IDS Face-to-Face Minutes
November 15, 2023

Meeting was called to order at approximately 10:55 am ET November 15, 2023.

Attendees –

Matt Glockner	Lexmark
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Michael Rhines	Qualcomm
Anthony Suarez	Kyocera
Alan Sukert	
Michael Sweet	Lakeside Robotics
Bill Wagner	TIC
Uli Wehner	Ricoh
Steve Young	Canon

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2023-11-15-IDS-F2F v1.pdf.

- Minute Taker
  - Alan Sukert taking the minutes.

2. Agenda:
   - Introductions, Agenda Review
   - Discuss status of the Hardcopy Device international Technical Community (HCD iTC), the HCD Interpretation Team (HIT and plans for future HCD collaborative Protection Profile (cPP) / HCD Supporting Document (SD) releases since the publishing of v1.0
   - Debrief on Fall 2023 CCUF Workshop and ICCC 2023
   - ICAM 2023 Presentation
   - HCD Security Guidelines v1.0 Status
   - Trusted Computing Group (TCG) / Internet Engineering Task Force (IETF) Liaison Reports
   - Wrap-Up / Next Steps
3. Alan went quickly through the PWG Antitrust, Intellectual Property and Patent policies.
4. Alan went through the current status of the HCD iTC, the HIT and potential content of the next releases of the HCD cPP and HCD SD. Most of the HCD iTC and HIT update presented at this meeting was taken from the HCD iTC Status presentation given at the 2023 International Common Criteria Conference (ICCC 2023) held in Washington DC on Oct 31 – Nov 2, 2023.

   Some of the key points from the HCD iTC Status discussion were:

   - Slides 7 and 8 provided a history of how the HCD cPP v1.0 and HCD SD v1.0 came to be in terms of the PPs that led to the HCD cPP and HCD SD.

     Al indicated that in Slide 7 he was involved in all of the WGs and Technical Committees that created the two 2600 PPs, the HCD PP and eventually the HCD cPP/SD. Al also noted on Slide 7 the role IDS played in the creation of the HCD cPP/SD.

     Slide 8 was more of a chronological history of when the various HCD-related PPs were published.

- Slide 9 showed where the 546+ comments against the HCD cPP and HCD SD in creating v1.0 were generated in terms of releases sorted by document. Note – SPD is the Security Problem Definition which is part of the cPP but is initially delivered as a standalone document.
- Slides 10, 12, and 13 showed how the HCD iTC is currently listed on the Common Criteria portal
- Slide 11 is a high-level list of what the HCD iTC has worked on.
- The HIT Status presented at ICCC 2023 was:
  - The HIT currently has 12 members. The current makeup of the HIT is six from HCD vendors, two from Evaluation Labs, one Consultant (AL), and three from Schemes (1 from NIAP and 2 from the Canadian Scheme).
  - HIT procedures v1.0 were finalized and approved by the HIT members and the HD iTC, and the necessary infrastructure was set up by Al. The HIT will be using GitHub for the end-to-end process of documenting Requests for Interpretation (RfIs) and for creating and tracking the changes to HCD cPP v1.0 and HCD SD v1.0 for approved RFIs. To help Al created a new HCD-IT repository and a new Integration baseline where all the HIT approved changes will be placed and used to create any new v1.0 related releases.

    However, in attempting to try as a group to process one of the HIT issues we encountered several issues that required multiple changes to the documented HIT procedures. For example, the Interpretation baseline was determined to be unnecessary; baselines are now created of the main HCD-IT Template branch. The new procedures are being worked out in real time or offline, and the HIT Procedures will have to be updated to reflect the new processed being developed.
  - One of the first things the HIT did was determine its scope; i.e., what issues should the HIT work on ad what issues should be elevated to the full iTC. The HIT agreed that the HIT should be able to resolve any issue that involves clarification of existing requirements in either the HCD cPP v1.0 or HCD SD v1.0

    For any issue that involves new content to either the HCD cPP or HCD SD, the HIT should make a recommendation to the full HCD iTC, which would then have the responsibility to resolve the issue
  - Slide 16 was a graphic of the HIT Process. Al just went through it very quickly since it is a bit of an “eye chart”
  - Slide 17 provided some statistics on the 12 Issues that had been generated against the HCD cPP and HCD SD v1.0at the time of this meeting. The key stats were:
    - 16 Issues had Editorial comments; 13 Issues had technical comments
    - 22 comments were against the HCD cPP; 9 comments were against the HCD SD
  - The HIT has had 10 meetings at the time of this presentation. During these 10 meetings the HIT processed the following 21 Issues:

