IDS Meeting Minutes
April 15, 2021

This IDS Meeting was started at approximately 3:00 pm ET on April 15, 2021.

Attendees

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

Agenda Items

- The topics to be covered during this meeting were:
  - Review of the discussions at 3/22/21 and 3/29/21 HCD iTC Meetings
  - 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 PWH 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 4/5/21 and 4/12/21 Hardcopy Device international Technical Community (HCD iTC) Meetings. Both meetings basically were review of comments against the Security Problem Definition (SPD) and GitHub Issues generated to implement the Network Subgroup's recommendations to includes SFRs and Assurance Activities from the Network Device cPP/SD for the four secure protocols, the SFRs that are dependencies for the four secure protocols, NTP and X.509 certificate verification.

  Al discussed in detail three main topics covered by the HCD iTC during these two meetings:

  - At the 4/12/21 meeting JBMIA presented a proposal to modify SFR FPT_KYP_EXT.1, Protection of Key and Key Material. The slides JBMIA presented for their proposal can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/FPT_KYP_EXT_from_JBMIA_20210412-1.pdf.

    JBMIA's rationale was that this SFR is for protection of key and key material, but the SFR does not provide requirements on how the key and key material should be protected. The SFR just says that it should not be stored in plain text. They felt the SFR should be stated more like the corresponding SFR in the Full Disk Encryption cPPs.

    There was a nice discussion at the IDS meeting about the JBMIA proposal which will be discussed at the next HCD iTC meeting. Al felt it may be the right idea but might be crossing the boundary between describing "what" needed to be done and "how" it needed to be done. Graydon expressed concerns that this proposal, and the SFR in general, did not address what vendors typically do for storage of key and key material - they store public keys in plain text and store hash values of private keys in fuses or similar nonvolatile hardware. Additionally, for public keys we only need to protect their integrity; we don't need to protect their confidentiality. The bottom line is that we have to be careful we make a distinction in how we handle requirements for storage of public vs. private keys.

  - The second area was NTP. One of the recommendations from the Network Subgroup was that we include NTP requirements in HCD cPP/SD v1.0 because NTP is so widely used, However, when the iTC discussed the inclusion on NTP it raised unexpected discussion. The issue was around the NTP SFRs in the ND cPP that would be included in the HCD cPP if the iTC agreed to add NTP.

The NTP SFRs in the ND cPP included a couple of important requirements:

- It requires the use of NTPv3 or NTPv4. Ira mentioned that NTPv3 is old and that vendors should be using NTPv4.
- It required the use of secure NTP by virtue of the requirement that the system time has to be updated either via authentication using authentication via a select set of message digest algorithms or via a trusted communication channel between the device and the NTP time source using either IPsec or DTLS.

It was mentioned that for secure NTP the new authentication scheme being used is for securing NTP is Network Time Security (NTS). We noted that NTS is mentioned in the NTP SFR from the ND cPP, likely because NTS is so new. We felt that maybe this is one case where instead of following the ND iTC we should lead the ND iTC and include NTS in the NTP SFR we include in the HCD cPP.

A third requirement for NTP is that “The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.” Ira pointed out this requirement was probably put in to be compatible with NTP v3, but that if DTLS is used this requirement becomes unnecessary.

Finally, Ira mentioned that RFC 8633, Network Time Protocol Best Current Practices might be a good place to look for NTP requirements.

- Finally, Al summarized the current recommendations of the HCD iTC subgroup looking into Hardware-anchored integrity verification requirements for HCDs. It is using the Dedicated Security Components (DSC) cPP as the basis for the SFRs that it will recommend be included in the HCD cPP to address this area.

