The Printer Working Group

Imaging Device Security

May 3, 2017

Virtual Face-to-Face

Agenda

When	What
10:00 – 10:10	Introductions, Agenda review
10:10 – 10:20	Review Proposed IDS Charter Update
10:20 – 11:50	Review results of Latest MFP TC Meeting
11:50 – 12:00	Wrap Up

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

IDS Charter Update

- Draft available at ftp://ftp.pwg.org/pub/pwg/ids/charter/wd-ids-charter-20170501-draft.pdf
- Purpose of this charter update is to expand liaison role of IDS to monitor the MFP Technical Committee and any other TCs that create standards or Protection Profiles for hardcopy devices
- Will review off-line via email before going to the Steering Committee for review and subsequent vote for approval
  - Provide any comments/feedback to me directly

New HCD Protection Profile

- The new Protection Profile for Hardcopy Devices (PP_HCD_V1.0) was published on September 11.
- You can find it on NIAP's web site … https://www.niap-ccevs.org/pp/PP_HCD_V1.0/
- … and on IPA's (including links to both the original and the Japanese translation) https://www.ipa.go.jp/security/publications/pp-jp/hcd.html
- It is a US/Japan PP, not a "cPP" with broader international support.

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

- Japanese Scheme (IPA/JISEC) initiated a formal evaluation of the HCD Protection Profile (PP) against the Common Criteria PP assurance requirements
  - IPA is sponsoring the evaluation
  - ECSEC is performing the evaluation
  - It is based on the APE assurance class
    - APE is part of the standard CEM, and does not comprehend explicit assurance activities as are found in new style PPs
    - Officially, the evaluation will not cover assurance activities
    - However, the lab may make notes about them anyway
  - A draft Evaluation Technical Report has been issued to IPA
  - Final ETR is expected soon
  - Certification is expected by the end of May

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

- HCD Protection Profile (PP) evaluation results
  - Found some inconsistencies in the dependencies and in other areas that were not spelled out at the meeting
  - These inconsistencies need to be fixed
  - Will require some changes to Security Functional Requirements (SFRs); we don't know the extent of the changes – are they just grammatical changes or something more substantive
  - IPA developed an Errata to the HCD PP to address the issues found by the evaluation of the PP and sent it to NIAP for approval. NIAP will review the Errata by mid-May
    - Errata also includes the two Technical Decisions on the HCD PP made by NIAP; when published, the TDs will be archived
    - We are trying to see if we can get an advanced copy of the Errata so we can start judging the impact

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

- NIAP has available on GitHub a new template for key destruction and user data destruction that does cover Solid State Drives (SSDs)
  - Allows logical erase to meet key destruction requirements
  - Lays out different user cases based on technology that vendor can choose from in ST.
  - Also covers Self-Encrypting Drives (SEDs) and includes FDP_RIP.1 requirement to cover replaceable SDDs
- See also the CSfC Data at Rest Capability Package

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

- NIAP Technical Decisions (TDs) for the HCD PP
  - Two TDs explicitly related to the HCD PP issued:
    - FCS_CKM.1(a) Cryptographic Key Generation now an "optional" requirement
    - Clarified test assurance activities for SEDs
  - There is one TD currently in process dealing with IPsec; NIAP was not specific on exactly what the issue was, but has something to do with server and client requirements being different
  - No TDs against the HCD PP between NIAP and IPA

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

- NIAP Technical Decisions (TDs) for other PPs
  - Concern is that there are other TDs against the Network Device (ND) collaborative PP (cPP) and Full Disk Encryption (FDE) cPP from which many of the SFRs in the HCD PP came from
    - MFP TC has to assess if any of the ND and FDE TDs apply to the HCD PP
    - In the interim submit to Technical Rapid Response Team (TRRT) for the ND and FDE TDs in question to see if interpretations apply to HCD PP. Also submit to TRRT areas where there may be no TDs yet but some type of correction is needed so there can be some type of resolution

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

- Key Management Description (KMD) / Entropy Document/ TOE Summary Specification (TSS)
  - Requirements in HCD PP appendices for these two documents do not agree with requirements in the applicable SFR assurance activities for these two documents
  - The TSS should contain the information that would be publicly available around key management; any proprietary information should go in the KMD. Same approach to Entropy and other documents required by the PP.
  - Have as much information in the TSS as possible; minimize what is in the KMD and other documents
  - Include diagrams in the KMD and Entropy document to show the "big picture"; helps explain the text.
    - PP should be updated to clarify what diagrams are needed and why
  - Look at completed NIAP certifications to get a sense of what "level of detail" is required

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

- Lot of Assurance Activities are copied from other PPs and do not get the introspection they deserve or don't reflect the technology they are transferred to. Should raise the ones in question as TRRT issues
  - if too specific or don't work for a specific technology or are too general.
- We recommended that a Printer Interpretation Team (PIT) for HCDs be established to collect and process issues before going to NIAP
  - Could act as a focal point between vendors and NIAP in both directions
  - Should be something discussed between NIAP and IPA

