IDS Meeting Minutes
June 10, 2021

This IDS Meeting was started at approximately 3:00 pm ET on June 10, 2021.

Attendees

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Erin Huber	Xerox
Ira McDonald	High North
Alan Sukert	
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

- The topics to be covered during this meeting were:
  - Review of the discussions at 6/7/21 HCD iTC Meeting
  - Status of the HCD Security Guidelines
  - Round Table Discussion
- Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust- policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
- Al reviewed what was discussed at the 6/7/21 Hardcopy Device international Technical Community (HCD iTC) Meetings. The main topics discussed at this meeting were:
  - Al quickly reviewed some of the comments that were adjudicated by the HCD iTC at the meeting. The comments consisted of:
    - One editorial comment against the HCD Security Problem Definition
    - Two comments against the HCD collaborative Protection Profile (cPP) – one to approve a requested change by JBMIA to modify the wording of the Key Destruction SFR (**FCS_CKM.4**) to agree with the wording of the corresponding Key Destruction SFRs from the Full Disk Encryption CPPs and one to address a JBMIA proposal to add an Application Note to the Key Protection SFR **FPT_KYP_EXT.1** to clarify how keys are to be protected.
    - One comments against the HCD Supporting Document (SD) that address a JBMIA proposal to replace the current Assurance Activities for the Key Protection SFR **FPT_KYP_EXT.1** with the Assurance Activities from the corresponding Key Protection SFRs from the Full Disk Encryption CPPs. It was noted that NIAP Technical Decision 0458 modified the Assurance Activities for the Key Protection SFRs in the Full Disk Encryption CPPs, so JBMIA is reviewing the NIAP changes to determine if they are OK with those changes before the HCD iTC approves this comment.
  - Al then discussed the current status of the HCD iTC's Hardware-anchor Integrity Verification Subgroup. In previous IDS WG meetings Al had discussed the Secure Boot SFR (**FPT_SBT_EXT.1**) that the subgroup had developed and the Assurance Activities that were formulated to accompany that SFR.
    - A couple of changes were proposed to the SFR. First, for element **FPT_SBT_EXT.1.2** which currently reads:

      FPT_SBT_EXT.1.2 The TSF shall use the Root of Trust to confirm integrity of its firmware/software at boot time using a [selection: digital signature, message authentication] verification method.

it was proposed that a 'hash' option be added to the list of possible message authentication options. The subgroup agreed that it was a valid option and will propose the change to the full HCD iTC.

Also, regarding element **FPT_SBT_EXT.1.4** which reads:

FPT_SBT_EXT.1.4 Following failure of verification, the TSF shall provide a mechanism to: [selection: revert to previous TOE image, reinstall TOE image, perform a factory reset, contact vendor support].

in response to a question from JBMIA about the "contact vendor support" option it was proposed that we add the Application Note the Network Device iTC added to its Secure Boot SFR the subgroup used to create **FPT_SBT_EXT.1**, and which addresses the "contact vendor support" option. Again, the subgroup agreed that it was a valid option and will propose the change to the full HCD iTC.

- There was also the consideration of what crypto requirements needed to be included in the HCD cPP to support the Secure Boot SFR. The subgroup felt that to support the verification in **FPT_SBT_EXT.1.2**, crypto requirements were needed to support:
  - Hash
  - Digital signature verification
  - Message authentication
  - AES and symmetric encryption
  - HMAC
  - CMAC

  In looking through the current HCD cPP draft, the subgroup found that the following crypto SFRs already in the HCD cPP would satisfy these needs:

  - Hash -- **FCS_COP.1(c) Cryptographic operation (Hash Algorithm)**
  - Digital signature verification **-- FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)**
  - Message authentication – **FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)**
  - AES – **FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)** and **FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)**
  - HMAC -- **FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)**

  Regarding CMAC the subgroup could not find any SFRs in any cPPs looked at that included CMAC as a selection option. The subgroup decided for now to not include any CMAC support in the HCD cPP and see if we get any comments regarding CMAC when the public drafts are released.

- The subgroup also looked at what additional wording needed to be added to the HCD cPP to address Secure Boot. It agreed that wording needed to be added to the section on Major Security Functions of the HCD and the section on USE CASE 1: Required Use Cases.

  Regarding the wording in the section on Major Security Functions of the HCD, the subgroup had come up with the preliminary wording "The HCD performs hardware-anchored integrity verification of firmware/software at boot to ensure corrupted firmware/software is detected." At the time we felt we couldn't complete work on this wording until ITSCC and JISEC addressed the question as to what is more important when an integrity verification of the boot

process failed – notifying someone or preventing operational code from executing. Since ITSCC and JISEC had not yet provided their answer yet it was waiting for the two Schemes response before proceeding, which was promised by the next HCD iTC Meeting on 6/14/21. Al asked the attendees if they had any comments on the wording of this sentence – Ira indicated he agreed with the wording as currently stated.

Regarding the wording in the section on USE CASE 1: Required Use Cases, the subgroup came up with the wording:

Verifying HCD function: The HCD checks itself for malfunctions by performing a self-test **and verifying software/firmware integrity** each time that it is powered on.

which will be proposed to the full HCD iTC.

- There also needs to be included some wording on what Root of Trust (RoT) is in the HCD cPP. The questions were what to include and where in the cPP to include it. Al indicated the definitions of RoT that Ira provided at the last IDS WG Meeting will be used as part of the RoT discussion. As to where in the cPP such a discussion of RoT should go, some potential places proposed are the TOE Overview, an App Note to the Secure Boot SFR or the Glossary Appendix with the definition of Root of Trust. The subgroup looked at the TOE Overview but felt that the way it is written probably did not lend itself for including a discussion of Root of Trust there. The subgroup will work on this in future meetings.

- Al then went through the current HCD iTC schedule. The 3rd Internal Drafts of the HCD cPP and SD were supposed to be available on 6/1, but they will actually be available on 6/14 so the HCD iTC is already two weeks behind schedule. Al indicated that the review of the 3rd Internal Drafts will probably extend to the end of June, but depending on the comments received there is still the possibility that the updates could be completed in time to make the 7/18 date for release of the first Public Review Draft. It is, however, more likely that draft will be delayed until at least the beginning of August.

  Al also indicated that although the goal was to have all functionality needed for v1.0 in the first Public Review draft, it is highly unlikely that will happen. However, all functionality needed for v1.0 has to be in the 2nd Public Draft, and it should be.

- Ira had no update status for the HCD Security Guidelines.
- There was no Round Table discussion.
- **Actions:** None

Next Steps

- The next IDS Meeting will be June 24, 2021 at 3:00P ET / 12:00N PT. Main topics will be review of the 6/14/21 & 6/21/21 HCD iTC Meetings, Paul Tykodi's monthly 3D Printing report and HCD Security Guidelines Status Update.