

## IDS Face-to-Face Minutes February 6, 2020

Meeting was called to order at approximately 9:00 am local February 6, 2020.

### Attendees –

Graydon Dodson	Lexmark
Smith Kennedy	HP Inc.
Cihan Colakoglu	Kyocera
Mathew Glockner	Lexmark
Erin Huber	Xerox
Sean Kau	Google
René Laan	Canon
Jeremy Leber	Lexmark
Ira McDonald	High North
Alan Sukert	Xerox
Michael Sweet	Lakeside Robotics
Bill Wagner	TIC
Brian Volkov	Ricoh
U Wehner	Ricoh
Rick Yardumian	Canon

### Agenda Items

Note: Meeting slides are available at <https://ftp.pwg.org/pub/pwg/ids/Presentation/2020-02-06-IDS-F2F.pdf>.

1. Minute Taker
  - Alan Sukert taking the minutes
2. Agenda:
  - Introductions, Agenda Review, Status
  - Discuss results of latest HCD TC Meetings and potential HCD cPP content
  - TLS 1.2 / TLS 1.3 Discussion
  - Review latest HCD Security Guide 1.0 Draft
  - Wrap-Up / Next Steps
3. Went through the PWG Intellectual Property policy.
4. Went through minutes of the HCD Technical Community (TC) Conference Calls held on 12/10/2019 and 01/10/2020, the current status the vote of the CC Management Committee (CCMC) to approve generation of an HCD international TC (iTC) and some thoughts on what the content of HCD collaborative Protection Profile (cPP) v1.0 should include. Some of the key points from this discussion were:
  - The Crypto Forum has delegated specification of TLS requirements to the Network Device iTC
  - The HCD TC/iTC is going to have to look at what TLS cipher suites should be included in HCD cPP v1.0 and how to tailor that list for the various national schemes.
  - The CCMC has finally started voting. So far, all votes return has approved formation of the HCD iTC but we have to wait for the official vote tally to formally begin formation of the iTC. Our hope is that it will be done before the CCUF Workshop Mar 15-17 in Burlington MA.

## IDS Face-to-Face Minutes February 6, 2020

- A couple of suggestions for inclusion in HCD cPP v1.0 were:
  - Looking in quantum computing and breaking weaker algorithms
  - Private block-chain models for printers

The consensus was that these were more longer-term areas that might be looked at in later versions of the HCD cPP.

- In terms of the thoughts on HCD cPP v1.0 content:
  - We definitely have to follow the industry and other standards bodies and remove support for TLS 1.0 and TLS 1.1 as well as support for 3DES and SHA-1
  - Syncing with the ND cPP and the FDE cPPs will be more important now
  - Don't forget to keep in mind EU Cybersecurity Act and ENISA

5. Ira then went through his slides on TLS 1.2 and TLS 1.3 that are part of the meeting slides; this was essentially a dry run for a presentation Ira will make to the HCD TC. A couple of keys points made were:

- Several of the standards referenced in the slides will probably have to be referenced in HCD cPP v1.0 (e.g., TLS and DTLS Security Modules, draft-09, December 2019).
- The HCD iTC will have to consider the mandatory TLS 1.3 cipher suites mentioned on Ira's slides in its implementation of TLS 1.3 in the HCD cPP.

6. Ira went through the changes made in the PDF rev version of the 1/20/2020 draft of the HCD Security Guide which is available at <https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20200120-rev.pdf>. Besides correcting the comments made to the 12/31/19 draft of the document, the only substantive changes made to the 12/31/19 draft was in Section 12 – Appendix A Internet Protocol Suite where he tried to distinguish which protocols “can be used in the Internet Protocol Suite” (non-IETF protocols) from protocols “in the Internet Protocol Suite” (IETF protocols). The only comment to the draft was as follows:

- Line 870 – Remove “used”

Ira stated that he needs to clean up Section 12 some more and was given an action to do so.

Ira indicated that the next update to the HCD Security Guide will focus on Section 4 HCD Network Security starting with discussions of TLS and SSH.

7. Alan indicated that he is retiring from Xerox on April 1<sup>st</sup> so this is his last IDS Face-to-Face Meeting.

### 8. **Wrap Up**

- Next Steps for the HCD cPP v1.0
  - Implement the transition from the HCD TC → HCD iTC
  - Complete transfer of HCD PP v1.1 to HCD cPP v1.0 draft
  - Initiate HCD PP v1.1 → HCD cPP Supporting Document draft
  - Have the first iTC meeting
  - Start work on HCD cPP v1.0
  - Develop detailed plan for development, review and release of HCD cPP v1.0
  - Determine detailed list of issues for HCD iTC to review for inclusion in HCD cPP v1.0
  - Initiate work on subgroups and create more subgroups as necessary

## **IDS Face-to-Face Minutes February 6, 2020**

- Generate first full HCD cPP v1.0 draft
- Update and review drafts as necessary to create “final” version
- Get iTC review and approval for “final” version
- Release HCD cPP v1.0
  
- AI indicated that he would like the IDS WG to pursue the following goal in 2020 -- Expand its “outreach with other standards bodies involved in HCD security issues” to other standards bodies beyond the HCD Technical Community
- Next IDS Conference Calls will be on March 5<sup>th</sup> and March 19<sup>th</sup>, 2020.
- Next IDS Face-to-Face Meeting will be during the May 5-7, 2020 PWG Face-to-Face Meeting at Lexmark in Lexington KY.

### Actions:

- Ira – Fix “all the “that can be used” clauses in Section 12 in the HCD Security Guide.

The meeting was adjourned at 10:58 am local on February 6, 2020.