IDS Conference Call Minutes
December 10, 2020

This IDS Conference Call was stated at approximately 3:00 pm ET on December 10, 2020.

Attendees

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Erin Huber	Xerox
Smith Kennedy	HP
Ira McDonald	High North
Alan Sukert	
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

- The topics to be covered during this Conference Call were:
  - Detailed review of the latest draft of the HCD Security Guidelines
  - Review of the discussions at the 11/09/2020 HCD iTC Meeting.
  - Round Table Discussion
- The main topic of the meeting was Ira's detailed review of the 11/01/2020 update of the HCD Security Guidelines which can be found at:
  https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20201101-rev.docx
  https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20201101-rev.pdf

  The vast majority of the changes were in Section 4, HCD Network Security. Ira went through the changes line-by-line. Key points addressed in Ira's review were:
  - Most of the "requirements" in Section 4.1, Network Interface Defences, really has to do with trying to stop privilege escalation and Denial of Service attacks on the device which should be a basic essential of HCD operations.
  - Ira noted there was an error in Section 4.2.2 on Line 397 – there is a missing reference to an IEEE spec for WPA2. Ira also noted that there are some protocols for the soon to be published WPA3 that he needs to add a note for in the next draft of the Guidelines. Ira will work with Smith on this note.
  - In Section 4.3.1, in Item 2 for IPsec v2 the referenced BCP for IPsec indicates that use of IPsec v2 means that there can be no use of IPsec v1 and IKEv1. Ira indicated he hasn't included anything on key exchange for IPsec yet; that will be in an upcoming draft of the Guidelines.
  - For the SSH rules in Section 4.3.2, Ira mentioned that a key rule is not to make a root shell.
  - When discussing TLS and Section 4.3.3, the group got into brief discussion of IPP and IPP Everywhere. Ira mention the forthcoming IPP Everywhere 2.0 will mandate the use of TLS. Ira also noted that the DTLS 1.3 RFC will be published in Jan 2021. Ira's final point on IPP was that he felt you can't have a secure printing service without IPP.
  - In discussion SNMPv3 over TLS in Section 4.5.1, Ira noted that SNMPv3 should be in a container.
  - Section 4.5.3 on NETCONF was interesting because Ira pointed out that most people haven't heard of NETCONF. NETCONF is usually used more with routers but it can have uses for HCDs, which is why he made support for NETCONF a 'MAY' Ira stated that NETCONF uses YANG and SMIv2.

  - Ira stated that one of his philosophies in writing the Guidelines is to avoid a discussion of classes of HCDs and instead talk about HCDs in general.
  - Ira indicated that he will next work on Section 6, HCD System Architecture, but gave no indication when the next draft might be available.
  - We did get into a brief discussion at the end of Ira's talk about what were the intended audience and intended use of the HCD Security Guidelines, but went too far into that discussion.
- Al next reviewed what was discussed at the Hardcopy Device (HCD) international Technical Committee (iTC) meetings since the last IDS Conference Call on November 12th. The key points discussed at these meetings were:
  - The majority of these meetings were used to review comments against the second draft of the HCD collaborative Protection Profile (cPP). There were 15 new comments against the second HCD cPP draft. Some of the key comments/issues that came up during the review of these 15 comments were
    - One of the comments identified a problem that the cPP author was having with referencing Section numbers. The problem was the current method used was causing the references to change with each draft, thus causing the references in the PDF versions to be incorrect. Al worked with Brain Wood, the Chair of the CCUF Tools Working Group, who came up with a solution to the problem so now the referencing doesn't change and is correct each time.
    - A major missing item that the HCD iTC forgot was that per the iTC development process we have to create and get approved the Security Problem Definition (SPD), which is Section 4 of the cPP. We hadn't done that yet, so the HCD cPP author created a standalone SPD document from the latest HCD cPP draft which has been sent out for internal iTC review before being sent out for public review.
    - Along those lines, there were a couple of comments pointing out areas where the HCD cPP draft did not match the Essential Security Requirements (ESR) document, which is the main document approved by the Common Criteria Development Board that drives what the HCD cPP must contain. It is very important that the HCD cPP is consistent with the ESR, so the next draft of the HCD cPP and the SPD will have to address these inconsistencies with the ESR.
    - The Network Subgroup (SG) of the HCD iTC is in the process of reviewing the SFRs and Assurance Activities of the four secure protocols (IPsec, TLS, SSH and HTTPS) with the goal of synching up with the Network Device (ND) cPP v2.2e and ND Supporting Document (SD) v2.2. To date, the Network SG has recommended that the SFRs and Assurance Activities for the HTTP and IPsec protocols and the TLS SFRs be replaced in the HCD cPP and SD by the corresponding HTTP and IPsec SFRs and Assurance Activities from the ND cPP and SD. That has been formally proposed to the full iTC via comments against the latest HCD cPP draft and is now under review by iTC members.
    - At the last HCD iTC meeting on December 7th Al brought up the point that a key requirement from the ESR that so far has not been addressed in an HCD cPP or HCD SD draft is the requirement "The HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications." A subteam led by Jerry Colunga and Ira was tasked by Kwangwoo Lee, the HCD iTC Chair, at the meeting to address this oversight.

      Al noted at this meeting that there was one other set of requirements that he felt had to be added to the HCD cPP/SD from the ND cPP/SD – NTP because it is so heavily used to set the time for HCDs.
- Round Table: There was no round table discussion at this meeting.

Actions: None

Next Steps

- This is the last IDS Conference Call in 2021. The next IDS Conference Call will be January 7, 2021 at 3:00P ET / 12:00N PT.
- Everyone have a Happy Holiday Season and a Happy New Year and let’s hope 2021 is better that 2020.