IDS Face-to-Face Minutes
February 10, 2021

Meeting was called to order at approximately 9:45 am ET February 10, 2021.

Attendees –

Amitha	Konica Minolta
Nick Bartolotti	Pharos
Graydon Dodson	Lexmark
Andrew Flowers	
Matt Glockner	Lexmark
Sean Kau	Google
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Marc Mulders	Konica Minolta
Alan Sukert	Xerox
Anthony Suarez	Kyocera
Michael Sweet	Lakeside Robotics
Bill Wagner	TIC
Uli Wehner	Ricoh
Steve Young	Canon

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2021-02-10-IDS-F2F.pdf.

- Minute Taker
  - Alan Sukert taking the minutes

2. Agenda:
   - Introductions, Agenda Review
   - Discuss results of latest Hardcopy Device international Technical Community (HCD iTC) Meetings and potential HCD collaborative Protection Profile (cPP) v1.0 content
   - HCD Security Guidelines 1.0 Status
   - TCG/IETF/Linux Foundation Liaison Reports
   - Wrap-Up / Next Steps
3. Went through the PWG Antitrust and Intellectual Property policies.
4. Went through the current status of the HCD iTC and its efforts to develop HCD cPP v1.0 and HCD Supporting Document (SD) v1.0. Some of the key points from this discussion were:

   - The 2nd internal drafts of the HCD cPP and HCD SD were reviewed by the full HCD iTC – 15 comments were received against the HCD cPP draft and 30 comments were received against the HCD SD draft. All comments were addressed. The final tally of the comment resolutions was as follow:

     For the 2nd HCD cPP draft:

     - 13 comments were ‘Accepted’ to be fixed for the next draft
     - 1 comment was ‘Accepted in Principle’ to be fixed in some later draft

- 1 comment was ‘Deferred’ to be addressed a later time, possible in a later version of the HCD cPP

For the 2nd HCD SD draft:

- 24 comments were ‘Accepted’ to be fixed for the next draft
- no comments were ‘Accepted in Principle’ to be fixed in some later draft
- 5 comments were ‘Deferred’ to be addressed a later time, possible in a later version of the HCD cPP
- 1 comment was ‘Not Accepted’

- The HCD iTC continued to address a major issue that started with the proposal by Ricoh concerning non-field replaceable non-volatile storage. The proposal was that non-field replaceable non-volatile storage be allowed to store key material in clear text rather than encrypted as long as the HCD had some type of “purge” function that would allow the key material to be deleted when the HCD was ready to be decommissioned or moved to another location.

  The core of the issue continues to be around the following requirement in the Essential Security Requirements (ESR) document approved by the Common Criteria Development Board (CCDB) contained the:

  “The HCD shall encrypt user document data and/or the HCD critical data (for confidentiality protection) stored on the nonvolatile storage device if it uses nonvolatile storage device for the purpose of storing those data. To support encryption, the HCD shall maintain key chains in such a way that keys and key materials are protected. Note that the initial data of the key chain stored on the nonvolatile storage device without protection do not meet the requirement”.

  Part of Ricoh’s rationale for its proposal was that one of the assumptions in the Security Problem Definition in the draft HCD cPP is that the appropriate physical security is in place in the Operational Environment. If that is the case that that should protect any non-field replaceable non-volatile memory from being removed while the device is in operation.

  The HCD iTC engaged the Korean Scheme to understand what was the rationale for this requirement. The Korean Scheme indicated that they are concerned about the Use Case where the HCD itself (includes either non-Field-replaceable or Field-replaceable non-volatile storage device) can be taken out of the operational environment; the Korean Scheme feels that in that Use Case both Field-replaceable and non-Field-replaceable non-volatile storage device need proper protection and a “purge” function does not provide such protection.

  Further discussions led the Korean Scheme to agree that vendors can suggest the "proper" level of the protection for "initial" key materials under this Use Case, meaning if vendors can show that non-Field Replaceable non-volatile storage can properly be protected without encryption, they may accept the proposed change to the ESR to allow e “Ricoh proposal”.

