HCD iTC Ad-hoc Meeting Minutes
Feb 25, 2021

This HCD iTC Ad-hoc Meeting (titled "HCD iTC Temporary Meeting") was started at 9:00 AM KST on February 25, 2021.

Attendees

Kwangwoo Lee	HCD iTC Chair
Alan Sukert	HCD iTC Vice Chair
Tom Benkart	Acumen Security (Intertek)
Toshiyuki Sato	Toshiba
Brian Volkoff	Ricoh
Asuka Araki	RISO
Brian Smithson	Coda
Keita Kajizuka	Fuji Xerox
Ryuichiro Ohya	Fuji Xerox
Dawn Adams	EWA Canada (Intertek)
Graydon Dodson	Lexmark
Takeshi Hokiyama	Canon
Matthew Glockner	Lexmark
Takahiro Minamikawa	Fuji Xerox

Agenda Item

- A Summary of the ESRv0.7 discussion
    - At the HCD iTC meeting (2/9/2021) meeting, ITSCC (Korean Scheme) has clarified to the HCD iTC what the HCD WG's rational was for inclusion of the requirement in the ESR that user document data and/or the HCD critical data (for confidentiality protection) stored on the non-volatile storage device must be encrypted. The main concern was making sure that the data stored on the nonvolatile storage device had the proper level of protection when the HCD was taken out of its operational environment where the assumption of "physical protection" might no longer apply. At this meeting, HCD chair got a confirmation that all attendees understand the intention of HCD WG's ESR text.
    - ITSCC mentioned that they are willing to change the ESRv0.7 text (e.g. Attack resource, Use Case, and other Sections to clarify their intention but ITSCC was not intended to change the ESR section since it was clear requirement.)
    - However, HCD iTC wanted to have a full consensus. Therefore, HCD iTC got an action item to provide an input to the HCD WG how HCD iTC want to move forward (whether HCD iTC request the change of the ESR or not to the HCD WG).
    - At the HCD iTC meeting (2/16/20201) after reviewing what ITSCC told HCD iTC SME the previous week, there were arguments presented at the meeting both for proposing a change to the ESR in some way to address the issue and leaving the ESR as it is. Since HCD iTC failed to get a consensus, HCD iTC agreed to vote on whether or not to propose a change of the ESR to the HCD WG.
    - At the HCD iTC meeting (2/23/2021), the HCD iTC announced voting result that there were 20 votes cast in all, by a total of 20 of different entities. 10 entities votes for Yes (Positive, Propose a change of the ESRv0.7 to the HCD WG), while 9 entities votes for No (Negative, Do not change the ESRv0.7 and keep the requirement that user document

data and HCD critical data stored on nonvolatile storage must be encrypted)) and 1 invalid vote since HCD iTC received the vote after due date.

- However, the HCD iTC SMEs still had an issue to move forward at the HCD iTC meeting (2/23/2021) since we didn't finalize what HCD iTC will proposed a change to the HCD WG. Therefore, the HCD iTC decided to set up the HCD iTC ad-hoc meeting (scheduled as HCD iTC temporary meeting) (2/25/2021). The main purpose of this meeting was to create the text to propose a change of the ESRv0.7. The main attendees are the HCD iTC SMEs who voted "Yes (Positive)" for the previous vote and some key persons who discussed the same issue on the Network SG meeting.
- Before the HCD iTC Temporary meeting (2/25/2021), Brian Volkoff sent out the email to HCD iTC chair to request the ITSCC's clarification regarding his question/concern. HCD iTC chair forwarded the email to the ITSCC, and gratefully the HCD iTC received a prompt feedback from ITSCC.
- At the HCD iTC Temporary meeting (2/25/2021), Brian V. first shared his position and email thread that we communicated together with the ITSCC. After that, to discuss a proposal for an ESR change, Tom thankfully presented his perspectives on ITSCC's position relative to the ESR. This was based on an ad hoc discussion with the participants on the previous day's HCD Network Subgroup call.
    - Please refer to the attached emails "*Question to the ITSCC", "ITSCC's clarification for the ESRv0.7", "Perspectives on ITSCC's position relative to the ESR" and* "Brian's Email after ITSCC's response"
    - Brian made a statement in one of his emails (see "Brian's Email after ITSCC's response") before the meeting. Brian presented his email and conclusion, which was agreed by others at the meeting, from the ITSSC response to his questions was that ITSSC would not accept any change to the ESR requirement to encrypt the user document data and/or the HCD critical data stored on the non-volatile storage device.
    - During the HCD iTC Temporary meeting, all attendees agreed that Essential Security Requirements section (lines 186-190) of the ESRv0.7 is clear, and it is not a scope of change that HCD iTC has to proposed to the HCD WG. However, other parts such as lines 214 of the "Out of scope of Evaluation" section" need to be revisited since "Resistance against physical attacks of the HCD directly from outside are not to be considered." were confusing and undermined the usefulness of the requirements along with the mix of messages on welcoming vendors to contribute suggestions on state-of-the-art mechanisms.
    - Tom mentioned that because of the ITSSC response any proposed ESR change that reverted back to what is in the HCD PP (i.e., the requirement would apply only to Field-Replaceable Non-Volatile storage) would also not be accepted.
- Ohya has concerned how the vendors achieve the ITSCC's requirement with the Trusted Platform Module (TPM) since TPM requires the authorization factor in their knowledge.
    - Kwangwoo explained that ITSCC requirement is to protect the initial data of the key chain when it stored on the nonvolatile storage device, it can be satisfied by the various security mechanisms such as access control and so on. It should be confirmed by the schemes at the end.
- As a conclusion of HCD iTC Temporary meeting (2/25/2021), all attendees confirmed that they understand the intention of the ITSCC's requirement that are described in the email titled "ITSCC's clarification for the ESRv0.7". Also, HCD iTC agreed to consider the "stolen scenario". To follow up on this, HCD iTC agreed to discuss "how HCD iTC's vendor SMEs will implement ITSCC's requirement" and "What is the proper level of protection" to provide a feedback to the ITSCC.

