IDS WG Meeting Minutes
Jun 8, 2023

This IDS WG Meeting was started at approximately 3:50 pm ET on June 8, 2023.

Attendees

Jerry Colunga	HP
Jeremy Leber	Lexmark
Ira McDonald	High North
Alan Sukert	
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Latest status on the HCD iTC and the HCD Interpretation Team (HIT)
   - Discussion on how to accelerate development of the HCD Security Guidelines.
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 gave a quick status of the HCD iTC and the HIT
   - As far as the HCD iTC itself, all the meetings over the last couple of the months have basically been status meetings. The last HCD iTC meeting (May 8th) was before the May PWG Face to Face Meetings, so the latest HCD iTC status was presented at the IDS Session on May 18th.
   - Al then went through the current status of the HIT. Al first went through the new Interpretation branch that he set up under the HCD-IT repository and briefly explained the process that the HIT is setting up to create any new v1.0 releases.

     The Interpretation branch will be where the updated HCD cPP and HCD SD files that include fixed for one or more issues written against v1.0 will be placed. The process for creating an update to v1.0 in brief is as follows:

     a) When an Issue gets to the state where it has completed review by the HIT, the Issue has been accepted by the HIT for action by the HIT[1] and the solution has been created to address the issue, a TD (Technical Decision) will be created.

     b) After the TD is created the HIT member responsible for the creating the fix will create in the Working directory in the HCD-IT repository an updated .adoc file of the HCD cPP v1.0 or HCD SD v1.0 as applicable that includes the fix. A file in this context can include fixes for more than one TD.

     c) Once the file containing the fix(es) for one or more TDs is created in the Working branch, a Pull Request will be used to move the file from the Working Branch to the Interpretation Branch. The Pull Request will list all the TDs that are resolve by the file.

        Eventually the files with various TD fixes will be merged into a "super" file of the HCD cPP and/or HCD SD that includes all of the changes up to a certain date or up to a certain TD number that will form an update of the HCD cPP v1.0 or HCD SD v1.0 to be published. A Pull Request will be used to create this "super" file so we can track all of the TDs that go into the update.

[1] If the Issue is not accepted for action by the HIT it will either be rejected or passed on to the full HCD iTC for action. If rejected, no further action by the HIT is necessary; if passed on to the full HCD iTC the HIT will first generate a Technical Recommendation (TR) with the HIT's recommended action for the Issue and send the Issue and the TR to the full HCD iTC for its action

Al pointed out that Pull Requests require a minimum of three reviewers to approve it before it can be committed. One of the reviewers can be the submitter; the submitter of the Pull Request will select two other HIT members to be the reviewers to approve the Pull Request. That way there always will be a review of the file before it is placed in the Interpretation branch

d) When the "super" file for an eventual update of the HCD cPP v1.0 or HCD SD 1.0 is created, it will undergo a review by the HIT and then by full HCD iTC for any non-technical comments. Once the non-technical comments are corrected the "super" file will be moved via a Pull Request approved by the 3 authors to the Master baseline for eventual publishing

To help the process Al created a TD Template .adoc file in GitHub in the Working branch under the HCD-IT repository which he showed at the meeting. The important information that is in the TD Template is:

- Number and Title of the TD (the number is sequential starting with HCD0001)
- Applicable document (HCD cPP or HCD SD) affected
- Issue (with Issue number) that is being addressed by the TD
- Resolution of the Issue (a summary of the fix to address the Issue)
- The actual fix itself - the actual text in the HCD cPP or HCD SD that is added, modified or deleted

- Al then quickly went through the 7 open issues that have been generated against v1.0 of the HCD cPP and SD:
  - HCD-IT #8: Update of Application Notes in SFR FPT_KYP_EXT.1 Needed in HCD cPP v1.0 to Clarify Key Storage Conditions was created as an action from the discussion on HCD-IT #1: The FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption) SFR in HCD cPP v1.0 is inconsistent with TPM 2.0 Architecture specification section "26.6 Sensitive Area Encryption". It was felt that SFR FPT_KYP_EXT.1.1 had several conditions when a key in plain text could be stored, but it was not always clear what these conditions really meant. This issue was to update FPT_KYP_EXT.1 to add an Application Note to better explain what all these conditions for allowing storage of keys in plain text were.
  - As far as the other 6 open issues, HCD-IT #2: Clarification is needed about algorithm verification of Root of Trust in the Test Assurance activities for the Secure Boot SFR is ready to create the TD; the other 5 open issues (including the 4 NIAP certification-related Issues) are still in the "Under Review" state.

