IDS WG Meeting Minutes
August 05, 2021

This IDS WG Meeting was started at approximately 3:00 pm ET on August 05, 2021.

Attendees

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

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the discussions at the HCD iTC Meetings since the last IDS WG Meeting on 7/8/21.
   - Preparation for the upcoming PWG IDS Virtual Face-to-Face on August 19th
   - Round Table Discussion
2. 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.
3. Al reviewed what was discussed at the Hardcopy Device international Technical Community (HCD iTC) Meetings since the last IDS WG Meeting on 7/8/21. The main topics discussed at these meeting was:
   - Most of the work done at these meetings was review of comments submitted against the 3rd Internal Draft of the HCD collaborative Protection Profile (cPP) and comments resulting from the work of the HCD iTC Hardware-anchored Integrity Verification Subgroup. The majority of the comments against the 3rd Internal Draft of the HCD cPP came from JISEC, the Japanese Scheme. It took the HCD iTC three meetings to go through the 51 JISEC comments against this 3rd Internal Draft.
   - There was a review of a further updated JBMIA proposal for the **FPT_KYP_EXT.1 Protection of Key and Key Material** SFR. This update was to amend the proposed application note to add examples to clarify when a key is not part of a key chain. The discussion at the HCD iTC meeting this updated proposal was presented got bogged down in understanding why these examples were necessary and in understanding how it related to the rest of the Application Note. After a lengthy discussion it was felt that JBMIA needed to go back and reword the Application Note so it was more understandable and the context of newly added text was clearer.
   - Al then reviewed the update to the May 10th HCD iTC schedule he was proposing, the update was based on the fact that the release and review of the 3rd Internal Draft of the HCD cPP and HCD SD was running around 4 weeks behind the current planned schedule. This meant that instead of the 1st Public Draft of the HCD CPP and HCD SD being released on July 18th, the Public Draft of the HCD CPP was now looking to be released on August 17th and the 1st Public Draft of the HCD SD sometime after that.

     Based on that Al developed an updated schedule with the key dates as follows:
     - 1st Public Draft of the HCD cPP: 8/17/21
     - 1st Public Draft of the HCD SD: 8/30/21
     - 2nd Public Draft of the HCD cPP/SD: 12/13/21
     - Final Draft of the HCD cPP/SD: 4/4/22

- HCD cPP/SD Published: 5/13/22 (Note: Publish Date for the 5/10 Plan was 3/25/22).

- Al then reviewed the key outcomes from the HCD iTC Hardware-anchored Integrity Verification Subgroup meetings since the last IDS Meeting. The main outcomes were:

  - The Subgroup completed work on the **FPT_SBT_EXT.1** Secure Boot SFR and it accompanying Assurance Activities. The completed proposed **FPT_SBT_EXT.1** SFR is:

    FPT_SBT_EXT.1.1 The TSF shall contain one or more chains of trust with each chain of trust anchored in a Root of Trust that is implemented in immutable memory.

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

    FPT_SBT_EXT.1.3 The TSF shall [selection: enter maintenance mode, halt boot process, reboot the device, [assignment: another behavior of TOE]] in the event of a boot time verification failure so that the corrupted software/firmware isn't executed.

    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, indicate a need to contact vendor support].

    FPT_SBT_EXT.1.5 The TSF shall contain [selection: hash data, digital signature data, message authentication code, public key for digital signature, symmetric key for message authentication with confidentiality protection as defined in FPT_SBT_EXT.1.6] in the Root of Trust.

    FPT_SBT_EXT.1.6 If symmetric key is selected in FPT_SBT_EXT.1.5, the TSF shall make the symmetric key accessible only to the Root of Trust.

    and the proposed Assurance Activities for **FPT_SBT_EXT.1** are:

    TSS
    The evaluator shall verify that the TSS describes each chain of trust and its associated Root of Trust. For each chain of trust, the evaluator shall verify:

    - that the TSS describes the hash, digital signature, or message authentication verification performed by the TOE at boot.
    - that the TSS describes data and/or key contained in the Root of Trust and how they are used for firmware/software integrity verification.
    - that the TSS describes how the Root of Trust is immutable.

    Application Note: Due to the proprietary nature of this information, the vendor may provide the information pertaining to the root of trust in a separate document. This document must be provided for review to the evaluation lab and the scheme for review but will not be posted on the approved products list page.

    Guidance
    The evaluator shall examine the guidance documentation and verify that procedures are provided on the remediation of an integrity verification failure in a chain of trust.

    Application Note: Acceptable actions for remediation of the device include reverting to a previous TOE image, reinstalling the TOE, performing a factory reset of the TOE, or contacting vendor support for assistance.

    Test
    The evaluator shall carry out the following tests.

1. During initial boot of the TOE, the evaluator shall review the initialization output or audit records and verify that the TOE successfully performs verification of the firmware/software.
2. For every link in each chain of trust, the evaluator shall attempt to boot the TOE using firmware/software with an invalid hash, digital signature, or message authentication verification and verify that the verification check fails and the TOE doesn't execute corrupted firmware/software.

