IDS Face-to-Face Minutes
May 6, 2021

Meeting was called to order at approximately 10:00 am ET May 6, 2021.

Attendees –

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Sean Kau	Google
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Alan Sukert	
Michael Rhines	Qualcomm
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/2021-05-06-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 HCD collaborative Protection Profile (cPP)/Supporting Document (SD) v1.0 status
   - MASS DOT discussion with the IDS WG
   - HCD Security Guidelines 1.0 Status
   - TCG/IETF 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 SD v1.0. Some of the key points from this discussion were:
   - Additional comments were raised against the 2nd internal drafts of the HCD cPP and HCD SD to implement the recommendations of the Network Subgroup to use the SFRs and Assurance Activities from the latest versions of the Network Device (ND) cPP and SD for the four security protocols (IPsec, HTTPS, TLS, and SSH), the 7 SFRs that were dependencies for the four secure protocols and the three X.509 certificate validation SFRs.
     - 26 additional comments were received against the HCD cPP draft and all but one comment was adjudicated by the HCD iTC. The tally of the comment resolutions so far was as follow:
       - 13 comments were ‘Accepted’ to be fixed for the next draft
       - 0 comment was ‘Accepted in Principle’ to be fixed in some later draft
       - 10 comments were ‘Deferred’ to be addressed a later time, possible in a later version of the HCD cPP

  - 1 comment was not accepted
- 48 additional comments were received against the HCD SD draft; comments have only been partially adjudicated by the HCD iTC. The tally of the comment resolutions so far was as follow:
  - 29 comments were 'Accepted' to be fixed for the next draft
  - 0 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
  - 1 comment was not accepted

- The main work of the HCD iTC the past few weeks has been to complete the Security Problem Definition (SPD), send it out for internal review and fix any comments so it could be sent out for public review – a key milestone in the CCDB cPP Development Process. The SPD went through the internal review and 7 comments were generated; all 7 comments were reviewed by the HCD iTC, accepted and have been implemented in the SPD. The SPD is now in the final stages of being prepared for submittal for public review hopefully next week.

- Another Essential Security Requirements (ESR) document requirement is "The HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications" which was added at the request of the HCD iTC. The HCD iTC formed a Hardware-anchored Integrity Verification subgroup to address this requirement. This subgroup has already determined the Threats, Organizational Security Policies and Security Objectives required to go into the SPD to address this requirement and had them included in the SDP version that will go out for public review.

  In addition, the subgroup has developed a Secure Boot SFR (FPT_SBT_EXT) that addresses this ESR requirement that the subgroup will recommend to the full HCD iTC be put into the HCD cPP. This Secure Boot SFR was a merge of requirements taken from the Root of Trust SFR (FPT_PRO_EXT) from the Dedicated Security Component cPP and the Secure Boot SFR (FPT_SBT_EXT) SFR that the ND iTC developed for inclusion in the next version of the ND cPP. The subgroup is now working on the Assurance Activities that need to go into the HCD SD to accompany the proposed Secure Boot SFR.

  Ira made a comment that the subgroup aught to look into run-time integrity verification and remote attestation; Al felt these were good "parking lot" issues for future versions of the HCD cPP/SD but we wanted to keep this simple for v1.0.

- Some of the issues that the HCD iTC are working on now are:
  - The proposal to add the NTP SFR from the ND cPP is on hold while vendors determine whether they can support "secure NTP", since the NTP SFR from the ND cPP requires updating the time via either authentication using a message digest algorithm or a trust communication channel using either IPsec or DTLS.
  - JBMIA (The Japanese Manufacturing Association) presented a request to change the FPT_KYP_EXT Protection of Key and Key Material SFR. The SFR currently states "The HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications." JBMIA's concern is that the SFR is meant to meet the ESR requirement "*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," but* as stated the SFR does not indicate how to protect the keys.

    The JBMIA's proposal was to change the wording of the SFR to be more like the wording in the Full Disk Encryption SFRs which specifies various criteria that the stored protected keys

can meet to fulfil this requirement. Currently the HCD iTC is awaiting member comments on this proposal that are due by next Monday's HCD iTC meeting.

- ITSCC (the Korean Scheme) looked at the ESR requirement "The HCD shall generate audit data, and be capable of sending it to a trusted external IT entity and store it in the HCD" and made two important determinations – (1) the requirement meant that it was mandatory that every HCD had to store the audit log on the device as well as be able to transfer the audit log to a trusted external IT entity and (2) it was mandatory, not optional, that the audit log had to be readable by a device interface (although that interface did not have to be on the device so a web interface would be acceptable). This is going to be a major issue because most vendors do not now provide the ability to view the audit log via a device interface.

  The HCD iTC will have to implement the ITSCC's position because both JISEC (the Japanese scheme) and NIAP (the US Scheme) have agreed with the ITSCC's position, and we need the approval of all three schemes for the final HCD cPP/SD. The good news is that the current draft HCD cPP already has SFRs that address viewing of the audit log and restricting who can view the audit log, but they currently are optional; these SFRs will now have to be made mandatory.

  We got into a discussion at this point about whether syslog could be used to help store the audit log on the device. Ira indicated that some the IPP work may help here because it defines the fields for job creation.