  In discussing the NIAP comments, Al mentioned that the Canadian Scheme is also reviewing HCD cPP v1.0 for certification purposes, so it is expected that the Canadian Scheme will also have comments. Based on that Al suspects that the first v1.0 update will most likely be an Errata release to address all of the NIAP and Canadian Scheme comments.

  Along that lines Al asked what the ND iTC used for a naming convention for its Errata release against ND cPP v2.0. Turns out it was "Errata 20180314" – just Errata plus the publication date. Al wasn't sure that was what the HCD iTC should use, but nomenclature conventions for any v1.0 update is an issue that will have to be decided by the full HCD iTC – it is a topic at the next HCD iTC Meeting on Jun 26th.

- Al then showed the group two "projects" he had been working on over the last month. One was a deep look at the changes in ND cPP v3.0 that he felt should be looked at by the HCD iTC for potential inclusion in HCD cPP v1.1 or later releases. These changes included, for example, all of the changes in TLS and DTLS SFRs to implement TLS 1.3, the conformance to the NIAP SSH Package for SSH, and some new SFRs added to ND cPP v3.0 that were not in ND cPP v2.2e. The PDF version of this document can be found at ND cPP v3.0 Differences Considered for HCD cPP Updates.pdf - ONLYOFFICE.

  The other project was a deep look at the changes in the SFRs in CC:2022 Part 2 from the SFRs in CCv3.1R5. This is important since per the Transition Plan all cPPs have to be CC:2022 compliant by 12/31/2025 which isn't that far away, so it is important to know what is new and different in CC:2022. Some of the changes are subtle and important – for example, **FAU_GEN.1.1** in CC3.1R5 (which is the current wording in HCD cPP v1.0) states:

FAU_GEN.1.1 The TSF shall be able to generate audit records of the following auditable events:…

However, in CC:2022 **FAU_GEN.1.1** states:

FAU_GEN.1.1 The TSF shall be able to generate audit data of the following auditable events:..

That is a subtle but important difference. That is just one example. Another is that for Random Number Generation HCD cPP v1.0 used an Extended Component FCS_RNG_EXT.1 (as did the ND cPP and very other cPP). However, CC:2022 has a family of 6 FCS_RNG SFRs as well as a new FCS_RNG.1 SFR for Random Number Generation. The question will be whether in future updates on the HCD cPP do we go to one of the CC:2022 FCS_RBG SFRs or not or di we include the FCS_RNG.1 SFR.

The PDF version of this document can be found at CC2022 Differences Considered for HCD cPP Updates.pdf - ONLYOFFICE.

One last thing – Ira mentioned that at the recent 4th RBG Workshop NIST indicated that it is working with the UK and Germany to get the terminology in the SP 800 series documents closer to their terminology with respect to RBG. He also mentioned that there are plans to change entropy and RBG/RNG requirements to require reseeding n every call.

4. We then had a discussion with Ira on how we could help preparation of the HCD Security Guidelines move forward. Al felt this was important because given the important of standards and best practices in the new National Cybersecurity Strategy this was a golden opportunity for IDS to contribute to that strategy in a meaningful way.

   Ira indicated that what he really needed was editors – people to help him write the guidelines who had knowledge of the security protocols or who had knowledge in application protocols and domain guidelines. Any other help would really not be useful.

   We had a nice discussion of the general state of standards development and the fact that the people who actually develop standards in general are behind the people who develop the products in terms of the technology the standards are being developed for. Ira also mentioned that SOGIS (and basically EU Standards) and NIST/ISO are not in sync with respect to crypto standards, which will make integration efforts of things like EUCC and CC more difficult.

   At the end of the discussion, we left it that Ira will try to do the best he can to develop the guidelines and we will try to find him the right kind of help if it is available.

5. **Actions:** None

Next Steps

- The next IDS WG Meeting will be Jun 22, 2023 at 3:00P ET / 12:00N PT. Main topics will be the latest status of the HCD iTC and HIT and likely a special topic on a TBD as of now topic.