IDS Conference Call Minutes
November 12, 2020

This IDS Conference Call was stated at approximately 3:00 pm ET on October 29, 2020.

Attendees

Gerardo Colunga	HP
Erin Huber	Xerox
Ira McDonald	High North
Alan Sukert	
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

- The topics to be covered during this Conference Call were:
  - Review of the discussions at the 11/09/2020 HCD iTC Meeting.
  - Round Table Discussion
- Al reviewed what was discussed at the Hardcopy Device (HCD) international Technical Committee (iTC) meeting on November 9th. The key points discussed at the meeting were:
  - We looked at the updates to the HCD iTC schedule. Jerry needed an extra week to get the 2nd draft of the NSD Supporting Document ready, so it will be available Nov 16th instead of Nov 9th. That pushes back the due date for comments one week to Dec 14th and will definitely push the updates based on those comments to sometime in Jan 2021 because of the Christmas holidays. Kwangwoo also indicated that the 3rd internal draft of both the HCD cPP and SD would be available on Jan 7th 2021.

    All the meeting attendees agreed that the current schedule was unrealistic, especially the plan to have the first public draft of both documents available for release by Feb 2nd 2021. We agreed that the schedule needs to be reworked. Al agreed to bring this topic up with Kwangwoo at the next HCD iTC meeting,
  - We then discussed the status of the Ricoh proposal about allowing non-field replaceable non-volatile storage to store key material in plaintext as long as the HCD has some type of “purge” function. The way the issue was left after the last HCD iTC meeting was that the issue was deferred but that the ESR has to be changed to allow the proposal. The HCD iTC felt that before we could ask the HCD Working Group to change the ESR to allow this proposal the Security Problem Definition (SPD) that aligned with the ESR had to be developed and publicly reviewed and approved.

    The meeting attendees strongly disagreed with the iTC’s position, because we felt that the ESR had priority over the SPD. So, the HCD iTC really had to make a decision on this proposal rather than deferring it, and if the HCD iTC agreed with the proposal the ask the HCD WG to go forward with the appropriate ESR change.

    It was also brought up whether the ND cPP allowed non-field replaceable non-volatile storage to store key material in plaintext. Jerry checked the NC cPP and he indicated that the Key Destruction SFR did strongly imply that it did. Al agreed to check further into the ND cPP as well as the Mobile Device cPP at Ira’s suggestion.
  - Al then provided the latest status of the HCDC iTC Network Steering Group (SG). The Network SG is starting to look at incorporating the Secure Protocol SFRs and Assurance Activities into the next draft of the HCD cPP and SD by going through the documents Al did comparing the SFRs and Assurance Activities between what is in the first HCD cPP and SD draft and what is in the ND cPP v2.2.e and ND SD v2.2.

So far, the Network SG has looked at the ND HTTPS SFRs and ND cPP SFRs IPsec SFRs FCS_IPSEC_EXT.1.1 - FCS_IPSEC_EXT.1.10. All have been accepted for inclusion in the next HCD cPP draft with one important caveat.

When Al did the comparison, he noted that it was important that the Network SG avoid what happened when the HCD PP was created, where SFRs where just "cut and pasted" from the ND cPP and FDE cPPs and just dropped into the HCD PP without looking at them to make sure they were applicable to an HCD. The idea was to examine the differences in the ND cPP and ND SD and make sure they were acceptable.

This was borne out in FCS_IPSEC_EXT.1.7 were two important differences were noted:

1. The ND cPP SFR requires that the IKEv1 Phase 1 SA and IKE2 Lifetimes be configurable; the current HCD PP and HCD cPP draft does not require this. If we include this SFR as is, this would be a brand-new requirement that vendors would have to implement.
2. The HCD PP and current HCD cPP allow the lifetimes to be based on number of packets/number of byte as a possible selection, whereas the ND cPP only allows number of bytes as a selection. That means that if a vendor used number of packets as the selection to meet this SFR, if we went with the ND cPP SFR as is that implementation would no longer be compliant.

The Network SG noted these issues which will have to be discussed with the full HCD iTC.

Ira mentioned that the Network SG should also look at the IETF Best Practices for the secure protocols such as BCP 146.Ira agreed to send links to these BCPs so the Network SG could look at them.

The SG plans to use the Network Device (ND) cPP and SD as the basis for the SFRs and Assurance Activities that will be recommended for inclusion in HCD cPP/SD v1.0. However, we have to recognize that an HCD is difference from other network products like routers because HCDs do have server connections. So, the SG will have to look at the SFRs and Assurance Activities for the Secure Protocols carefully to make sure they are applicable for an HCD. We don't want to be in the situation the HCD TC was when developing the HCD PP where NIAP forced the TC to just "cut and paste" SFRs as is from the ND cPP and FDE cPPs into the HCD PP without any consideration as to whether they were applicable.

- Al then brought up something that came up at the CCUF Workshop he had attended the day before. At the CCUF Crypto Working Group Status presentation the WG lead indicated that they would have their SSH Package ready for publication by the end of 2020. He also indicated that this was after addressing all comments from the CCDB Crypto WG.

  The fact that this SSH Package has the de facto blessing of the CCDB Crypto WG puts the Network SG and thus the HCD iTC in an interesting dilemma – we want to use what is in the ND cPP for all the secure protocols but this SSH Package has the "blessing" of the CCDB Crypto WG and thus indirectly the CCDB. Further, as Ira pointed out, the long-term goal of the ND iTC is to eventually use packages for the secure protocols so there is commonality among all the cPPs that use them.

  So, does the HCD iTC stay with what is in the ND cPP or do we switch to the SSH package. What makes it more difficult is that Al did a comparison of the earlier draft of the SSH package with the ND cPP and they are very different (e.g., the SSH Package does not have separate SSH as a client and SSH as a server requirements like the ND cPP does). We will have to see what the Network SG and the HCD iTC decides to do.

- Round Table:
  - Jerry mentioned that the DBMS cPP does claim EAL2.

- Some upcoming events are as follows:
  - Nov 16-18: International Common Criteria Conference
  - Nov 16-20: IETF 109 Meeting in Shanghai China

Actions: None

Next Steps

- The next IDS Conference Call will be December 10, 2020 at 3:00P ET / 12:00N PT. This will be the last IDS Conference Call in 2020.