IDS Meeting Minutes
May 27, 2021

This IDS Meeting was started at approximately 3:00 pm ET on May 27, 2021.

Attendees

Ira McDonald	High North
Alan Sukert	
Brian Volkoff	Ricoh
Steve Young	Canon

Agenda Items

- The topics to be covered during this meeting were:
    - Review of the discussions at HCD iTC Meetings since the IDS Face-to-Face Meeting on May 6th
    - 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 4/10/21, 4/17/21 and 4/24/21 Hardcopy Device international Technical Community (HCD iTC) Meetings. The main topics discussed at these meetings were:
    - Al again reviewed the new Secure Boot SFR (FPT_SBT_EXT.1) that the HCD iTC's Hardware-anchored integrity verification subgroup had proposed to the HCD iTC to address the hardware-anchored integrity verification requirement in the Essential Security Requirements (ESR) document (see the minutes from the 04/29/21 IDS Meeting at https://ftp.pwg.org/pub/pwg/ids/minutes/IDS-call-minutes-20210429.pdf). He also reviewed the following Assurance Activities the subgroup developed for this SFR:

        TSS
        The evaluator shall verify that the TSS describes the digital signature or hash-based message authentication verification performed by the TOE at boot. The evaluator shall additionally examine the TSS to ensure that it 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 a secure boot failure.

        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.

        Tests
        The evaluator shall carry out the following tests.

        1. During initial boot of the TOE, the evaluator shall review the initialization output or audited events and verify that the TOE successfully performs a digital signature or message authentication verification of the firmware/software.

2. The evaluator shall attempt to boot the TOE using firmware/software with an invalid digital signature or message authentication verification and verify that the verification check fails and the TOE halts initialization.

   Application Note: Verification of the Root of Trust is out of scope for Test 2.

3. The evaluator shall attempt to boot the TOE using an invalid firmware image and verify that upon failure, the TOE performs the action selected within FPT_SBT_EXT.1.4.
4. (conditional) If ‘revert to previous TOE image’ is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation and perform the actions and confirm that the TOE returns to an operational state following the remediation action.
5. (conditional) If ‘boot into single user mode’ is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation and perform the actions and confirm that the TOE returns to an operational state following the remediation action.
6. (conditional) If ‘reinstall TOE’ is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation and perform the actions and confirm that the TOE returns to an operational state following the remediation action.
7. (conditional) If ‘factory reset’ is selected, the evaluator, following a failed boot attempt, shall review the guidance documentation and perform the actions and confirm that the TOE returns to an operational state following the remediation action.

Application Note: If ‘contact vendor support’ is selected, the evaluator may work directly with the vendor point of contact for the evaluation to exercise the guidance actions. An actual ticket is not required to be generated and submitted on the vendor support page.

- Al then went through the JBMIA comments against the FPT_SBT_EXT.1 SFR and Assurance Activities:

  1. **Comment: The expected functions and the target objects for FPT_SBT_EXT.1.2 and FPT_TST_EXT.1 looks very close. Do you expect that FPT_TST_EXT.1 will be removed?**

     JBMIA agreed the two SFRs were not redundant after It was brought that the TST Testing SFR is aimed at meeting a different ESR requirement (The HCD shall test some subset of its security functionality to ensure that the security functionality is not compromised by the detectable malfunction) than the Secure Boot SFR e.

  2. **Comment: It should be described what is "Root of Trust" in somewhere.**

     It should be described what comprises of "Root of Trust" and how "Root of Trust" is used to guarantee the integrity of software/firmware.

     It was acknowledged that this information is missing and that we are working on adding wording in the HCD cPP and HCD SD to address this issue.

     Ira provided two definitions of Root of Trust to help address this comment:

     From ISO Online Terms dictionary: Root of Trust: The complete set of Roots of Trust has at least the minimum set of functions to enable a description of the platform characteristics that affect the trustworthiness of the platform. [ISO/IEC 11889-1:2015]

     Roots of Trust: Highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. Roots of trust provide a firm foundation from which to build security and trust. Source(s): NIST SP 800-172 from NIST Roots of Trust Project

3. **Comment: What if we modify FPT_SBT_EXT.1.3 so that the expected purpose is added, and include an assignment section which allows vendor to define an appropriate behavior to fulfill the expectation in the selection? For example,**

   FPT_SBC_EXT.1.3 The TSF shall [selection: enter maintenance mode, boot into single user 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 invoked.

   According to MoM of Hardware Anchored Integrity Verification SG, I know that you are asking ITSCC and JISEC's expectation when the corrupted software/firmware is detected. I guess the result may affect this SFR, but if the expectation would be specified, please consider the above proposal.

   The discussion eventually boiled down to the question the HCD iTC posed to ITSCC (the Korean Scheme) and JISEC (the Japanese Scheme) - if an integrity verification of firmware/software at boot fails, what is more important to Scheme members -- “Notifying the user of the failure” in some way or “not execute operational code (such as printing, scanning, etc.) and allowing the device to power down in some way”. It was felt his issue couldn’t be adequately until a response from ITSCC and JISEC on this question was received.