Issue #	Issue	Status
HCD-IT #1	CFB is the only AES mode allowed by the TPM 2.0 specification but it is not included as n allowable mode in SFR FCS_COP.1/KeyEnc	Potential Solution being reviewed by HIT

IDS Face-to-Face Minutes
November 15, 2023

Issue #	Issue	Status
HCD-IT #2	In HCD SD Section 2.6.1 FPT_SBT_EXT.1 Extended: Secure Boot, 2.6.1.3 Tests, need clarification that the algorithm verification for Root of Trust should be avoided	Solution developed; Technical Decision being prepared
HCD-IT #3	Extraneous "selection" in SFR FCS_CKM.4 Cryptographic key destruction in HCD cPP v1.0	This issue was closed because it duplicated another comment
HCD-IT #4 – HCD-IT #7	These four issues were a set of four comments from NIAP stating areas such as improperly defined Extended Component Definitions and bolding of the selection prompt where the HCD cPP did not follow the conventions stated in Section 5.1	These issues cited by NIAP have mostly been fixed. Remaining concern is how to address the comment on Extended Components
HCD-IT #8	Requested that the Application Notes in SFR FPT_KYP_EXT.1 be modified to more clearly explain what each of the conditions for key storage in that SFR mean	This issue is linked to Issue HCD-IT #11 and will be fixed jointly with that issue
HCD-IT #9	This issue is about the test cases for SFR FDP_DSK_EXT.1 in the HCD SD requiring an “operational TSFI” (i.e., an external human interface such as a web interface) when user and confidential data stored on nonvolatile data on the HCD is only accessed by the OS and required no human interface	Working on a proposed solution to be presented to the HIT at our next meeting
HCD-IT #10	This issue is for the Security Objective an O.KEY_MATERIAL being mapped to a Conditionally Mandatory SFR FPT_KYP_EXT.1 when it should be mapped to a Mandatory SFR, because protection of keys and key material should be a mandatory security objective	The solution for this issue is known and is being worked jointly by the HIT at a HIT meeting
HCD-IT #11	This issue deals with FCS_CKM.4 and whether encrypted keys are within the scope of key destruction. The real issue, though, is the fact that FCS_CKM_EXT.1 states that only plaintext keys and key material must be destroyed, whereas other cPPs require all keys and key material must be destroyed	Resolution of this issue is on hold while we determine why the HCD cPP only required plaintext keys to be destroyed; HIT divided on this issue

Issue #	Issue	Status
HCD-IT #12	This issue is from the Canadian Scheme and was for the fact that three threats - T.TSF_FAILURE. T.UNAUTHORIZED_UPDATE, and T.WEAK_CRYPTO did not have the required asset information in their definition	This issue is being worked by the HCD cPP Editor and Canadian Scheme Representative
HCD-IT #13	This issue stated that the title of SFR FDP_DSK_EXT.1 - Protection of Data on Disk – was misleading as it might lead someone to assume it only applied to HCDs that had a hard disk drive.	Solution is to change title so it is clear this SFR applies to any HCD that stores data in Nonvolatile Storage
HCD-IT #14	This issue is a simple issue where the sections where the SFRs FIA_AFL.1 and FCS_CKM.1/AKG reside are different between the HCD cPP and the HCD SD	Issue has been assigned to a HIT member to resolve
HCD-IT #15	This issue is a case where the title of the SFR FCS_COP.1/CMAC is correct where it is defined in Section A,,3, but is incorrect when FCS_COP.1/CMAC is included in a dependency list for another SFR	Issue has been assigned to a HIT member to resolve
HCD-IT #16	This issue documents three comments – two editorial and one technical – from the required CCMB review of the HCD SD v1.0	The CCMB comments are under review by the HIT for assignment to a HIT member(s) to analyze and resolve
HCD-IT #17	This issue documents three comments – two editorial and one technical – from the required CCMB review of the HCD SD v1.0	This issue was closed because it duplicated of Issue HCD-IT #16
HCD-IT #18	The issue is that the TSS Assurance Activity for SFR FCS_CKM.1/SKG Cryptographic key generation (Symmetric Keys) has to clarify a disconnect how the TOE obtains a symmetric key through direct generation from a random bit generator between the two standards referenced in the SFR.	Issue has been assigned to a HIT member to resolve
HCD-IT #19	This issue is whether Tests 1 and 2 for SFR FCS_CKM.4 Cryptographic key destruction apply to only volatile memory	Issue has been assigned to a HIT member to resolve. Solution appears to be a simple one to implement