- Sato and Ohya have asked the meeting minutes (Sato mentioned as a “document”) to the HCD iTC chair so that the JBMIA members can understand the current situation. Sato (as a chairperson of JBMIA) and Ohya mentioned that JBMIA understand the limits of what changes they can propose to the ESR that ITSSC will accept.
    - ITSSC will only change the use cases and portions of the ESR other than the actual essential security requirements section themselves to clarify this "stolen HCD" threat

Next step

- JBMIA got an action item to create a draft proposal for the change of the ESR first to make a consensus at least JBMIA members internally. JBMIA will complete this action item within a week (due date: 3/5/2021).
- Once JBMIA creates the proposal change to the ESR, the HCD iTC SMEs will review it together in a HCD iTC weekly meeting (3/9/2021) to propose a change of the ESR to address the current issue.
- Note that other members who are not a JBMIA member agreed this work plan during the call (Graydon Dodson, Matthew Glockner, Brian Volkoff, Dawn).

Action Item

- AI – Kwangwoo to share the meeting minutes with the summary our discussion and consensus
- AI – Sato/Ohya to share the current situation to the JBMIA members
- AI – JBMIA (Liaison/Representative: Toshiyuki Sato) to create the proposed ESR change text to the HCD iTC SMEs (due date: 3/5/2021)

This HCD iTC Temporary Meeting was completed at 10:20 AM KST on Feb 25, 2021 (Seoul/Tokyo).

Question to the ITSCC

Sent by Brian V.

2021-02-24 14:13 (KST/JST)

Forwarded by Kwangwoo to ITSCC

2021-02-24 16:53 (KST/JST)

Is there any chance ITSCC could provide more clarification before tomorrow's meeting? These are my questions/concerns:

1. expectations of physical protections of the HCD are part of the ESR

2. an HCD removed from the operating environment is subject to many types of physical attacks beyond "dumping" a nonvolatile storage memory component (I.e. flash)

The Threat Model this ESR solves has not been clearly articulated

A) must the system be resilient to physical attack when removed from the operating environnent?

B) if a TPM is used to wrap HCD keys, what prevents the HCD from operating normally outside its intended environment?

B.1) if there is an expectation that an HCD must not operate outside of its intended operating environment, how is this accomplished. An example is an Apple iPhone needing to be unlocked by the owner before access to Secure Enclave is granted. Is this envisioned for HCD?

- does an HCD now need to protect against physical attacks such as bus analyzers? Is bus encryption now required?

ITSCC's clarification for the ESRv0.7

Sent by ITSCC (Eunkyoung Yi)

2021-02-24 9:18 PM (KST/JST)

Dear Kwangwoo and HCD iTC members,

First of all, We are grateful for your continuing support.

We know that there were, and still are, a lot of discussion to clearly understand the ESR among members.

As initiator for the creation of the HCD cPP/SD, we would like to share our background and rationale for needs once more.

Note that this is ITSCC's view point on the HCD cPP.

1. Background

Our government has security requirements regarding data stored in the HCD non-volatile storage devices.

They are mainly focused on confidentiality protection of user document data and the HCD critical data by

- either making unavailable of those data (e.g. complete deletion) (of course, we understand the term "complete deletion" may cause technical debate.)

- or encryption.

