized software on the HCD."
  - Propose to supplement the attacker's access to firmware / software above by adding the following attacker's access:
    "An attacker may change (modify or delete) firmware / software in the HCD through one of the HCD's interfaces"

    The proposed attacker's access covers access to firmware / software outside the firmware / software update process

Comment accepted by the HCD TC

Comments to ESR Draft

- Execution of corrupted code can degrade the security of the HCD. As such, the HCD should detect corrupted code, and alert when corrupted code is detected, to enable corrective action
  - Add to ESRs "HCD shall detect corrupted code"

  Comment deferred by HCD TC to be decided by HCD iTC
- Having a root of trust for the verifying boot firmware provides added assurance of the security mechanism
  - Add to ESRs "HCD shall have root of trust for verifying integrity of boot firmware"

  Comment deferred by HCD TC to be decided by HCD iTC

Comments to ESR Draft (from 1/24/19 IDS Teleconference)

- Fax should be added to the 'Use Case' discussion

  Comment rejected by the HCD TC
- Under 'Attacker's Resources' there was the statement "There is numerous PC software providing HCD users with a variety of applications delivered by each HCD vendor." Some rewording of this sentence to make it grammatically correct was suggested.

  Comment accepted by the HCD TC
- There is also the statement "The tools used for attacks are expected to be tools that are free or non-free according to the knowledge levels of the attackers"; statement should be revised or removed (Note: Chose to remove it)

  Comment accepted by the HCD TC – statement removed

Comments to ESR Draft (from 1/24/19 IDS Teleconference)

- Need to add something about physical attacks to the 'Attacker's Access' section
- Under the 'ESR' section, the statement "HCD shall test some subset of its security functionality to help ensure that subset is operating properly" should add some wording about when this subset is run and be reworded slightly to make this statement clearer

Comments to ESR Draft (from 1/24/19 IDS Teleconference)

- Under 'Assumptions' need to clarify what is meant by public access in the statement "The Operational Environment is assumed to protect the HCD from direct, public access to its LAN interface"

  Comment accepted by the HCD TC

- Under 'Optional Extensions' expand the discussion of network-fax separation to discuss prohibition of any type of network bridging

  Comment deferred to HCD iTC to determine proper wording

Comments to Draft ESR

Additional Comments from the IDS WG:

Comments to Draft ToR

- Most of the ToR refers to the iTC Chair when referencing the Chairperson. However, Lines 171 and 172 (Section 8.2) talks about Chairpersons. The ToR should be consistent in how it refers to the iTC Chair
  - Recommended using ‘iTC Chair’ consistently

Comments to Draft ToR

- Concerned about the process described in Section 7.6.2 for making technical decisions. Specifically, the Core SMEs should determine how to resolve the issue by consensus, and if no consensus is reached the iTC Chair should make the decision how to resolve the issue; then it should be up to the Technical Editor and original issuer on how to implement the resolution that is decided upon.

  Also, the Technical Editor should not be making the judgement what to do with the proposed solution; the iTC Chair should be doing that.

  - Proposal is to replace the current text on Technical Decisions and Voting in the HCD ToR with the corresponding text from the OSPP TC ToR

Comments to Draft ToR

- The ”Hardcopy Devices International Technical Community - Key persons and affiliations” document referenced in the ToR needs to be provided
  - The HCD TC will have to create this document although I did prepare a draft for TC review
- The ToR does not really talk about how persons are assigned to a given role (are they elected, do they volunteer, is there some other method used) and how long a person such as the iTC Chair stay in that role. I don't want to create a beaurocracy or a complicated process here, but the ToR should at least say something generic about this.
  - Recommended something like “The roles described below are assigned on a voluntary basis, and a person stays in a role as long as he/she wants to perform that role”

Comments to Draft ToR

- Since we may or may not be able to continue indefintiely with the Causeway tool, we shouldn't make specific reference to it in the ToR (similar to comment above).
  - Recommended something like:

    line 25: ...provided separately in the HCDiTC collaboration area

    lines 43-44: ...sends a request to the HCDiTC Chair

Comments to Draft ToR (from 1/24/19 IDS Teleconference)

- Determine what functions were applicable to an HCD in this context, whether Fax was an optional function or not, and whether the scope should include the 'Transform' function. It was agreed to relook at the 'Scope' statement in the ToR and revise as needed to address the comments
  - Proposed for now "The scope of this international Technical Community (iTC) is Hardcopy Devices (HCDs) that support at least one of the job functions of printing, scanning, copying, or fax."
- Instead of referencing Causeway in the ToR we just refer to an "approved collaboration tool" so we don't have to revise the ToR if we change collaboration tools
  - Proposed for example "In order to avoid updating this Terms of Reference (ToR), and potentially requiring another submission for approval, the key persons are defined in "Hardcopy Devices International Technical Community - Key persons and affiliations" [2] provided separately in the approved collaboration tool area"

Comments to Draft ToR (from 1/24/19 IDS Teleconference)