Issue #	Issue	Status
HCD-IT #20	This issue is whether for Test 2 for SFR FDP_DSK_EXT.1 Protection of Data on Disk decryption of the data is not required if the data is encrypted by "another key"	Issue is being reconsidered as to whether it is a valid issue
HCD-IT #21	This issue is to clarify when Tests 3 and 4 for SFR FDP_DSK_EXT.1 are required to be run	Concern is whether Tests 3 and 4 are "out of scope" for this SFR and why they were added in the first place

- As far as HIT-related releases, there will definitely need to be an Errata release for HCD cPP v1.0 and HCD SD v1.0 address the NIAP and Canadian Scheme evaluation comments and the CCDB comments against the HCD SD.

  The Errata may also include fixes for one or more of the open issues (at the time of release) against HCD cPP v1.0 and HCD SD v1.0, although as of now the plan is for the Errata to strictly include just the fixes listed above.

  There may be additional standalone HCD cPP or HCD SD v1.0.x releases after the initial Errata release. If so and how many of these releases will occur likely depend on the comments we get from: the review of the HCD cPP from the other Schemes and the current Lexmark and Japan certification and future certifications against HCD cPP v1.0 or HCD SD v1.0 from the applicable Evaluation Lab or applicable Scheme. But as of no the HIT is not planning any additional v1.0.x releases.

- Kwangwoo Lee, who presented the HCD iTC Status slides at ICCC 2023, included the following lessons learned in his presentation:
  - It took much longer than we expected or planned to create or update the PP, so don't expect a new or update PP to be developed quickly either.
  - The Schemes that sponsor an PP or cPP need to commit the necessary resources support from the beginning to the TC/iTC to address questions/concerns/issues as they come up.
  - If you pull in requirements into a PP from other PPs or cPPs, ensure these requirements are assessed to make sure they apply to the PP they are being inserted into or modify them so they apply.
  - Have a plan and process in place from the beginning for updating a PP once it is approved, because updates will be needed.
  - Make sure you get the involvement from vendors, consultants, and CCTLs as well as the Schemes in developing the requirements that are to go into a PP.
  - Make sure assurance activities are consistent with their corresponding requirements and can be performed by vendors and CCTLs
  - Have a process in place from the beginning to obtain interpretations and questions on requirements or assurance activities as the PP is being created, and more importantly, as the PP is being implemented.

- The "Post v1,0 Release Plan" slide was changed this time to reflect that there are now five key issues that will likely drive what content will go into the next and future releases of the HCD cPP and HCD SD, These five issues, in order of priority from high to low, are:
  - CCDB Specification of Functional Requirements for Cryptography
  - CC:2022 Compliance
  - Syncing with ND cPP / SD v3.0
  - CNSA 2.0
  - Mutual Recognition with EUCC

Al indicated that some of the presentations in the special topics will get into details on these five topics.

- Regarding CNSA 2.0, Al just pointed to the chart below that showed the CNSA 2.0 algorithms:

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels SHA256/192 recommended
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels

- Al then listed, based on the above discussions, his view of the likely potential content for the next update to the HCD cPP/SD, whe6her it be a v1.1 or v2.0:
  - Incorporate SFRs from the CCDB Specification of Functional Requirements for Cryptography once it is published and we get a transition plan
  - Updates for the relevant changes in CC:2022
  - Update for the relevant changes in ND cPP v3.0e
  - Initial CNSA 2.0 Implementation – Removal of SHA-1
  - Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
  - NC iTC and NIAP are developing competing TLS Packages
  - NIAP wants to standardize on a common TLS Package
  - May not come in V1.1 timeframe
  - Incorporate the NIAP Functional Package for SSH so can claim conformance to it
  - Inclusion of AVA_VAN and ALC_FLR.*
  - Sync with new EUCC
  - Initial implementation of CNSA 2.0 algorithms
  - Changes due to any approved RfIs (Issues) to HCD cPP/SD v1.0
  - Inclusion of NTP

