IDS Conference Call Minutes
October 15, 2020

This IDS Conference Call was stated at approximately 3:00 pm ET on October 15, 2020.

Attendees

Cihan Colakoglu	
Gerardo Colunga	HP
Graydon Dodson	Lexmark
Erin Huber	Xerox
Smith Kennedy	HP
Rene Laan	Canon
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 HCD iTC Meetings since that last IDS Conference Call on Sept 17th.
  - Status of the HCD Security Guidelines
  - Round Table Discussion
- Al reviewed what was discussed at the Hardcopy Device (HCD) international Technical Committee (iTC) meetings since our last IDS Conference Call on September 17th. The key points discussed at the meeting were:
  - The key issue that was discussed was a proposal by Ricoh dealing with non-field replaceable (or non-field removable) non-volatile storage. Ricoh proposed that non-field replaceable non-volatile storage be allowed to store key material in clear text rather than encrypted as long as the HCD had some type of "purge" function that would allow the key material to be deleted when the HCD was ready to be decommissioned or moved to another location.

    The issue was that the Essential Security Requirements (ESR) document approved by the Common Criteria Development Board (CCDB) contained the following requirement:

    "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. **To support encryption, the HCD shall maintain key chains in such a way that keys and key materials are protected. Note that the initial data of the key chain stored on the nonvolatile storage device without protection do not meet the requirement**"

    The bolded text would seem to imply, depending on how you interpreted what "protected" meant, that the ESR would not allow such a proposal, so if we agreed on this proposal the ESR would have to be changed. Jerry pointed out that any change to the ESR would have to be approved by the CCDB so ESR changes cannot be taken lightly. Ira then suggested that if we are going to make this change, assuming this proposal is eventually accepted, that there will likely be other ESR changes required as we develop the HCD cPP/SD v1.0 so we should submit all the ESR changes at one time, which makes sense.

    There were several arguments for and against this proposal presented at the iTC meetings – for example, Tom Benkart pointed out that if the HCD become broken and the purge cannot be performed that the key material is still vulnerable. At the current time there is no

consensus as to how to resolve this proposal. Ira suggested that a subcommittee of the iTC be formed to come up off-line with a recommendation to the full iTC as to whether we should accept or reject this proposal so we don't get bogged down like we did with the EAL1 vs. EAL2 issue. Al agreed to present this option to Kwangwoo Lee, the HCD iTC Chair.

- Al went quickly through a JBMIA (the Japanese vendor association) proposal that was related to this issue. The interesting point was that in their analysis they found an inconsistency in the Full Disk Encryption (FDE) cPP related to key material. Al agreed to pass that inconsistency along to the FDE iTC.
- Ira provided a high-level summary of the HCDC iTC Network Steering Group (SG) he is leading. This Steering Group's main goal is to determine how to address the requirements for the four secure protocols – IPsec, TLS, SSH and HTTPS – in the HCD cPP/SD. The main points that Ira mentioned were that:
  - The Network Device (ND) TLS subgroup is addressing TLS 1.3 and DTLS but there is no ND SSH subgroup.
  - SSH requirements are being addressed by the CCUF Crypto Working Group which has released an SSH package
  - The Network SG clearly agrees that both TLS and SSH should split requirements into separate client and server requirements
  - The current Network SG recommendation is that HCD cPP/SD 1.0 use the IPsec, TLS, SSH and HTTPS requirements taken from ND cPP/SD v2.2e **as is**.
  - Regarding DTLS, the current Network SG position is that HCD cPP/SD v1.0 will not include requirements for DTLS unless vendors indicate that they need to support it.
- Al then quickly went through the 68 comments against the first draft of the HCD cPP, all of which have all been reviewed and processed by the full HCD iTC. The next step will be to review the 28 comments against the first draft of the HCD SD starting at the next HCD iTC meeting.

- Round Table:
  - The International Cryptographic Module Conference was held Sep 21-24. Since this is the major crypto certification conference of the year, Al asked if any of the meeting attendees had attended the conference and could give a brief summary, Erin and Graydon had attended and their summary was:
    - A big topic at the conference was the changes in the definition of entropy. NIST is changing SP 800-90A and 800-90B and adding a new SP 800-90C. NIST SP 800-90B is going to become more important.
    - There was a lot of discussion about FIPS 140-3 that goes into effect 9/21/21 and the new NIST "400" series publications that implement FIPS 140-3.
    - NIAP is updating their crypto policy but there weren't a lot of details presented at the conference. We do know that CAVS is being replaced by ACVP.
  - Some other upcoming events are as follows:
    - Oct 19-21: NIST Lightweight Crypto Workshop
    - Nov 3-4: IEEE 1609 Workshop
    - Nov 4-6: NIST NTDS Workshop
    - Nov 11-12: CCUP Virtual Workshop
    - Nov 16-18: International Common Criteria Conference

Actions: Al: Discuss Ira's suggestion for resolving the Ricoh proposal with Kwangwoo

Next Steps

- The next IDS Conference Call is scheduled for October 29, 2020 at 3:00P ET / 12:00N PT
- The next IDS Working Group Virtual Face-to-Face is scheduled for November 4, 2020 at 10:00A EST / 7:00A PST