IDS Conference Call Minutes
January 21, 2021

This IDS Conference Call was stated at approximately 3:00 pm ET on January 21, 2021.

Attendees

Gerardo Colunga	HP
Matt Glockner	Lexmark
Erin Huber	Xerox
Smith Kennedy	HP
Ira McDonald	High North
Alan Sukert	
Bill Wagner	TIC
Brian Volkoff	Ricoh
Steve Young	Canon

Agenda Items

- The topics to be covered during this Conference Call were:
  - Review of the discussions at the 1/11/21 and 1/18/21 HCD iTC Meetings
  - Status of the HCD Security Guidelines
  - Upcoming new addition to the IDS Conference Calls
  - Round Table Discussion
- Al reviewed what was discussed at the Hardcopy Device (HCD) international Technical Committee (iTC) meetings on 1/11/2021 and 1/18/2021. The key points discussed at the two meetings were:
  - The HCD iTC finished reviewing all of the comments against the latest draft of the HCD Supporting Document (SD). Most of them were editorial comments, although there were a couple of comments related to non-volatile storage that were deferred until the field-replaceable vs. non-field-replaceable issue is resolved (see below).
  - Al then went through the status of The Network Subgroup (SG) of the HCD iTC since the last IDS Conference Call. The Network SG has made significant progress – it finished reviewing the SFRs and Assurance Activities for the DTLS protocol from the ND cPP v2.2e and ND SD v2.2; the Network Subgroup recommended adding the DTLS SFRs/Assurance Activities to HCD cPP/SD v1.0.

    The Network SG started reviewing the crypto SFRs and associated Assurance Activities that are dependencies on the four secure protocols starting with **FCS_COP.1/**DataEncryption Cryptographic Operation (AES Data Encryption/ Decryption) in the ND cPP. It turns out there are two SFRs in the HCD cPP that deal with data encryption - **FCS_COP.1(a)** Cryptographic Operation (Symmetric encryption/decryption) and **FCS_COP.1(d)** Cryptographic operation (AES Data Encryption/Decryption). It turns out that **FCS_COP.1(a)** is closest to with **FCS_COP.1/**DataEncryption Cryptographic Operation (AES Data Encryption/ Decryption). The Network SG reviewed both SFRs and decided to replace **FCS_COP.1(a)** in the HCD cPP with **FCS_COP.1/**DataEncryption Cryptographic Operation (AES Data Encryption/ Decryption) from the ND cPP and keep **FCS_COP.1(d)** as is.

    The Network SG also review the following SFRs from the ND cPP:
    - **FCS_CKM.1** Cryptographic Key Generation (for Asymmetric Keys) **[FCS_CKM.1(a) i**n the HCD cPP**]**
    - **FCS_COP.1/SigGen Cryptographic Operation** (Signature Generation and Verification) **[FCS_COP.1(b)** in the HCD cPP**]**

- **FCS_COP.1/Hash Cryptographic Operation** (Hash Algorithm) **[FCS_COP.1(c)** in the HCD cPP**]**
- **FCS_COP.1/KeyedHash Cryptographic** Operation (Keyed Hash Algorithm/Keyed Hash Message Authentication) **[FCS_COP.1(h)** in the HCD cPP**]**
- **FCS_RBG_EXT.1 Random Bit Generation [FCS_RBG_EXT.1 in the HCD cPP]**

The Network SG determined that in all cases the ND SFR/Assurance Activity can replace the corresponding versions in HCD cPP/SD v1.0. However, there were a couple of cases where we have to be careful. For example, **FCS_COP.1(b)** includes a DSA option that is not in the ND version; we have to make sure eliminating that option will not negatively impact vendors.

There is also a second keyed-hash SFR in the HCD cPP - **FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)**. It is a dependency of all four secure protocols (TLS, HTTPS, SSH and IPsec) but has no equivalent in the ND cPP. We need to determine whether **FCS_COP.1(g)** is still needed in the HCD cPP, given that we are now going with the ND cPP for keyed-hash message authentication.

Finally, the Network SG is recommending that we add FCS_CKM.2 to HCD cPP/SD v1.0; FCS_CKM.2 is also a dependency in the ND cPP to the four secure protocols but is not currently in the HCD cPP/SD.

- Ira mentioned that the Network iTC TLS Working Group's TLS Package work to implement TLS 1.3 has stalled and there is no outlook for when that work will be completed. On a more positive note, DTLS 1.3 should be published very soon, maybe as early as the end of this week.
- Al updated the status of the Ricoh proposal to "not require encryption keys be encrypted on non-field replaceable nonvolatile storage as long as the device has some type of purge function" that the HCD iTC has been struggling with for several weeks. Brian Woods who is Chair of the Biometrics iTC provided a source that indicated that the CCDB at the Singapore CCUF Workshop joint session, in response to a question from the CCUF, stated that change to the ESR did not require CCDB approval.

  The current approach is to put together a proposal with changes to the Security Problem Definition and ESR in line with the Ricoh proposal and have the full iTC vote on it per the voting process in the HCD iTC's Terms of Reference document. The results of the vote will determine how the iTC proceeds on this issue. Ira and others noted that although the CCDB might not have to approve the ESR change we still might have to get approval from the HCD Working Group (which is the Japanese and Korean Schemes). We will have to see if that is the case. The HCD iTC is still looking for input from ITSCC (the Korean Scheme) and NIAP on this issue also,
- We briefly discussed the status of addressing the key requirement from the ESR that "The HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications." Jerry Colunga indicated he had sent an email trying to get volunteers to help with this effort and would be setting up a meeting shortly to start working on it.
- Finally, we talked about the HCD iTC schedule. Al mentioned that at this point the schedule is essentially "blown up" – there is no way we can make the scheduled Feb 2nd date for release of the first public draft of the HCD cPP and SD. Al as Deputy HCD iTC Chair wrote a note to Kwangwoo Lee, the HCD iTC Chair, about the schedule issues. Hopefully we can discuss the schedule at the next HCD iTC meeting.

- Ira gave an updated status of the HCD Security Guidelines as follows:
  - Ira hopes to have an updated draft of the HCD Security Guidelines by the beginning of February. The draft will contain the updates to Section 4 on Wi-Fi and IEEE 802.1R that Smith helped write as well as updates to Chapter 5.
- Al shared a new subject that will become a recurring topic at future IDS Conference Calls. Al received an email from Paul Tykodi who is on the PWG Steering Committee. In brief, Paul stated that

"many different components involved in the 3D printing thread will likely be making presentations about cyber security. It might be helpful to add a recurring item into the IDS meeting calendar to report on known webinars, web sites, publications, etc. that seem relevant to IDS mission in order to build up a reference for IDS members". Al agreed that to accommodate that on the second IDS Conference Call each month there would be a "3D Printing" section where Paul could provide information on 3D printing topics he felt might be of interest to IDS members. The first such "3D Printing" section will be at the February 18th IDS Conference Call.

- Round Table:
  - ENISA Cybersecurity Standardization Conference 2010 is Feb 2-4 (see https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021), Registration is Free
  - Next TCG Meeting is Feb 22-26
- **Actions:** None

Next Steps

- The next IDS Conference Call will be February 4, 2021 at 3:00P ET / 12:00N PT. Main topic will be preparation for the upcoming PWG IDS Virtual Face-to-Face Meeting on February 10th at 10:00A ET / 7:00A PT