  - Changes due to requests from JISEC, ITSCC, NIAP, Canada and possible other Schemes due to on-going certifications against HCD cPP/SD v1.0
- The list of changes that could go in future releases likely beyond the next update to the HCD cPP/SD is essentially the same as it was for the August 20th IDS Face-to-Face Meeting, but some new items were added (the items in bold are the ones AL feels should be the higher priority items on the list):
  - **Full implementation of CNSA 2.0**
  - **Support for Cloud Printing**
  - **Incorporate NIAP Functional Package for X.509 when it becomes available**
  - **Support for post quantum and other new crypto algorithms**
  - **Any other new NIAP Packages**
  - **Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, and NIAP TDs**
  - **Updates to Address 3D printing and the Digital Thread to Additive Manufacturing**
  - **Support for Artificial Intelligence**
  - **Support for Wi-Fi**
  - **Any new CCDB Crypto WG or CCUF Crypto WG Packages or Specifications**
  - Support for Security Information and Event Monitoring (SIEM) and related systems
  - Support for SNMPv3
  - Support for NFC
  - Updates based on new technologies, customer requests or government mandates
  - Syncing with newer updates to ND and FDE cPPs/SDs
- Key next steps for the HCD iTC are:
  - Continue HIT activities for maintaining HCD cPP/SD v1.0 and issue the necessary TDs/TRs and Errata to address all documented RfIs
  - Get HCD cPP/SD v1.0 certified by June 30, 2024
  - Get HCD cPP/SD v1.0e published be the end of 2023
  - Develop an HCD cPP/HCD SD release plan for future versions of the HCD cPP and HCD SD
  - Determine the content for and then create the next HCD cPP/SD version after HCD cPP/SD v1.0e
  - Fully engage the HCD iTC to work on the next update to the HCD cPP and HCD SD
  - Engage in long-range planning to determine what content will be needed in the HCD cPP/SD in the 3-5 year range and beyond
- The set of "Lessons Learned" for this meeting are::
  - The toughest thing to do is to resist the urge to add more into a release than you can reasonably address. Sometimes "you just have to get the release out even if it doesn't contain everything you want "
  - This may sound confusing, but I've learned that in trying to develop PPs sometimes "the best you can do is the best you can do", and that's OK
  - One regret in developing the HCD PP and now the HCD cPP/SD is that we didn't celebrate enough or appreciate enough as a team what we had accomplished. We (I mean the global "we') need to celebrate our victories more because they are so few and far between

5. Al then went through his two special topics. The first was a debrief on the Fall 2023 CCUF Workshop and ICCC 2023. Al decided to do this a different way than normal. Since the slides from both events are in PDF format, Al selected a few representative talks and will go through the PDF versions of the presentations. The presentations selected were:

    - EUCC Implementing Regulation
    - 2023 CC Statistics Report
    - An Update on EUCC
    - 2023 NIAP Update
    - CC 2022 IN ACTION: SECURING CRYPTOGRAPHIC PROTOCOLS AND THEIR IMPLEMENTATIONS
    - Post Quantum Cryptography: A Quintessential Quagmire
    - CCDB Crypto Working Group Status
    - Network Device iTC Update
    - Application of Common Criteria in Cooperative Intelligent Transportation Systems

    EUCC Implementing Regulation (IR)

    Al indicated this was the “800 lb. gorilla” throughout both the CCUF Workshop and ICCC 2023. Essentially what happened was that ENISA issued its final version if the EUCC IR just before the CCUF Workshop with comments due by October 31st. Some of the statements in the final draft if the EUCC IR were so controversial that the first fay of the CCUF Workshop was devoted entirely to preparing comments against the draft EUCC IR.

