IDS Meeting Minutes
July 08, 2021

This IDS Meeting was started at approximately 3:10 pm ET on July 08, 2021.

Attendees

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Erin Huber	Xerox
Alan Sukert	
Bill Wagner	TIC
Brian Volkoff	Ricoh
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the discussions at 6/29/21 and 7/6/21 HCD iTC Meetings
   - HCD Security Guidelines Status
   - Round Table Discussion
2. 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 PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al started the meeting with a brief discussion about the topic at the last IDS Meeting about the mew White House Executive Order on Improving the Nation's Cybersecurity. He mentioned that there was a segment at last Sunday's "60 Minutes" program about the Solarwinds cyberattack. In the segment one of the industry SMEs interviewed mentioned the criticality of protecting the software supply chain that was attacked by the Solarwinds cyberattack. In fact, it was the Solarwinds cyberattack that was the primary event that caused the Executive Order to be written.

   Al brought up the fact that one of the main focuses of this new Executive Order is the new NIST guidelines that will be published by November on how to protect the software supply chain for any contractor that supplies products to the Federal Government. This will have a very big impact now and in the future for HCD vendors since most HCD vendors sell to the Federal Government.
4. Al reviewed what was discussed at the 6/29/21 and 7/6/21 Hardcopy Device international Technical Community (HCD iTC) Meetings. The main topics discussed at these meeting was:
   - There was a review of a further updated JBMIA proposal for the **FPT_KYP_EXT.1 Protection of Key and Key Material** SFR. This update was to incorporate the storage of keys and key material in TPMs or TPM-like and still incorporate the NIAP TD into its proposal. This updated proposal both the SFR itself and the Assurance Activities for the SFR to reflect (1) initial value of key chain that is protected (encrypted) by TPM-owned key and (2) initial value of the key chain stored in protected storage area. The implication of this is that in the Assurance Activities the evaluator does not need to verify the protection method in detail for the initial value if the key to protect is not in the key chain specified in the FCS_KYC_EXT.1 SFR or the evaluator does not need to verify the protection method implemented in the protected storage device if the key is stored in the protected storage device
   - Next Al reviewed the new naming conventions that were established thanks to Brian Volkoff for the various Cryptographic Operations and Cryptographic Key Generation SFRs. Now, instead of an SFR being denoted as FCS_COP.1(d) it is now denoted as FCS_COP.1/StorageEncryption. The idea is that the SFR names will be more understandable for the user and reviewers of the HCD cPP and HCD SD and will be much easier for the HCD iTC when trying to develop, and edit the documents. The file with the new names is attached to these minutes.

HCDPP-SFR-iterations
_updated.xlsx

- Al reviewed the key outcomes from the Hardware-anchored Integrity Verification Subgroup meetings since the last IDS Meeting. The main outcomes were:
    - Since FujiFilms indicated that they used CMAC in their products, the Subgroup had to come up with an SFR to include CMAC. JBMIA came up with a proposal for such an SFR, but it was found the Full Disk Encryption (FDE) cPPs had a CMAC SFR also. After reviewing both their own proposed SFR and the FDE cPP SFR JBMIA came back with the following SFR for CMAC which the Subgroup approved for submittal to the full HCD iTC:

        FCS_COP.1.1(c) Refinement:
        The TSF shall perform cryptographic [message authentication] in accordance with a specified cryptographic algorithm [selection: HMAC14 SHA-256, HMAC-SHA-384, HMAC-SHA-512, CMAC-AES-128, CMAC-AES-192, CMAC-AES-256] and cryptographic key sizes [assignment: key size (in bits) used in [selection: HMAC, AES]] that meet the following: [selection: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”, NIST SP 800-38B].

        Application Note:
        If one or more HMAC algorithms are selected, the ST author selects “HMAC” in the second selection and “ISO/IEC 9797-2:2011, Section 7 ‘MAC Algorithm 2’”in the third selection.

        For the assignment, the key size [k] falls into a range between L1 and L2 (defined in ISO/IEC 10118 for the appropriate hash function). For example, for SHA-256, L1 = 512 and L2 = 256 where L2 ≤ k ≤ L1.

        If one or more CMAC algorithms are selected, the ST author selects “AES” in the second selection and “NIST SP 800-38B”in the third selection.

        For the assignment, the key size will fall into a range between 128 and 256.

    - The Subgroup addressed the issue of protecting symmetric keys for message authentication. JBMIA was tasked to determine how to expand the scope of the FPT_KYP_EXT.1 SFR to include protecting the key for key-hashed message authentication. JBMIA’s conclusion was that it couldn't find the appropriate modification of the FPT_KYP_EXT.1 SFR for the purpose. Instead, it proposed the following:

        There can be 5 options based on current SFRs; Option 4 requires confidentiality for symmetric key.

