IDS Conference Call Minutes
March 21, 2019

This ISD Conference Call was stated at approximately 3:00 pm ET on March 21, 2019.

Attendees

Cihan Colakoglu	Kyocera
Gerardo Colunga	HP
Graydon Dodson	Lexmark
Ira McDonald	High North
Alan Sukert	Xerox
Bill Wagner	TIC
Rick Yardumian	Canon

Agenda Items

1. Reviewed the minutes from the Mar 11th Hardcopy Device (HCD) Technical Committee (TC) Teleconference.

   - There was a long discussion about the concept of Roots of Trust and the associated entry "HCD shall verify the integrity of initial boot, operating system, and application software/firmware" the HCD TC agreed upon for inclusion in the HCD TC's version of the Essential Security Requirements (ESR) document[1].

     After a spirited discussion the members present agreed to propose to the HCD TC the following change to this requirement that would encompass the idea of "roots of trust" in the proper hardware sense:

     - **HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications.**

   - We also discussed the three ESR "requirements" that the Japanese and Korean Scheme indicated will be included in the ESR they submit to the Common Criteria Development Board (CCDB):

     a. (Conditionally mandatory) Regardless embedded or Field-Replaceable, the nonvolatile storage device should be encrypted to protect the document data and/or HCD critical data.

     b. (Optional requirement) The irretrievable deletion shall be supported by the vendor's technologies such as image overwrite, purge data, periodical erase, etc.

     c. Do not store the encryption keys as a plaintext-form, obfuscated-form, encoded-form or another obscure way. To protect these keys, HCD WG strongly recommends using the dedicated security component such as TPM, security element, or USB thumb drive.

     After some discussion we agreed to again propose to the HCD TC that they suggest to the Japanese and Korean Schemes that these three ESR "requirements" be changed to read:

     a. (Conditionally mandatory) If nonvolatile storage is present, then the nonvolatile storage device (either embedded or Field-Replaceable) should be encrypted to protect the document data and/or HCD critical data.

     b. (Optional requirement) The irretrievable deletion shall be supported by the vendor's technologies such as image overwrite, purge data, periodical erase, etc … (No change)

[1] Officially, the HCD Working Group (WG) consisting of the Japanese and Korean Schemes is responsible for preparing the ESR to be submitted to the Common Criteria Development Board. Our goal is to merge the version of the ESR the HCD TC is preparing with the version the HCD WG is preparing.

c. Do not store encryption keys in a plaintext-form, obfuscated-form, encoded-form or another obscure way. To protect these encryption keys, HCD WG strongly recommends using the dedicated security component such as a TCG TPM or Global Platform Secure Element. (we all strongly agreed that storing encryption keys in USB thumb drives was not secure at all and should not be done under any circumstances.

   Note that Ira made an important point that TPM has to be listed as TCG TPM and what the two Schemes denoted as 'security element' is actually 'Global Platform Secure Element'; both changes are required because of copyright issues.

2. Al went through briefly the iTC development process formulated by the CCDB and documented at https://www.commoncriteriaportal.org/files/communities/Establishing%20iTCs%20and%20cPP%20development%20-%20v0-7.pdf). We are currently at Step 5 heading towards Steps 6/7/8.
3. Al indicated that there were 6 comments against the HCD PP v1.1 approved by the HCD TC. All but one were correcting or including changes that had previously been approved by the HCD TC. The only new substantive change was to implement the latest NIAP Technical Decision (TD TD0939: Require FTP_TRP.1(b) only for printing documented at https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD_ID=403. This TD essentially states that the FTP_TRP.1(b) which is around ensuring a secure path between non-administrative users and the device is moved from being a Mandatory requirement to be a Conditionally Mandatory requirement, where the condition is that the HCD has a remote, non-administrative interface (so if the device is a standalone copier it would not have to meet this requirement).
4. We reviewed the latest version of the "Key Persons" list that can be found at https://ftp.pwg.org/pub/pwg/ids/wd/HCD iTC Key Persons v0.2.docx. We went through the list and made the following suggested changes to be communicated to Kwangwoo Lee who is maintain the list:
   - Change Bill Wagner's entry to read - US/TIC, IEEE-ISTO PWG/Bill Wagner, wamwagner@comcast.net
   - Add Rick Yardumian from Canon to the 'Other SMEs' list.

Actions

- Al to contact Kwangwoo Lee about the changes to the Key Persons list.

Next Steps

- There will be an IDS Conference Call in two weeks on April 4th at 3PM ET to review the output from the proposed March 25th HCD TC Conference Call and help Al prepare for the HCD TC Face-to-Face at the CCUF Workshop in Rome the week of April 8th.
- There will be a IDS WG Face-to-Face on Apr 18th at 9AM ET as part of the next PWG Face-to-Face.

This IDS Conference Call was completed at approximately 3:55 pm ET on March 21, 2019.