We consider asset value and access opportunity stored in the both Field-Replaceable and non-Field-Replaceable non-volatile storage devices are same. In our understanding, desolering of non-Field-Replaceable non-volatile storage devices from the HCD itself is not that difficult. Once non-Field-Replaceable non-volatile storage devices are separated from the HCD, their interfaces are exposed to be accessed similar to Field-Replaceable non-volatile storage devices. So, we consider they need the same level of protection.

Our main concern was that existing HCD PPs are partially satisfying our government requirements.

We thought about the feasibility of our government requirements in terms of the Protection Profile development and the HCD technology.

We concluded that the cPP approach is most feasible for us.

2. iTC/cPP whitepaper

* Establishing iTCs and Developing cPPs Version 0.7

This document gives us motivaiton to develop the HCD cPP/SD together with HCD vendors.

It encourages a cPP to include state-of-the-art technology, and CCRA participants will express their national government requirements via ESR developed by the CCDB WG.

Note that the document says that Initially the members of a WG (and hence the authors of an ESR) will be primarily a group of CCRA Participants, and the ESR will describe only national government

requirements from CCRA Participant nations. In future this requirement may be relaxed (Please refer to the page 15).

3. Expectation of the cPP

We really appreciate vendors', schemes', and other experts' support to establish existing PPs.

We expect that the cPP will provide "state-of-the-art technology" than before.

It's been a long time since the latest HCD PP was established, and we believe that the technology is advancing.

4. Issues need further clarification/discussion

As we mentioned in #1, our primary assets are user document data and the HCD critical data. (Please refer to the line #186 of the ESR v0.7)

We all have no doubt that Field-Replaceable non-volatile storage devices shall encrypt those data to provide confidentiality because it is very easy to access data stored in these storage devices once they are taken out of the operational environment.

Regarding non-Field-Replaceable non-volatile storage devices, it is also possible to be taken out of the operational environment due to maintenance or repairs. But attackers need more steps to access these storage devices because it requires physical manipulation such as desoldering. Once these storage devices are separated from the HCD, these are exposed to be accessed similar to Field-Replaceable non-volatile storage devices. So, they need the same level of protection like Field-Replaceable non-volatile storage devices.

This is an attack scenario we assumed. We consider this is basic.

We did not assume sophiscated physical attack such as probing or invasive attacks like the Integrated Circuit evaluation area.

We searched other alternative security mechanisms from existing PPs such as image overwriting or purging. Unfortunately, we concluded that the purging data will not provide the same level of confidentiality protection compared to the encryption because it is invoked by "an authorized administrator" (i.e., human intervention).

To support encryption, the most difficult issue will be the protection of keys and key materials. We expect vendors will suggest "state-of-the-art technology" to address this issue.

5. ESR

If the current version of ESR does not clearly express our intention mentioned above, we are willing to revisit the ESR.

But please understand that we need to consult with schemes who issued the Position Statement on the ESR prior to update it.

We hope our response will help iTC members to agree related issues.

Perspectives on ITSCC's position relative to the ESR

HCD iTC Temporary meeting

2021-02-25 09:00-10:00 AM (KST/JST)

Presented by Tom Benkart

On today's HCD iTC Temporary Meeting to discuss a proposal for an ESR change, I presented my perspectives on ITSCC's position relative to the ESR. This was based on an ad hoc discussion with the participants on the previous day's HCD Network Subgroup call.

- ITSCC support for the iTC/cPP is critical
    - Two sponsoring schemes are required (Korea and Japan)
    - Japan is following Korea's lead on the cPP
    - NIAP has shown no interest in being a sponsor, but vendors want NIAP endorsement of the cPP
- ITSCC has stated that the cPP must provide greater security than the current HCDPP
    - Otherwise they do not consider a new cPP to have sufficient value over HCDPP
- Therefore, the cPP needs to address the stolen scenario in a way that is acceptable to ITSCC
    - As an indication of how ITSCC feels about the scenario, ITSCC considered password-on-boot to be practical
    - Vendors consider password-on-boot to be impractical so favor other solutions
    - ITSCC considers a stored cleartext key to be unacceptable
- The current ESR requires "protection" of the key chain
    - Don't assume stronger solutions are mandated
- One example could be a TPM-like device that provides protection for the key chain
    - Passing a stored value through the TPM on boot for some cryptographic operation is likely to be sufficient
        - The stored value (start of the key chain) is not cleartext since the TPM performs a cryptographic operation
        - The TPM is not just doing a "hardware integrity check"
    - This is only meant to be an example of an acceptable solution, it is not a recommendation
- Many other solutions are acceptable

HCD WG (ITSCC)'s interim response for the "Inquiry about ESR v0.7 (2020-May-08)"

HCD WG (ITSCC)'s response (January 29, 2021)

Shared by Kwangwoo Lee to HCD iTC (Feb, 2, 2021)

Dear Kwangwoo,

Thank you for waiting for our reply.