#	Verification Method	What’s in immutable memory	Key protection Requirements	Data protection Requirements
1	Hash	Hash	n/a	Integrity
2	Digital Signature	Public Key	Integrity	None
3		Digital Signature	None	Integrity
4	Message Authentication	Symmetric Key	Integrity & Confidentiality	None
5		Message Authentication Code	None	Integrity

Based on this table, JBMIA proposed adding the following two elements to the FPT_SBT_EXT.1 Secure Boot SFR:

FPT_SBT_EXT.1.5 The TSF shall contain [selection: hash data, digital signature data, message authentication code, public key for digital signature, symmetric key for message authentication with confidentiality protection as defined in FPT_SBT_EXT.1.6] in the Root of Trust.

FPT_SBT_EXT.1.6 The TSF shall make the symmetric key accessible only to the Root of Trust.

JBMIA also proposed the following addition to the Assurance Activities for FPT_SBT_EXT.1:

TSS
The evaluator shall verify that the TSS describes data and/or key contained in the Root of Trust and how they are used for firmware/software integrity verification.

Guidance
None

Test
None (existing test should cover)

JBMIA also included two important remarks with its proposal:

- *Concept of chain of trust in integrity verification needs to be discussed separately, and application note may need to include description about how later chain of trust (i.e., not root of trust) need to be treated in regard to those two SFRs.*
- *There may be a discussion whether we should include such description in TSS (i.e., public) or in other private documents (like Key Management Description). If we want to keep it in private, we can put the requirement on other private documents (like Key Management Description) instead of TSS.*

The Subgroup agreed to accept the proposal with the following two changes:

a. In **FPT_SBT_EXT.1.5** and **FPT_SBT_EXT.1.6** change “Root of Trust” to Hardware Root of Trust”

b. The Subgroup agreed with JBMIA’s second remark that the data and/or key contained in the Root of Trust and how they are used for firmware/software integrity verification should not be public information and thus should be put in the KMD and not in the TSS.

- The Subgroup agreed that the HCD cPP needed to address the concept of Chains of Trust and, more importantly, the testing of the full chain need to be including in the Assurance Activities not just the anchored Root of Trust. The Subgroup agreed that the following needed to be included in the HCD cPP and HCD SD:

  - Definition of Chain of Trust in the Glossary
  - Describe in the KMD the data and/or key contained in each part of the Chain of Trust and how they are used for integrity verification of each step in the chain
  - Test integrity failure at each step in the chain
  - Include appropriate requirements regarding Chain of Trust in the HCD cPP

  The Subgroup decided that for v1.0 we should only allow for multiple chains of trust, each with its own Root of Trust and deal with any other cases in future versions of the HCD cPP/SD.

  The Subgroup decided that to fold the Chain of Trust requirements into the Secure Boot SFR, since this was the only SFR in the HCD cPP that was appropriate. It modified **FPT_SBT_EXT.1.1** and **FPT_SBT_EXT.1.2** to become:

FPT_SBT_EXT.1.1 The TSF shall contain *one or more chains of trust each with a chain of trust anchored in* a Root of Trust that is implemented in immutable memory.

FPT_SBT_EXT.1.2 The TSF shall use the *chain(s) of trust* to confirm integrity of its firmware/software at boot time using a [selection: digital signature, message authentication] verification method.

It also agreed to add an Application Note that clarifies that the Secure Boot SFR would apply to the case of multiple Chains of Trust with multiple or common Roots of Trust.

- Al finally went briefly through some of the comments that the Japanese Scheme (JISEC) had made against the latest draft of the HCD cPP. Most of them were editorial type comments (e.g., wrong versions of documents, missing dependencies, missing definitions, etc.) although some of the comments were very technical (e.g., request to split FCS_COP.1/SigGen into two separate SFRs – FCS_COP.1/SigGen and FCS_COP.1/SigVer). There are some 53 JISEC comments and so far, the HCD iTC has only gone through ten of them.

5. Ira couldn't attend the meeting, but he sent an email prior to the meeting with his report. I do not have an HCD Security Guidelines update (although I do have ideas for new content due to the EO on Supply Chain Security and the winding up of the two US NIST competitions on Lightweight Crypto (LWC) and Post Quantum Crypto (PQC).

   US NIST senior people have said in recent weeks that NIST will mandate support for at least one algorithm for PQC signatures for all federal government purchases sometime in 2022. The Common Criteria community is going to need to take the NIST and ETSI / ITU-T PQC projects much more seriously quite soon, to avoid gaps in crypto support for admin operations.

6. Round Table:

   - International Cryptographic Module Conference, September 1-3, 2021. Note: Early registration ends July 28th.
   - International Common Criteria Conference, Oct 19-20, 2021. Note: Early registration by Sep 14th.

7. **Actions:** None

Next Steps

- **No IDS Meeting on July 22, 2021.** The next IDS Meeting will be August 5, 2021 at 3:00P ET / 12:00N PT. Main topics will be review of the HCD iTC Meetings, HCD Security Guidelines Status Update and preparation for the upcoming PWG August IDS Face-to-Face Meeting.
- PWG August IDS Face-to-Face Meeting will be Thursday August 19, 2021 at 10:00 ET.