- The rules around 'Technical Decisions' and how they are made in the ToR are not correct
  - No agreed-upon way to fix it; HCD TC will have to work on correcting the 'Technical Decisions' process
- The ToR should include in its 'Voting' discussion some wording around who can participate to vote in terms of meeting attendance; the concern was that we didn't want to allow the case where someone joins the iTC, does not come to any meetings and then comes to a meeting where a vote is to be taken and votes against the proposal in question.
  - No agreed-upon way to fix it; HCD TC will have to work on the voting process

Comments to Draft ToR (from 1/24/19 IDS Teleconference)

- It was pointed out all the different types of SMEs mentioned in the TOR, but that only the Core SMEs are included in the technical decisions. We agreed that the whole SME discussion should be simplified in the ToR
  - Proposed something like “The Core SME team is comprised of members from industry, end user, evaluation labs, government and other Common Criteria experts who can work effectively with the rest of the iTC members.”

Comments to Draft ToR

Additional Comments from the IDS WG:

Expected Timeline for HCD PP v1.1

- Concern raised is that if we get HCD PP v1.1 approved all in-process certifications against the HCD PP would have to conform with v1.1
  - Don’t know what impact that will have
- Still need to understand the process for getting v1.1 update approved by NIAP and JISEC
  - NIAP position still appears to be to incorporate v1.1 changes into new HCD cPP
  - JISEC says to follow the same process used to approve HCD PP v1.0
- Realistic goal is now to have the contents of HCD PP v1.1 finalized and approved by the HCD TC by the Spring 2019 HCD TC Face-to-Face meeting (date TBD) and then approved by NIAP/JISEC as soon as possible thereafter

Expected Timeline for HCD iTC

- Want to finalize ESR and have a draft Terms of Reference as soon as possible so they can be submitted to the CCDB to be reviewed/approved at its April 7-9 meetings
  - Need to coordinate
- Goal is to have formation of the HCD iTC approved by the CCDB at its Spring 2019 Meeting
  - Determine who should be on the initial core team for the HCD iTC and how to recruit additional members
  - Want to have membership from vendors, CCTLs and Schemes
  - Looking for support from Korean, Japanese, US, Canadian and Swedish Schemes if possible
  - Want to have the first HCD iTC meeting at the Spring 2019 CCUF Workshop (date TBD)

Expected Timeline for HCD cPP v1.0

- Current plan is to base HCD cPP v1.0 off of HCD PP v1.1 whether it is approved or not
  - Want HCD cPP out sooner that 2-3 years after iTC formation; hope to get HCD cPP v1.0 out in 12-18 months max
  - May follow the process used by the ND iTC where new versions are available every 6 months after the initial version
- Have to determine what content beyond what is in HCD PP v1.1 should be included in HCD cPP v1.0
  - Only include what is absolutely necessary in v1.0 (e.g., NIAP TLS Package?)
  - Deal with other issues in subsequent versions

Wrap Up/ Next Steps

- Finalize HCD PP Version 1.1 and submit to NIAP/JISEC for approval as soon as possible
- Finalize HCD ESR and TOR with HCD WG (Korea and Japanese Schemes). HCD WG will submit to CCDB for its approval (hopefully no later than Mar 2019)
- Continue work to have HCD iTC in place by April 2019
- Work on a plan for what will go into HCD cPP v1.0 to present at April HCD TC Face-to-Face
- Set up HCD iTC meeting cadence and process for reviewing/approving proposed inclusions in HCD cPP by HCD iTC

BACKUP

Proposed ToR Technical Decisions/Voting Text

6.2 Decision-making

6.2.1 Editorial decisions

Editorial decisions (including correction of technical inconsistencies) are made after consulting with the SMEs (OS and/or CC SMEs) and/or Chairperson as needed.

6.2.2 Technical decisions

Decisions will be made by a consensus of the participating members. Consensus is defined as receiving no documented objections during the decision period.

Decisions may be made via email or during an in-person meeting or telephone conference call. In the case of email, the iTC will provide one or two weeks to make the decision. For in person or telephone conference calls, only members that attend the meeting will be able to participate in making the decision.

Consensus is the default and strongly preferred method for resolution. However, if after a month consensus cannot be reached for a particular issue, then majority voting will be implemented.

If there are members that disagree with a decision, they can request the reason for the objection to be documented.

Once a decision has been made by the group it will be adopted and implemented. However, as a means to change direction or scope, any member can try to build a consensus for reversing a prior decision.

Only the iTC can decide to change the Terms of Reference for the Community.

6.2.3 Comment management and resolution

All iTC members are permitted to submit comments. Comments shall be constructive, i.e. provide alternative wording to resolve the comment in a way that it could be used for a voting decision.

All written comments will be recorded, posted, and receive a posted response. Comments are made available for viewing by iTC members.

6.2.4 Voting

All comments will be taken into consideration by the iTC members who will decide either by consensus or majority voting whether the comments are viable and to be included in the HCD cPP.

Every member organization has one vote.

The majority will be calculated from the number of votes cast (including those abstaining). Majority is considered to be over 50% of the votes cast.

The iTC may vote by 2/3 of the votes cast to change the community rules set out in this document at any time.