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

- Need better way of NIAP letting vendors know about policy changes that affect the requirements in the HCD PP.
  - Need to submit a TRRT against NIAP Policy 5 to allow PPs that state compliance with FIPS 186-3 to use of FIPS 186-3 instead of requiring FIPS 186-4 as Policy 5 states
  - NIAP needs to work with vendors and labs to get products certified to meet their national security customer needs.
- Will not be held to changes in ND cPP or FDE cPP in updates to evaluations in progress against HCD PP v1.0
  - Can submit a TRRT if are things we need immediately; otherwise, any updates that we find need to be addressed should be put in update to a HCD PP

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

Questions to NIAP:

1. Can we do CC certifications against the NIAP based on TRRT responses to issues with pending TDs? IPA is OK with approach that but NIAP wasn't sure
2. What do we do for SFRs in the HCD PP that have no assurance activities associated with them? Submit to NIAP TRRT to determine if this was intentional or a mistake. However, got sense that as vendors we'll have to do something to address these missing assurance activities.
3. Can we do additional testing beyond what is indicated in the various HCD PP assurance activities? Based on the concept of 'Exact Assurance' probably not, but we should bring to TRRT to decide if acceptable

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

More Questions to NIAP:

4. Can we do alternate tests or test methods in place of the assurance activities listed in the HCD PP for a given SFR? Would have to be brought to the TRRT to determine if acceptable NIAP will look to see if it provides the same amount of assurance and same goals – that is the key.
5. What about removable flash drives? Not clear how NIAP will handle them because there is no garbage collection routines.
   - NIST has a cryptographic erase for keys that they accept but DoD doesn't accept it
   - NIAP wants to include it, however, for overrun situations or loss of devices where can't physically destroy the media but not for EOL (End of Life) situations
   - For EOL have to destroy the media

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

More Questions to NIAP:

6. Self–Encrypting Drives (SEDs) have to be certified via FDE cPP to be used for the HCD PP, but right now there are no SEDs that have been certified – what should a vendor do? NIAP hope is that there will be soon a certified SED(s) against FDE cPP v2 that would become the only NIAP-approved SEDs vendors can use in a certified product
7. If a TPM is FIPS 140-2 certified or even CC certified is that sufficient for HCD PP? NIAP wasn't sure.
   - Example is that the HCP PP requirements for RSA certification do not line up with RSA cert requirements for TPM that uses RSA. Becomes an issue in TRNG source.
   - Also difficult to submit an Entropy document for TPM – treated as 3rd party source

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

More Questions to NIAP:

8. What else should we submit to TRRT?
   - Areas where selections, assignments are unclear or inconsistent; same for SFRs in general
   - If causes confusion or missing text
   - Determine how much "is enough" in terms level of detail. Especially true for 3rd party components
9. For a certification against the HCD PP, can we use a previous TD decision regarding one of the SFRs in the HCD PP from an evaluation against another PP against?
   - It would require a new TRRT for the HCD PP

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

More Questions to NIAP:

10. What will the sunset/archive requirements be for the HCD PP? Didn't get an answer.
11. What do we do for government customers that request EAL3 given the new HCD PP?
    - We should reach out to NIAP and tell them what customers are requesting this so NIAP can address the communications gap

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

- IPA indicated there is one on-going certification against the HCD PP in Japan (Konica) and there soon will be one in the US
- IPA agreed that they will accept FIPS 140-2 certified algorithms in accordance with NIAP Policy 5.
  - Will relook at this agreement when FIPS 140-3 is finally issued (supposedly later this year)

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

Future Work for the MFP TC

- NDcPP and FDE cPP changes and updates – should they be reflected in the HCD PP at some point?
  - Will have to be coordinated between NIAP and IPA
  - Changes will have to be reviewed by the MFP TC to determine which ones need to be applied to HCDs.
- Are there some "parking lot" issues from the HCD PP development that need to be addressed?
  - TC needs to discuss these and come to some resolution
- Need to update HCD PP to address all of the issues listed in the previous slides, the Errata from the HCD PP evaluation and ND cPP and FDE cPP changes and updates
  - No defined process yet for updating the HCD PP and coordinating the changes between NIAP and IPA

Summary of April 24 & 26, 2017 MFP Technical Committee Meetings (cont)

- Still issue with IEEE 2600.1 and HCD PP both being required by different Schemes, so eventually need to transition to a cPP.
  - Is there a roadmap as to when an HCD cPP be created. NIAP doesn't have the resources to support an HCD cPP at this time.
  - To form an iTC will need CCMB/CCDB approval of the ESR, Terms of Agreement and Supporting Document rationale
  - Can try writing an ESR to get the process started, but still have to get two nations to sponsor this activity
  - Korea is very interested, but Japan has resource constraints just as the US does
  - May have to wait until the crypto WGs are finished.
  - May have to restructure the HCD PP to get it ready for a cPP format; also some administrative work that can be done
  - Will have to do require additional crypto testing beyond stating FIPS 140-2 compliance and make any crypto requirements general enough to meet needs of all the Schemes, especially in Europe.

Wrap Up/ Next Steps

- MFP TC will:
  - Review TDs against FDE and ND PPs for relevance to HCD PP
  - Review changes in FDE and ND PPs to SFRs that we pulled for HCD PP to see if corresponding changes need to be made in HCD PP
  - Look at "parking lot" issues for updates to HCD PP
  - Make updates into HCD PP v1.1 per TBD process.
  - Will continue to inform JSEC and NIAP as issues with use of the new HCD PP arise
- Will monitor move to an HCD cPP and formation of the corresponding iTC