IDS Meeting Minutes
April 1, 2021

This IDS Meeting was started at approximately 3:00 pm ET on April 1, 2021.

Attendees

Graydon Dodson	Lexmark
Smith Kennedy	HP
Ira McDonald	High North
Alan Sukert	
Brian Volkoff	Ricoh
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

- The topics to be covered during this Conference Call were:
    - Review of the discussions at 3/22/21 and 3/29/21 HCD iTC Meetings
    - Status of the HCD Security Guidelines
    - Round Table Discussion
- Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust- policy.pdf and the PWH Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
- Al reviewed what was discussed at the 3/22/21 and 3/29/21 Hardcopy Device international Technical Community (HCD iTC) Meetings. Both meetings basically were review of comments against the Security Problem Definition (SPD) and GitHub Issues generated to implement the Network Subgroup's recommendations to includes SFRs and Assurance Activities from the Network Device cPP/SD for the four secure protocols, the SFRs that are dependencies for the four secure protocols, NTP and X.509 certificate verification.

  Al reviewed four comments that were received from JISEC, the Japanese Scheme against the SPD and cPP. The four comments were as follows:

    - One of the requirements in the Essential Security Requirements (ESR) is that "The HCD shall generate audit data, and be capable of sending it to a trusted external IT entity and store it in the HCD". JISEC wants to change the 'Auditing' Organizational Security Policy in the SPD to agree with this ESR requirement. The issue is that this ESR requirement effectively means that the HCD has to store the audit log in the HCD as well as be able to transfer the audit log to an external server; that opens up questions as to how long the audit log has to be stored on the device (permanently vs. temporarily) and whether this requires the capability for the audit log to be read by an admin via some interface on the HCD. The HCD iTC decided to ask JISEC for some clarification on these questions before making a final determination.
    - The second comment was to address the ESR requirement that all non-volatile storage had to be encrypted in the 'Storage Encryption' Organizational Security Policy in the SPD, something the HCD iTC had already agreed to do.
    - The third comment was to add the statement "Note that the initial data of the key chain stored on the nonvolatile storage device without protection do not meet the requirement" that was in the ESR requirement to encrypt all non-volatile storage to the end of the discussion in the 'Storage Encryption' Organizational Security Policy in the SPD. What was surprising is that there was pushback from JBMIA, the Japanese Manufacturers Vendor Association, that adding this note was redundant. The HCD iTC decided to let JBMIA discuss its concern with JISEC and come back to the full iTC with a recommendation.

The fourth JISEC comment was for the HCD iTC to address in the cPP the ESR requirement “The HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications.” The HCD iTC formed a subgroup to do just that. Al summarized what this subgroup has done so far:

- The subgroup is using the Dedicated Security Components (DSC) cPP as the basis for the SFRs that we will recommend be included in the HCD cPP to address this requirement. We even had Shawn Geddis, the Chair of the DSC iTC, attend the Subgroup’s last meeting to answer some of our questions about the DSC’s SFRs.
- The Subgroup has recommended the following elements be added the HCD SPD to address this requirement:
  - Threats
    T.WEAK_CRYPTO: An unauthorized user or attacker that observes network traffic transmitted to and from the TOE may cryptographically exploit poorly chosen cryptographic algorithms, random bit generators, ciphers or key sizes.
  - Assumptions
    A.ROT_INTEGRITY: The vendor provides a Root of Trust (RoT) that is comprised of the TOE firmware, hardware, and pre-installed public keys or required critical security parameters, free of intentionally malicious capabilities. The platform trusts the RoT since it cannot verify the integrity and authenticity of the RoT.
  - Security Objectives
    O.AUTH_FAILURES: The TOE resists repeated attempts to guess authorization data by responding to consecutive failed attempts in a way that prevents an attacker from exploring a significant amount of the space of possible authorization data values.
    Note: This Security Objective needs to be Conditionally Mandatory based on the condition that the TOE has an internal authentication mechanism. Also, the HCD must ensure the HCD does not outlaw 3rd Party external authentication mechanisms.

    O.FW_INTEGRITY: The TOE ensures its own integrity has remained intact and attests its integrity to outside parties on request.

    O.STRONG_CRYPTO: The TOE implements strong cryptographic mechanisms and algorithms according to recognized standards, including support for random bit generation based on recognized standards and a source of sufficient entropy. The TOE uses key sizes that are recognized as providing sufficient resistance to current attack capabilities.
- The Subgroup is exploring SFRs to include in the HCD cPP to address this requirement. To date, the SFRs the Subgroup are looking at are:
  - FCS_STG_EXT.1 Protected Storage
  - FDP_ACC.1 Subset Access Control
  - FDP_ACF.1 Security Attribute Based Access Control
  - FDP_MFW_EXT.1 Mutable/Immutable Firmware
  - FDP_MFW_EXT.2 Basic Firmware Integrity
  - FPT_PRO_EXT.1 Root of Trust

  FDP_ACC.1 and FDP_ACF.1 are interesting in that these two SFRs are already in the HCD cPP, but they have to do with an Access Control Policy dealing with handling copy, print, scan and fax jobs; in this case these SFRs would be addressing an Access Control Policy dealing with the handling of encryption keys for the hardware anchor Root of Trust and subsequent stages of the boot process.
- Ira mentioned that ISO Glossary (https://www.iso.org/obp/) indicates this definition for root of trust: Root of Trust: component that needs to always behave in the expected manner because its

misbehavior cannot be detected. Ira also mentioned that integrity verification for firmware updates involving hardware anchors and RoTs should be done at the time of update and should be based on digital signatures using hash values stored in protected storage located in immutable storage.

- Round Table:

  Ira provided two important security links regarding SNMPv3:

  - **https://tools.ietf.org/html/rfc6353**-- Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)
  - https://datatracker.ietf.org/doc/draft-vaughn-tlstm-update/ -- TLS 1.3 Transport Model for SNMPv3

- **Actions:** None

Next Steps

- The next IDS Meeting will be April 15, 2021 at 3:00P ET / 12:00N PT. Main topic will be review of the 4/5/21 and 4/12/21 HCD iTC Meetings and a discussion by Paul Tykodi on 3-D related topics of interest to IDS members.