  The Subgroup has recommended to the full HCD iTC the following elements be added the HCD SPD to address this requirement:

  - Threats
    T.WEAK_CRYPTO: An unauthorized user or attacker that observes network traffic transmitted to and from the TOE may cryptographically exploit poorly chosen cryptographic algorithms, random bit generators, ciphers or key sizes.
  - Assumptions
    A.ROT_INTEGRITY: The vendor provides a Root of Trust (RoT) that is comprised of the TOE firmware, hardware, and pre-installed public keys or required critical security parameters, free of intentionally malicious capabilities. The platform trusts the RoT since it cannot verify the integrity and authenticity of the RoT.
  - Security Objectives
    O.AUTH_FAILURES: The TOE resists repeated attempts to guess authorization data by responding to consecutive failed attempts in a way that prevents an attacker from exploring a significant amount of the space of possible authorization data values.
    Note: This Security Objective needs to be Conditionally Mandatory based on the condition that the TOE has an internal authentication mechanism. Also, the HCD must ensure the HCD does not outlaw 3rd Party external authentication mechanisms.

    O.FW_INTEGRITY: The TOE ensures its own integrity has remained intact and attests its integrity to outside parties on request.

    Note: Ira mentioned that the last part of this objective - and attests its integrity to outside parties on request – amounted to remote attestation which is an area that is not fully developed. He strongly recommended the HCD iTC not include this part of the objective in the HCD SPD.

    O.STRONG_CRYPTO: The TOE implements strong cryptographic mechanisms and algorithms according to recognized standards, including support for random bit generation based on recognized standards and a source of sufficient entropy. The TOE uses key sizes that are recognized as providing sufficient resistance to current attack capabilities.

- The Subgroup is exploring SFRs to include in the HCD cPP to address this requirement. To date, the SFRs the Subgroup are looking at are:
  - FCS_STG_EXT.1 Protected Storage

    FCS_STG_EXT.1.1 The TSF shall provide [selection: mutable hardware-based, immutable hardware-based, software-based] protected storage for asymmetric private keys and [selection: symmetric keys, persistent secrets, no other keys].
  - FDP_MFW_EXT.1 Mutable/Immutable Firmware

    FDP_MFW_EXT.1.1 The TSF shall be maintained as [selection: immutable, mutable] firmware.
  - FPT_PRO_EXT.1 Root of Trust

    FPT_PRO_EXT.1.1 The TSF shall contain an SDO that contains the identity of the Root of Trust.

    Note: We have to figure out the HCD equivalent for what an SDO (Secure Data Object) is in a dedicated security component to put in this SFR. It would be an encryption key, key material, etc.

    FPT_PRO_EXT.1.2 The TSF shall maintain Root of Trust data as [selection: immutable, mutable if and only if its mutability is controlled by a unique identifiable owner].

  The subgroup is also looking at **FDP_MFW_EXT.2 Basic Firmware Integrity**, but the issue with this SFR is that the Assurance Activities for this SFR requires taking measurements of critical memory which is very difficult to do.

  The interesting part will be figuring out what the “TSF” is in the case of an HCD for these SFRs. For DSC the TOE is the dedicated security component so the TSF (TOE security functions) apply to the full dedicated security component. However, in the case of an HCD the TOE is the full HCD but these requirements only really apply to the boot process so the “TSF” only applies to a portion of the HCD software and hardware and not the entire HCD. The HCD iTC will have to figure that out.

- Round Table:
  - There will be a CCUF Virtual Workshop May 11 & 12, 2021. Sessions will be ½ days starting at 9:00ET.
  - 2021 Additive Manufacturing Workshop, June 14-21, 2021. For information see https://ammo.ncms.org/events/2021-additive-manufacturing-workshop/

- **Actions:** None

Next Steps

- The next IDS Meeting will be April 29, 2021 at 3:00P ET / 12:00N PT. Main topic will be review of the 4/19/21 and 4/26/21 HCD iTC Meetings and preparation for the upcoming IDS Face-to-Face (F2F) session at the May PWG Virtual F2F Meetings.
- The May PWG Virtual F2F Meetings will be May 4-7, 2021. The IDS F2F Session will be on May 6, 2021 from 10A – 12N ET.