    There were a lot of issues against the draft EUCC IR, but three main issues stood out:

    a. Mutual Recognition Agreements with Third Countries

        The draft EU IR states that “Third countries willing to certify their products in accordance with this Regulation, and who wish to have such certification recognised within the Union, shall conclude a (separate) mutual recognition agreement with the Union”

        This meant that every CCRA nation would have to negotiate a separate recognition agreement with the EU. The CCRA wants a single mutual recognition agreement between the EU and the entire CCRA as a group, not separate mutual agreements with each CCRA member nation

        Another side effect of tis is that each CCRA nation would have to have separate CC certifications with each EU Member Nation

    b. Transition to the EUCC

        The draft EU IR states that “This Regulation shall apply 12 months after its entry into force. The requirements of Chapter IV (Conformity Assessment Bodies) and Annex III (Content of a certification report) do not require a transition period and should therefore apply as of the entry into force of this Regulation”

        NIAP and others feel that 1 year is way too short of a time to handle transition to EUCC

    c. Continued EU association with the CCRA

        This is the #1 issue that even blind-sided the EU Member Nations.

        The draft EU IR stated that “This Regulation sets out conditions for mutual recognition agreements with third countries. Such mutual recognition agreements should replace similar agreements currently in place, such as SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and Common Criteria Recognition Arrangement (CCRA).

        In a number of Member States Common Criteria certificates are issued under national schemes using mutual recognition rules established in SOG-IS MRA and CCRA. This Regulation should provide an indicative list of existing national schemes which will cease to produce effects. **Member States should end their participation in the CCRA in the areas covered by this Regulation**."

No one is happy with this new policy that got put in without anyone's knowledge. I talked to CCRA delegates from Norway and Sweden at the ICCC and they were not happy about this, to put it mildly.

Basically, the CCMB and CCRA as well as the EU Member Nations are fighting these changes as well as other issues with the IR

2023 CC Statistics Report

This was one of the few presentations for which there were slides. Thus was a very interesting presentation on statistics governing certifications performed the first 9 months of 2023. Some of the more interesting findings were:

- 310 products were CC certified in the first 9 months of 2023, with a projection of 413 for the entire year
- The three top certifying schemes in 2023 so far, in order, are France, Netherlands, and the US. Over the past five years the top three certifying schemes, in order, are France, US, and Netherlands.
- In terms of Assurance Levels, 37% of the certifications were PP certifications. The next highest were EAL4 at 24% followed by EAL5 at 16%.
- MFD certifications made up 12% of all certifications and ND certifications made up 78% of all cPP certifications (remember – until Oct 31, 2022 all MFD certifications were against the HCD PP)
- Hardcopy Devices PP was the top non-CPP certified so far in 2023.

An Update on EUCC

The presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/Update on the EUCC.pdf

This presentation focused on the main items in the EUCC IR. Some of the key points were:

- Most provisions in the IR are in line with the ENISA candidate scheme requirements such as :
  - Assurance levels mapping with AVA_VANlevels
  - Commitment of applicants
  - Duration of certificates
  - Conditions of mutual recognition (Al questioned this one)
- Some new provisions introduced such as:
  - Adoption and use of PPs
  - Transition period
  - CCRA participation

  The two last bullets are key issues as stated above

  The slide stated "We Anticipate Discussions". I don't think they expected the level of discussions they are getting
- Additional points for discussion
  - Scope of EUCC vs. National Schemes
  - ALC_FLR vs. transition of existing certificates
  - Vulnerability management and disclosure based on AHWG pilots

The presentation then went on to talk about the evolution of the EUCC. Al mostly just quickly ran through that portion of the presentation.

2023 NIAP Update

The presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/NIAP Update.pdf.

The 2023 NIAP Update was dome by Jon Rolff, Director of NIAP. The key points that Al took from the presentation were:

- NIAP in FY 23 (Oct 1, 2022 – Sep 30, 2023) did 77 Product Evaluations (up slightly from FY 22); had 55 PPs, and 31 Nation Partnerships. 47% of the product evaluations were against the ND cPP.
- NIAP's PP update strategy will focus on:
  - PP Dependencies (something the HCD iTC has to focus on for v1.1)
  - CC:2022 impact
  - CNSA 2.0 Deadline
- There was a nice "eye chart" about the interconnection of PPs that should be looked at in a larger Zoom mode
- The key slides in the NIAP presentation were the PP Roadmap and Technology Roadmap. The PP Roadmaps:
  - Priorities
    - CC:2022 Conversion of various Groups
    - CNSA 2.0 – LMS/XMSS and then CRYSTALS Kyber/Dilithium
  - Key new PP is the X.509 Package thar will have to be included in the HCD cPP when made available
  - cPP Endorsement Reviews – includes the HCD cPP
- The Technology Focus is in the following areas:
  - CNSA Suite 2.0
  - Cloud Security – an area that Al thinks the HCD iTC should pursue in the future as indicated above
  - Multi-factor authentication – something that should be added to the list of items to consider in future HCD CPP/SD releases
  - Zero Trust – a topic the HCD iTC needs to learn more about since it is one the new "hot topics" in security
  - Vulnerability tracking
  - Software Bills of Materials (SBOMs) – SBOMs is a huge NIAP initiative now
  - Equivalency
  - Entropy Update – maybe another topic that should be added to the list of items to consider in future HCD CPP/SD releases
- Finally, Jon did mention the maintain mutual recognition with the EU as an area of concern