   Application Note: Verification of the Root of Trust is out of scope for Test 2.
3. For every link in each chain of trust, the evaluator shall attempt to boot the TOE using a corrupted firmware image and verify that upon failure, the TOE performs the action selected within FPT_SBT_EXT.1.4.

   Note: Corruption of the Root of Trust is out of scope for Test 3.

   a. (conditional) If 'revert to previous TOE image' is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation, verifies that the TOE performed the action of reverting to a previous TOE image and confirms that the TOE returns to an operational state following the remediation action.

      Note: The administrator might need to take an action to perform the remediation action.

   b. (conditional) If 'reinstall TOE image' is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation, verifies that the TOE performed the action of reinstalling the TOE image and confirms that the TOE returns to an operational state following the remediation action.

      Note: The administrator might need to take an action to perform the remediation action.

   c. (conditional) If 'perform factory reset' is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation, verifies that the TOE performs a factory reset and confirms that the TOE returns to an initialized state where it can be returned into an operational state following the remediation action.

      Note: The administrator might need to take an action to perform the remediation action.

   (conditional) If 'indicate a need to contact vendor support' is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation and verifies that the TSF provides an indication to contact vendor support.

- Finally, at the 7/8/21 IDS Meeting Al had indicated that the Subgroup had agreed upon an SFR to include CMAC since FujiFilms indicated that they used CMAC in their products. Al again reviewed the SFR that the Subgroup agreed upon at this meeting (see the minutes from the 7/8/21 IDS WG Meeting for the specific text of this SFR).

  The Subgroup agreed on the following Assurance Activities to accompany this CMAC SFR:

  TSS
  If HMAC was selected:
  The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.

  If CMAC was selected:

The evaluator shall examine the TSS to ensure that it specifies the following values used by the CMAC function: key length, block cipher used, block size (of the cipher), and output MAC length used.

Guidance
There are no AGD evaluation activities for this SFR.

KMD
There are no KMD evaluation activities for this SFR.

Test
If HMAC was selected:
For each of the supported parameter sets, the evaluator shall compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator shall have the TSF generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating HMAC tags with the same key using a known good implementation.

If CMAC was selected:
For each of the supported parameter sets, the evaluator shall compose at least 15 sets of test data. Each set shall consist of a key and message data. The test data shall include messages of different lengths, some with partial blocks as the last block and some with full blocks as the last block. The test data keys shall include cases for which subkey K1 is generated both with and without using the irreducible polynomial R_b, as well as cases for which subkey K2 is generated from K1 both with and without using the irreducible polynomial R_b. (The subkey generation and polynomial R_b are as defined in SP800-38E.) The evaluator shall have the TSF generate CMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating CMAC tags with the same key using a known good implementation.

4. Al then reviewed what is planned to be presented at the upcoming PWG IDS Virtual Face-to-Face Meeting that will be held on August 19th from 10A – 12 N ET. Ira will present his TCG and IETF Liaison report and HCD Security Guidelines status (Ira doesn't think he will have an updated draft of the HCD Security Guidelines in time for the meeting). Al will present his usual HCD iTC and HCD cPP/SD status updates with maybe a different twist this time and then some slides about the discussion he did at a previous IDS WG Meeting about the new White House Executive Order on Cybersecurity.

5. Round Table:

   Ira provided several links of interest to the IDS members as follows:

   - Department of Commerce and NTIS (National Telecommunications and Information Administration) announcement of minimum requirements for Software Bills of Materials (SBOMs) on software deliveries to the government - https://www.ntia.doc.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials
   - NIST announcement of two key publications to enhance software supply chain security called for by May 2021 Executive Order for Cybersecurity - https://www.nist.gov/news-events/news/2021/07/nist-delivers-two-key-publications-enhance-software-supply-chain-security
   - Announcement of NIST recommended minimum standards for vendor or developer verification (testing) of software based on the May 2021 Executive Order for Cybersecurity - https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or
   - An article on the report by the Senate Committee on Homeland Security and Governmental Affairs on the readiness of 8 government agencies to defend against cyberattacks -

https://arstechnica.com/information-technology/2021/08/the-state-department-and-3-other-us-agencies-earn-a-d-for-cybersecurity/

Conferences of Note:

- USENIX Security, August 11-13, 2021
- International Cryptographic Module Conference, September 1-3, 2021.
- International Common Criteria Conference, Oct 19-20, 2021. Note: Early registration by Sep 14th.

6. **Actions:** None

Next Steps

- PWG August IDS Face-to-Face Meeting will be Thursday August 19, 2021 at 10:00 ET.
- The next IDS WG Meeting will be September 2, 2021 at 3:00P ET / 12:00N PT. Main topics will be review of the recent HCD iTC Meetings, HCD Security Guidelines Status Update, PWG August IDS Face-to-Face Meeting Post-Mortem and Round Table.