IDS Conference Call Minutes
February 18, 2021

This IDS Conference Call was stated at approximately 3:00 pm ET on February 18, 2021.

Attendees

Gerardo Colunga	HP
Graydon Dodson	Lexmark
Matt Glockner	Lexmark
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 2/15/21 HCD iTC Meeting
  - Round Table Discussion

  Note: Originally the agenda was going to include the first monthly discussion by Paul Tykodi on 3-D Printing related issues of interest to the IDS WG, but Paul had to cancel at the last minute due to a family emergency.

- Al reviewed what was discussed at the 2/15/21 Hardcopy Device (HCD) international Technical Committee (iTC) meeting. The meeting was basically a continuation of the discussions on 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.

  At the 2/8/21 HCD iTC meeting a representative of the Korean Scheme had clarified to the HCD iTC what the HCD Working Group’s rationale was for inclusion of the requirement in the ESR that all user and critical data stored in non-volatile data must be encrypted. Its main concern was making sure that the data had the proper protection if the HCD was taken completely out of its operational environment where the assumption of ‘physical protection’ might no longer apply. It was felt that even non-field replaceable data could be compromised in this scenario so it needed to be protected by encryption.

  At the 2/15/21 meeting after going over what the Korean Scheme told us the previous week there were arguments presented at the meeting both for proposing a change to the ESR[1] in some way to address this issue and leaving the ESR as it current is. Finally, the discussions boiled down to how to deal with this issue once and for all.

  The HCD iTC members present agreed that there were essentially three alternatives:

  1. Do not change the ESRv0.7 and keep the requirement that user and critical data stored on all non-volatile storage must be encrypted.
  2. Propose a change of the ESRv0.7 to the HCD WG that only requires that user and critical data stored on all field-replaceable non-volatile storage must be encrypted (i.e., be the same requirement as in the current HCD PP)
  3. Propose a change of the ESRv0.7 to the HCD WG that allows the storing the cleartext CSP in the non-field replaceable storage device if TOE has a function to purge the cleartext CSP stored in the non-field replaceable storage device.

[1] Technically, the HCD Working Group owns the ESR, so the HCD iTC can only propose ESR changes to the HCD WG for its approval

Seeing that there was not a consensus on either of the three scenarios, it was decided that the most important thing was to determine whether the HCD iTC wanted to propose a change of the ESR to address this issue to the HCD WG in the first place. If so, then the iTC could determine what specifically to propose.

To do that the HCD iTC agreed to vote on whether or not to propose a change of the ESR to the HCD WG to address this issue. The voting is currently on-going this week and is to wrap up by 2/222/21.

It should be noted that in discussing this topic at the IDS Meeting we got into some interesting about related topics like storing encryption keys in TPMs, potential methods for meeting the current ESR requirement and where keys would be stored in not in non-volatile memory.

- Al quickly went through the status of The Network Subgroup (SG) of the HCD iTC since the last IDS Conference Call. The Network SG has now completed reviewing the SFRs/Assurance Activities in the ND cPP and ND SD for:
    - All of the four secure protocols (TLS, SSH, IPsec, HTTPS), including DTLS
    - The SSH Package created by the Common Criteria Users Forum (CCUF) Crypto Working Group
    - The SFRs that are dependencies for the four secure protocols
    - And at its last meeting on 2/16/21 all the X.509 Certificate Validation SFRs.

  All that is left for now is to review the NTP SFR which will be done next week.
- Round Table:
    - Ira mentioned that Paul Tykodi has been made chair of a new ISO technical committee on 3-D printing standards.
    - Network and Distributed System Security Symposium (NDSS) 2021 is 21-25 Feb
    - Ira’s notes from the latest ND iTC Meeting:
        - The TLS Working group is only about halfway through looking at the large set of NIAP comments they received against their latest TLS 1.3 draft.
        - The ND iTC has converted from MS Word to use of GitHub and asciidocs.
        - It appears the next version of the ND cPP/SD will be v3.0, not v2.3.
- **Actions:** None

Next Steps

- The next IDS Conference Call will be March 4, 2021 at 3:00P ET / 12:00N PT. Main topic will hopefully be a discussion with the Mass DOT on their interest in obtaining help from the IDS WG.