- Went through some of the deferred areas that the HCD iTC needs to make a decision on such as internationalization of SFRs and removal of support for TLS 1.0, TLS 1.1, SHA-1, cipher suites with RSA Key Generation with keys < 2048 bits, and all RSA and DHE Key Exchanges.
- Al had come up with a revised schedule in Feb 2021. Even after a couple of months it became clear a further revised schedule was necessary. Al came up with a new revised schedule that called for the following updated key milestones:
  - Submit SPD for Public Review: May 10, 2021
  - 3rd Internal Draft Submitted for Review: Jun 1, 2021
  - 1st Public Draft Submitted for Review: July 19, 2021
  - 2nd Public Draft Submitted for Review: Oct 25, 2021
  - Final Draft Submitted for Review: Jan 17, 2022
  - Final Documents Published: Mar 25, 2022
- Al finished the HCD iTC discussion with his thoughts on some lessons learned over the last 14 months since the HCD iTC was formed in Feb 2020. These were:
  - Pre-Planning and getting off to a good start are essential
  - Define and agree on your rules of conduct early on, then..
  - You need to be disciplined in following your rules of conduct once you agree on them
  - Things are not going to go as planned or as scheduled, so be prepared to be flexible and to adapt
  - Make sure you have strong leadership, but that has to include someone who is willing to ask questions and offer alternatives
  - Employ sub-teams as necessary to solve specific problems

  Bill Wagner and Ira added the following two lessons learned:
  - Need to get a clear understanding of the ESR early in the cPP development process
  - Need to develop guidelines to determine when consensus can't be reached and it's time to take a formal vote on an issue

5. Al then briefly went through a discussion the two members of the Massachusetts Department of Transportation (MASS DOT) had with IDS members at one IDS Working Group Meeting. MASS DOT has a diverse print environment with new and old machines (some > 10 years old) and the two MASS DOT members were looking for some help from IDS on "the best way to deal with how to ensure their fleet of printers are safe and secure". They wanted help on how to get a baseline secure configuration for each of their devices and how to ensure that their devices have a secure configuration "out of the box" by default.

   One of the most interesting things the MASS DOT members said was this - from their experience they have noticed that even when public interfaces are specified and in place for a long time, even if they are not correctly specified, they are very difficult to get changed because printer owners are concerned about unknown consequences to customers if configurations are changed. This is something that was new to many of us at the meeting.

   The main thing we talked to the MASS DOT members about was Ira's HCD Security Guidelines, what was going to be in it when it was completed, and how it could help them with what they are trying to achieve. Al also talked about the fact that one of the artifacts that comes out of a Common Criteria certification of a printer or MFP is a set of guidelines on how to securely install and operate the printer, and they should look for them. We also went briefly into threat modelling and how Common Criteria addresses it via the SPD.

   Overall, it was an interesting discussion and a good example of how the work we do in IDS can be applied to organizations outside of PWG.

6. Ira then covered the latest updates to the HCD Security Guidelines. The updates can be found at https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20210504-rev.docx or https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20210504-rev.pdf. The updates are primarily in Section 4, Network Security and mostly in Section 4.2, Datalink Security.

   Ira went quickly through all the changes he made in Section 4. Most of the changes in Section 4, other than in Section 4.2, were mostly in rearranging the 'MUSTs' and 'SHOULDs' to be under a common heading or to add explanatory wording indicating what that sub-section was describing. The changes to Section 4.2 were more substantive in adding detailed guidance for 802.1x and W-Fi Protected Access.

   Ira indicated that he needs to add RFC references, newer 802.1x versions and a discussion of Wi-Fi certifications in Section 4. Smith also indicated that the guidance for WPA3 in Section 4.2.3 probably will need to be change to a 'MUST' in the future because WPA3 will become mandatory. Finally, Ira indicated that Chapter 5, HCD Local Security, will include discussions of USB, Bluetooth and NFC.

   At this point Ira and Smith got into a discussion about Bluetooth and the large number of CVEs against Bluetooth. Ira's concern is that enabling Bluetooth on an HCD can be very dangerous because of all these vulnerabilities. Ira agreed to send IDS members pointers to where they could view these CVEs to get an idea of all the issues against Bluetooth.

7. For the final topic Ira presented his Liaison report on current standards developments for the Trusted Computing Group (TCG) and Internet Engineering Task Force (IETF). The key points from Ira's Liaison Report were:

   - Regarding TCG standards activities, the next TCG Virtual F2F will be 14-18 June 2021 which Ira will call into. Ira said a big focus of the TCG now is still on standards related to mobile devices.
   - Regarding IETF standards activities, some key items Ira stressed were:
     - RFC 8996 for deprecating TLS 1.0 and 1.1 is in effect, so any TLS libraries now will no longer contain any code for either TLS 1.0 or TLS 1.1.
     - DTLS 1.3 RFC will be approved next Monday (5/10)
     - In looking to deprecate SHA-1, remember that draft document that deprecates SHA-1 in TLS 1.2 also deprecates MD5.

- Regarding CBOR (Concise Binary Object Representation**)** JSON will now require use of CDDL.
- Remote Attestation Procedures is focusing on remote integrity verification.
- The IRTF Crypto Forum Research Group (CFRG) does research on crypto algorithms. Ira noted that **Hashing to Elliptic Curves** is important in that it is as been found to be resistant to quantum attacks.

At the end of Ira's Liaison Report Awl asked what things in TCG and IETF IDS member should follow. Ira indicated that since TCG was only open to TCG member companies there wasn't much that could be followed except through Ira's Liaison reports – however, Ira did suggest that IDS members should have their companies join TCG if they are not members already.

Regarding IETF, Ira suggested IDS should follow the following subgroups: TLS, NTP and NTF.

8. **Wrap Up**

- Next IDS Conference Call will be on May 27, 2021
- Next IDS Face-to-Face Meeting will be during the next PWG Virtual Face-to-Face Meeting August 17-19, 2021

Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 12:00N ET on May 6, 2021.