I'm still discussing this issue with KR government counterpart.

But I would like to share our backgroud and interim outcomes from the discussion.

<Background>

- We consider the a nonvolatile storage device contains sensitive data such as user document data and/or the HCD critiacal data.

- We consider both of use cases i) a Field-replaceable nonvolatile storage device can be taken out of operational environment, and ii) the HCD itself (includes either non-Field-replaceable or Field-replaceable nonvolatile storage device) can be taken out of operational environment.

- When a Field-replaceable nonvolatile storage device or the HCD itself is taken out of operational environment, sensitive data need to be protected from disclosure.

* Note that our intention regarding Assumption "the physical security of the HCD" is strongly related to the opertional environment. When a Field-replaceable nonvolatile storage device or the HCD is taken out of operational environment, they are physically accessible.

- Thus, both of a Field-replaceable and non-Field-replaceable nonvolatile storage device are subject to protection.

<Interim outcomes>

- For the reasons above, if 'purge' is appropriate measure to protection of a non-Field-replaceable nonvolatile storage device contained in the HCD which is taken out of operational environment, then we can consider the same level of security protection could be levied to a Field-replaceable nonvolatile storage device.

- But we do require more security protection requirements such as encryption.

- According to the Reference noted in the email, we assumed that the issue was raised due to the Essential Security Requirements "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".

>> We heard that the iTC was discussing this issue from last year, and we would like to understand "how to protect" keys and key materials. Note that we do understand that "initial" key materials are the most difficult ones, and we do not require any specific mechanism for the protection of "initial" key meterials. **We do expect that vendors suggest the "proper" level of the protection for "initial" key materials.**

I'll continuously contact you to solve this issue.

And, if we need to revisit the ESR to clarify our background and intention, please let us know.

Brian's Email after ITSCC's response

Brian Volkoff (Feb 25, 2021 01:38 AM (KST/JST)

Presented in the HCD iTC Temporary meeting (2/25/2021 9:00AM)

Hi Tom.

Thanks for wrangling cats if you are willing.

Referring to your other email "Thought's about last night's discussion", please see the ITSCC response forwarded below (down beyond my snippet) to some basic questions I had.

I don't think it is a "stolen" scenario as you have in your third bullet, simply removing the HCD from it's operational environment.

> Regarding non-Field-Replaceable non-volatile storage devices, it is also possible to be taken out of the operational environment due to maintenance or repairs. But attackers need more steps to access these storage devices because it requires physical manipulation such as desoldering. Once these storage devices are separated from the HCD, these are exposed to be accessed similar to Field-Replaceable non-volatile storage devices. So, they need the same level of protection like Field-Replaceable non-volatile storage devices.
>
> This is an attack scenario we assumed. We consider this is basic.

I think there are many more "basic" attack scenarios that apply to an HCD removed from its physically secure operating environment, however I'm not proposing we remove any of those physical security expectations.

If the ESR line 189-190

"Note that the initial data of the key chain stored on the nonvolatile storage device without protection do not meet the requirement."

*CANNOT* be changed, and that's my read of ITSCC's comment below:

> If the current version of ESR does not clearly express our intention mentioned above, we are willing to revisit the ESR.

Then I think there is nothing to be done. Let the vendors choose their state-of-the-art technology for meeting lines 189-190, be that a TPM, a physical token/fob that delivers an initial key, typing it in on the front panel, or something else.

Is it necessary to codify the allowed mechanisms? While it might be helpful to vendors to discuss some of the mechanisms available, the state of the art moves forward, and explicitly referencing those mechanisms just guarantees the cPP will need to be refreshed in the future.

-Brian

NIAP's response
for the "Inquiry about ESR v0.7 (2020-May-08)"

NIAP's response (Feb 11, 2021)

Shared by Kwangwoo Lee to HCD iTC (Feb, 16, 2021)

Hello Kwangwoo,

I sincerely apologize for the delay, as it took longer than expected to gather feedback. But I have the below response/comments from the SMEs on our end. If you have any further questions/clarifications, please let me know. Thank you!

It is a priority to include the use case for lost/stolen of field replaceable non-volatile storage containing sensitive data, which would require the encryption of those drives.

It would be preferred to include the use cases of end of life and overrun, which would require encryption of all non-volatile storage containing sensitive data.

Nonvolatile storage is all storage mediums that retain data without power, it would include all the examples that were listed, depending on what it is used for it may not need to be encrypted per the use cases above.

Cleartext storage of CSPs in non-field replaceable would be in line with the lost/stolen field replaceable use case. It would not be in line with the overrun or end of life use cases.