  The next steps in this will be for the HCD iTC to (1) update the Security Problem Definition (SPD) and ESR to include this new Use Case, (2) make a final decision on whether the ESR needs to change to address this non-field replaceable non-volatile storage issue and (3) implement the decision in terms of making any necessary changes to the ESR and SPD and getting them approved by the Korea and Japanese Schemes.

- Al discussed the latest status of the HCD iTC’s Network Subgroup. This subgroup is looking at what to do in the HCD cPP/SD for the SFRs and assurance activities for the four secure protocols – IPsec, TLS, SSH and HTTPS, although the subgroup’s charter has recently been expanded to look at additional SFRs and assurance activities for dependencies of the four secure protocols.

  Currently the Network Subgroup is leaning towards recommending to the full iTC the following:

  - Both TLS and SSH should split requirements into separate client and server requirements

- Use the IPsec, TLS, SSH and HTTPS requirements taken from ND cPP/SD v2.2e **as the basis** for the SFRs/assurance activities in HCD cPP/SD v1.0 and including DTLS. However, retain some SFRs or options in some SFRs and portions of Assurance Activities that are in the current draft HCD cPP/SD and incorporate them into the corresponding ND cPP SFRs or ND SD Assurance Activities that become part of HCD cPP/SD v1.0.
- Include the FIA_X509_EXT.* SFRs/Assurance Activities related to certificate evaluation
- Go with the ND SSHS/SSHC SFRs/Assurance Activities rather that the recently published CCUF Crypto Working Group's SSH Package but pull in selected options and tests from some of the SSH Package SFRs/Assurance Activities
- Modify the ND TLSC/TLSS SFRs to make TLS v1.2 mandatory and TLS v1.1 optional
- Use the ND cPP/SD equivalent for several crypto SFRs that are the dependencies for the four secure protocols.
- Add SFR FCS_CKM.2 which is also a dependency in the ND cPP to the four secure protocols.

One important topic was what to do about TLS 1.3 and TLS 1.1. We had hoped to incorporate TLS 1.3 into HCD cPP/SD v1.0 but were waiting to see what the ND iTC did about TLS 1.3 first. It turns out that the ND iTC's TLS Subgroup is currently stalled because NIAP recently submitted a large set of comments against the latest draft containing TLS 1.3 support, and many of the comments will require time to address. Thus, the likelihood of getting a TLS 1.3 solution from the ND iTC in time for inclusion in HCD cPP/SD 1.0 seems very unlikely at this point.

Regarding TLS 1.1, the IETF Transport Layer Security Working Group's is mandating deprecation of TLS 1.0 and TLS 1.1 and all major libraries will be pulling TLS 1.1 code by March 2021. This may force the HCD iTC to remove support for TLS 1.1 in HCD cPP/SD 1.0 rather that making it optional.

- It became very clear that the original schedule of having a first Public Draft of the HCD cPP and SD by Feb 2nd was clearly not going to be met. Al came up with a revised schedule that called for the following updated key milestones:
  - 3rd Internal Draft Submitted for Review: April 19, 2021
  - 1st Public Draft Submitted for Review: June 14, 2021
  - 2nd Public Draft Submitted for Review: Sept 20, 2021
  - Final Draft Submitted for Review: Dec 6, 2021
  - Final Documents Published: Feb 14, 2022
- Al finished the HCD iTC discussion with his thoughts what would be included in HCD cPP/SD 1.0.