4. **Comment: Test 1 looks not to verify the particular method, and it seems not a problem. If it is your expectation, isn't it okay to remove the sentence after "and verify that"?**

   It was pointed out that Tests 2-4 are tests for when the integrity verification fails, but Test 1 a test for a successful integrity verification, so Tests 2 and 3 do not cover Test 1. It was also pointed out that if you remove everything starting with “verity that…” from Test 1 you basically have no test case at all, so you no longer have any test case showing a successful integrity verification.

   It was agreed to make the following change to Test 1:

   During initial boot of the TOE, the evaluator shall review the initialization output or audited events and verify that the TOE successfully performs verification of the firmware/software.

5. **Comment: What kind of "mechanism" is expected for the option "contact vendor support" in FPT_SBG_EXT.1.4?**

   If you expect the indication for "contact vendor support", the wording for the option should be modified?

   We agreed that the device will not contact vendor support as the element seems to indicate, so we need to add an Application Note to clarify this particular entry. Ira made a good suggestion to change this particular option to read “display/print contact information to contact vendor support”. Al agreed to bring that up to the Hardware-anchored integrity verification subgroup at its next meeting.

6. **Comment: FPT_SBT_EXT.1.2**

   What kind of method do you expect to protect to store Symmetric key for message authentication?

   After a long discussion it was agreed that since we had to support key hash-based and hmac-based message authentication which depends on symmetric keys to do the integrity verification, we had to support protection of symmetric keys. What we will need to do next is look at what crypto SFRs are needed to support FPT_SBT_EXT.1 and what other SFRs are needed to support protection of symmetric keys.

    - Al then briefly went through three proposed changes currently being reviewed by the HCD iTC:
        1. JBMIA proposed changes to the FPT_KYP_EXT.1 Protection of Key and Key Material SFR to be more like the corresponding Full Disk Encryption (FDE) cPP and not just state that it should be stored in plaintext but spell out in more detail the specific requirements of how the key and key material shall be protected.
        2. JBMIA proposed two additional changes to the FPT_KYP_EXT.1 Protection of Key and Key Material SFR:
            - Add a new Application Note to the SFR to mimic the Application Note in the corresponding FPT_KYP_EXT.1 SFR in the Full Disk Encryption AA (FDE AA) cPP.
            - Completely change the Assurance Activities in the HCD SD for FPT_KYP_EXT.1 to add a TSS (TOE Security Specification) component and expand the required Key Management Document information.
        3. JBMIA also proposed changes to the FCS_CKM.1 Key Destruction SFR and associated Assurance Activities in the HCD SD to add requirements to address destruction of initial values of keys and key changes stores in TPMs and TPM-like devices. Al indicated that adding requirements related to TPMs and related devices was one area where work was needed in the HCD cPP and HCD SD.
           Note: Ira provided a good definition for key destruction:

           Key destruction: To remove all traces of a cryptographic key so that it cannot be recovered by either physical or electronic means. Source(s): NIST SP 800-57 Part 1 Rev.
    - Finally, Al gave a status on the latest HCD iTC schedule. The Security Problem Definition (SPD) public review is in process as per plan and the HCD iTC has received some comments – all editorial so far. The editors are developing the 3rd internal drafts on the HCD cPP and HCD SD to try to meet the 6/1/21 release data, although it's more likely the release date will be 6/8/21. Al still thinks the internal review can be done by 6/18/21 as scheduled.

      The goal is still to have all content in the first Public Review draft on 7/18, but given the issues that are still outstanding Al's personal opinion is that it's more likely there will be some issues that will not be resolved by 7/15. However, there will be sufficient content to have a first public draft by 7/15 and the second public draft on 11/1/21 will definitely have full content.
  - Ira then gave a quick update on the HCD Security Guidelines. The Trusted Computing Group's Network Equipment Group has developed an SNMP MIB for remote attestation of secure boot that will go to public review next week. This will be added to the SNMP subsection in Section 4.
- **Round Table**:
  - Enhancing Software Supply Chain Security: Workshop and Call for Position Papers on Standards and Guidelines, Virtual Only, June 2-3, 2021
  - NIST Post-Quantum Cryptography Standardization Conference, June 7-9, 2021
  - 2021 Additive Manufacturing Workshop, June 14-21, 2021. For information see https://ammo.ncms.org/events/2021-additive-manufacturing-workshop/
  - IETF 111, July 26-30, 2021
- **Actions:** None

Next Steps

- The next IDS Meeting will be June 10, 2021 at 3:00P ET / 12:00N PT. Main topics will be review of the 6/7/21 HCD iTC Meeting, Paul Tykodi's monthly 3D Printing report and HCD Security Guidelines Status Update.