IDS Conference Call Minutes
January 7, 2021

This IDS Conference Call was stated at approximately 3:10 pm ET on January 7, 2021.

Attendees

Graydon Dodson	Lexmark
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 HCD iTC Meetings since the last IDS Conference Call on Dec 10th, 2020
  - Status of the HCD Security Guidelines
  - Round Table Discussion
- Al reviewed what was discussed at the Hardcopy Device (HCD) international Technical Committee (iTC) meetings (12/14/2020 and 1/4/2021) since the last IDS Conference Call on November 12th. The key points discussed at the two meetings were:
  - The main topic discussed at these two meetings was around the requirement in the ESR that “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”. This is related to 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.

    The latest status of this issue is that the HCD iTC wants to understand what threats and problems the HDC Working Group (i.e., the Korean and Japanese Schemes) were concerned about in including this requirement, since it is a much stricter requirement than the corresponding requirement in the HCD Protection Profile (PP) that only required encryption of user document data and/or HCD critical data stored on field-replaceable nonvolatile storage devices.

    At this point this issue is basically holding up completion of the internal collaborative PP (cPP) and Supporting Document (SD) drafts and will definitely negatively impact our schedule until we get this issue resolved. Ira made a good suggestion to resolving this issue that the HCD iTC just reject the Ricoh proposal (let Ricoh fight this issue with the HCD WG since they are the ones that want it), drop this issue entirely and go with what is in the ESR because it is so difficult to get approval for an ESR change.
  - We then briefly talked about the HCD iTC schedule. The current schedule calls for a third internal draft of the HCD cPP and SD to be available mid-January. Since the HCD iTC hasn’t gone through the comments against the 2nd HCD SD draft yet (that will happen starting next Monday’s HCD iTC meeting) that clearly will not happen. The schedule as it stands now needs to be revised to reflect where the HCD cPP and SD are in their development, which means the scheduled initial first Public Draft of both documents in Feb 2021 almost certainly will be delayed.

The HCD iTC will have to replan the various drafts and come out with a revised schedule over the next couple of meetings.

- Al then went through the status of The Network Subgroup (SG) of the HCD iTC. To date, the Network SG has made significant progress – it has recommended that the SFRs and Assurance Activities for the HTTP, IPsec, TLS and SSH protocols from the ND cPP v2.2e and ND SD v2.2 be used in HCD cPP and HCD SD v1.0 instead of the current SFRs and Assurance Activities for these four secure protocols. This has been formally proposed to the full iTC via comments against the latest HCD cPP and SD drafts and are now under review by iTC members.

  The Network SG also finished reviewing the DTLS SFRs from ND cPP v2.2e and have started reviewing the DTLS Assurance Activities from ND SD v2.2; that should be finished at our next meeting.

  However, there has been an interesting development that has complicated things for the Network SG. Last week the Common Criteria Users Forum (CCUF) Crypto Working Group published its SSH Package, v1.0 which contains a standard set of SSH SFRs and Assurance Activities to be used in cPPs and SDs. Since this SSH Package was reviewed by the Common Criteria Development Board (CCDB) Crypto WG and their comments incorporated into this final version, that means that this SSH Package has tacit approval of the CCDP Crypto WG, and by extension the tacit approval of the CCDB itself.

  Where this might become an issue is that we don’t know what the various schemes like NIAP or Japan will do with this package. Will they require that it be used in cPPs to be approved for inclusion on their country’s approved product list – that is critical, for example, to be able to sell the certified products in those countries. Al took the action from the Network SG to assess the differences between the ND cPP/SD and the CCUF SSH Package; his initial assessment was that there were some requirements differences between the two, but the test requirements between the ND SD and the CCUF SSH Package were almost complete different. This will have cost and schedule impacts because the current tools are built around the ND tests and will have to be modified to the new SSH tests if the HCD iTC switches to this SSH Package. The Network SG will review the differences more thoroughly at its next meeting.

- Finally, we quickly discussed the key requirement from the ESR that so far has not been addressed in an HCD cPP or HCD SD draft that “The HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications.” Jerry Colunga had indicated at last Monday’s HCD iTC Meeting he needed help to address this requirement and wasn’t getting any. Ira indicated there must have been some type of miscommunication because he was available and wanted to help. Al stated he would contact Jerry about it.

  Al restated that he felt NTP had to be included in HCD cPP/SD v1.0 because it is so heavily used to set the time for HCDs.

- Ira gave an updated status of the HCD Security Guidelines:
  - Smith has helped Ira add updates to Section 4 on Wi-Fi and IEEE 802.1R. He and Smith will work on additional updates to the “Wi-Fi” sub-section.
  - Ira hopes to have a new version in “a couple of months” but no specific time was given.
- As an unscheduled topic, AL shared an email he received from Paul Tykodi who is on the PWG Steering Committee. In brief, the Massachusetts Department of Transportation (MassDOT) currently has 1100 printers in its network and currently uses COTS vulnerability scanning software to review the cyber security posture of many different classes of IT assets. They want to learn more about using Common Criteria to develop printer hardening profiles, which we could then load into the vulnerability scanning software. With this information loaded, the vulnerability scanning software would be able to report whether a particular printer or multi-function device was aligned with MassDOT hardening goals given its age and capabilities.

They asked if two IT Security architects could attend an upcoming IDS meeting with Paul to learn more about how the organization can leverage the existing Common Criteria framework to potentially develop printer model focused hardening profiles. Al agreed to have them attend our next IDS Conference Call om January 21st. This is a departure from the normal CC activities but should be something different for IDS to talk about at our meetings.

- Round Table:
  - IACR Real World Conference is Jan 11-14 (see https://rwc.iacr.org/2021/). Registration is $50.
  - ENISA Cybersecurity Standardization Conference 2010 is Feb 2-4 (see https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021), Registration is Free
- **Actions:** None

Next Steps

- The next IDS Conference Call will be January 21, 2021 at 3:00P ET / 12:00N PT.