CC 2022 IN ACTION: SECURING CRYPTOGRAPHIC PROTOCOLS AND THEIR IMPLEMENTATIONS

This presentation was about CC:2022 and, specifically the new Parts IV and V of CC:2022.. The presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/CC 2022 in Action - Securing Cryptographic Protocols and Their Implementations.pdf.

Slide 3 of the presentation is a good pictorial mapping between the 3 Parts of CC3.1R5 and the 5 Parts of CC:2022.

Slide 5 was a high-level overview of CC:2022 Part IV, Framework for the Specification of Evaluation Activities and Methods.

The rest of the presentation was a discussion of ISO/IEC 29128 Information security, Cybersecurity and Privacy Protection, Verification of Cryptographic Protocols:- Part 1: Framework; Part 2: Evaluation Methods and Activities for Cryptographic Protocols; and Part 3: Evaluation Methods and Activities for Protocol Implementation Verification (Note – Parts 2 and 3 are Working Drafts) and related the three parts back to Part IV of CC;2022. Al briefly went through the slides with no specific points stressed.

Post Quantum Cryptography: A Quintessential Quagmire

The presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/M23b-DowneyM-Updated.pdf.

This presentation was about plans for implementation of CNSA 2.0.

The 3rd slide was a list of the CNSA 2.0 algorithms which were discussed at a previous IDS WG Meeting and are shown in Slide 94.

Slide 4 was an important slide as it gave a graphical look at the timeline for planned CNSA implementation. The key high-level date that impacts the HCD iTC is:

- CNSA 2.0 algorithms for software /firmware signing should be implemented in CPPs/PPs by the end of 2030, but initial implementation should start by the end of 2025. Thus, means initial implementation of the LMS and XMSS algorithms should be in the HCD cPP by the end of 2025.

  Ira pointed out that, of course, is contingent on NIAP having CAVP or CVP for either of these algorithms ready by that date, and right now the chances of that happening are nearly zero/

The general process for NIAP implementation of CNSA 2.0 (the details are in the presentation) is:

a. NIST publishes the algorithm standard
b. NIST adds support for the algorithm to CAVP (Cryptographic Algorithm Validation Program)
c. NIAP updates the relevant PPs to include the newly-standardize algorithm as the preferred configuration option
d. New equipment must meet the updated PP requirements to be validated; already validated equipment must meet the updated PP requirements when it is due for its next update to remain compliant
e. After some time, non-CNSA 2.0 algorithms will be removed as options for PPs

The presentation noted that any current planned timeline for implementing CNSA 2.0 has been paused due to “implementation concerns”.

The final slide showed current effort to support CNSA 2.0. The key one from an HCD iTC perspective was “removal of older algorithms like SHA-1”; that is something as said above that the HCD iTC should do in the next HCD cPP/SD release

CCDB Crypto Working Group Status

The presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/CCDB Crypto Working Group Status.pdf.

This presentation from the CCDP Crypto Working Group was about the status of what they call the “SFR Catalog”, but what was presented to the CC community as the “Specification of Functional Requirements for Cryptography”.

The goal of the “SFR catalog” was to “harmonize the specification and evaluation of crypto mechanisms in collaborative Protection Profiles (cPPs) and product evaluations within the CCRA”.

The presentation listed all the new and modified crypto SFRs that are included in the catalogue, with an example (FCS_CKM.2) of how they are presented. The details of the specific SFRs included are in the presentation. The presentation also included a slide with some brief guidelines on how to use the catalog.