  In terms of what will definitely be in HCD cPP/SD 1.0:
  - Secure protocol SFRs and Assurance Activities and the dependent crypto SFRs and Assurance Activities from ND cPP/SD with some minor additions from current HCD cPP/SD drafts
  - FIA_X.509.* Certificate Validation SFRs
  - Support for FIPS 140-3
  - SFRs and Assurance Activities to support "hardware-anchored integrity of hardware/software"
  - Removal of support for TLS 1.0

  In terms of what will probably be in HCD cPP/SD 1.0:
  - NTP Protocol
  - FCS_CKM.2 Cryptographic Key Establishment

In terms of what may be in HCD cPP/SD 1.0:

- Removal of SHA-1 support
- Removal of support for cipher suites with RSA Key Generation with keys < 2048 bits
- Removal of support for all RSA and DHE Key Exchanges

Finally, in terms of what will probably not be in HCD cPP/SD 1.0:

- Removal of support for TLS 1.1 (as indicated above, this may have to change)
- Support for TLS 1.3
- Expansion of network-fax separation to "no bridging"
- Inclusion of ALC_FLR
- NIAP TLS Package

Some other area that attendees said the HCD iTC will have to be aware of in developing HCD cPP/SD 1.0 are:

- Internationalization of the crypto requirements
- Any changes necessitated by the updates to ISO/IEC Standard 15408 that are almost ready for publishing
- IETF deprecation of MD5 and SHA-1 and removal from libraries in the next 60 days
- The fact that the ND iTC is moving to the use of ascidocs which should make it easier to take SFRs and Assurance Activities from the ND cPP and ND SD.

5. Ira then covered the latest HCD Security Guidelines status. There was no update available for this meeting, unfortunately, Smith provided updates to the Wi-Fi content in Section 4 and Ira changes much of the guidance in Section 4 as a result. Ira plan to add some material on IPP to Section 4 also.

   Ira says he plans to have an update to the HCD Security Guidelines with material for Section 5 hopefully by the end of March, and a full-content update sometime in Q3 2021.

6. For the final topic we added something new to the IDS Face-to-Face (F2F) sessions. Previously Ira gave a Liaison Report on current standards developments for the Trusted Computing Group (TCG), IETF and Linux Foundation as part of the Plenary Session of the PWG Face-to-Face of which the IDS Session is a part of. After the November 2020 PWG Face-to-Face, it was decided that Ira Liaison Report would become part of the IDS Session.

   The key points from Ira's Liaison Report were:

   - Regarding TCG standards activities, the next TCG Virtual F2F will be 22-26 February 2021. Ira said a big focus of the TCG now is on standards related to mobile devices, especially the ***TCG Runtime Integrity Preservation for Mobile*** document under the Mobile Platform Working Group.

     One TCG effort Ira made special note of was the ***TCG MARS Use Cases and Considerations*** document. MARS stands for Measurement Attestation & Reporting System and is a tiny piece symmetric-based crypto hardware that is used primarily now in automobile and IOT applications. However, it has the potential for use to support secure boot applications for low-end printers.

   - Regarding IETF standards activities, some key items Ira stressed were:
     - DTLS 1.3 RFC will be publish by Apr 2021
     - RFC for deprecating TLS v1.0 and TLS v1.1 will be published the end of Mar 2021
     - **Importing External PSKs for TLS** – this will support TLS 1.3 and will be needed for bootstrapping
     - The current work on CBOR (Concise Binary Object Representation) is focusing on Packed CBOR

  - RATS (Remote ATtestation ProcedureS) is very important to all network devices. It is important that we review the latest **RATS Architecture Draft 10** document
  - The IRTF Crypto Forum Research Group (CFRG) does research on crypto algorithms. Ira noted that there is a later draft of the **Oblivious Pseudorandom Functions (OPRFs)** than the one shown on the slide.

- Regarding the Linux Foundation OpenPrinting, the links in the slides provide details on the "Summer of Code" and "Season of Docs" projects that were completed in 2020 as well as more information on Linux Foundation OpenPrinting itself. Ira did note that there was a special IPP Scan project that was completed in Dec 2020.

  For 2021, changes in the program have delayed until March definition of what "Summer of Code" and "Season of Docs" projects will be formed this year.

7. **Wrap Up**

- Next IDS Conference Call will be on February 18, 2021
- Next IDS Face-to-Face Meeting will be during the next PWG Virtual Face-to-Face Meeting May 4-6, 2021

Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 9:40 AM ET on February 10, 2021.