What Al found important was the next steps:

- Finalize review of comments and provide response
- Publish the revised catalogue after CCDB approval in spring 2024
- Develop evaluation methodology for the SFRs from the catalogue
- Extend the catalogue, e.g., with filled out operations for FTP_PRO
- Post-quantum cryptography

Network Device iTC Update

The presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/Network_Device_iTC_Update_CCUF_Oct2023.pdf.

Much of this presentation was general information about the Nerwrk Device iTC. What was important from an HCD iTC perspective were the following:

- NDcPPv3.to be published November 2023
- NDcPPv3.0e major changes:
  - Added TLS / DTLS v1.3
  - Removed TLS v1.1 / DTLS 1.0
  - CCMB comment resolution from their review of the Supporting Document v2.2 Added ALC_FLR as an optional additional assurance component to better align with EUCC SSH SFRs removed
  - NIAP's SSH Functional Package now required for SSH
  - Updated references to standards (RFCs and NIST SPs)
  - Removed support for published hash as a means of providing software integrity Address formatting issues and comments
  - PP Consistency Review
- NDcPP Roadmap
  - Publish NDcPPv3.0e (Nov. 2023)
  - Update FW module (ver. 1.5)
  - CNSA Suite 2.0
  - CC:2022

Application of Common Criteria in Cooperative Intelligent Transportation Systems

The presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/L31a-LirasDS-UPDATED.pdf.

Al indicated he selected this particular presentation specifically for Ira because he is involved in security standards for automobiles and Al thought he might be interested in the topic.

Al hadn't seen this presentation and wasn't familiar with the topic, so he just quickly went through the slides.

Ira was familiar with the C-ITS Stations and the CPOC Protocol mention in the presentation, and he was appreciative of the presentation and planned to pass it on to his colleagues.

6. Al then went through the presentation he gave to the ASTM International Conference on Advanced Manufacturing (ICAM) 2023.

   Because of time limitations Al skipped the first six slides that gave a brief overview of what the Common Criteria is and focused on the rest of the presentation that dealt with how CC could be applied to the Digital Thread for Additive Manufacturing (which is 3-D Printing),.

   The key points in the rest of the presentation were:

   - In the picture of the Digital Thread for Additive Manufacturing, the key for this presentation is to consider the picture as broken into two halves – the left half which is the computer that stored the CAD file and build simulations that mode the object that is to be printed, and the right half that is the actual 3-D printer that prints the actual object.
   - Slide 73 was a summary of the five parts of CC:2022. The message was that some of the new content in CC:2022, especially in Parts IV and V, provide methods that could make it easier to develop a PP for the Digital Thread.
   - One of the new concepts in CC:2022 is that of a “composite Target of Evaluation (TOE)”, which is defined as “comprising solely two or more separately identified components with a security relationship between their TOE security functionality (TSFs)” The idea is that this could allow the definition of the Digital Thread as a composite TOE between the 3D Printer (the right side of the Digital Thread picture) and the computer containing the CAD file and build simulations (the left side of the Digital Thread picture) and then develop a Protection Profile for the composite TOE based on the composite evaluation techniques in CC:2022 Part 5
   - The key concepts in CC:2022 that could help define a PP for the digital thread are that of a PP-Configuration and a PP-module. As Slide 75 stated, the idea would be that you:
     - Define a base configuration (the full Digital Thread in this case without considerations for the 3D Printer and Computer with the CAD file) with a Security Problem Definition and a set of applicable functional and assurance requirements to form a PP called the base PP
     - The 3D Printer and Computer with the CAD file/Build Simulation, etc. would each be treated as a separate PP-Module, each with its own Security Problem Definition and set of functional and Assurance requirements in the form of PP
     - The sum of the base PP and the PPs for the two PP-Modules would comprise the PP-Configuration
   - CC:2022 also includes some new and modified SFRs, especially in the FCO (crypto) class dealing with Random bit generation and Random number generation, Cryptographic key derivation and Timing and event of cryptographic key destruction and other new SFRs in the areas of Trusted channel protection, TSF initialization and Stored data confidentiality
   - In Slide 76, it was indicated that CC:2022 Part 4 defines a general model for defining a unique evaluation method and evaluation activities not in Parts 3 or 5 that can apply to an PP, PP-Module or PP-Configuration. This could be used to develop evaluation methods and activities that reflect the unique aspects of the Digital Thread
   - Based on these new concepts and SFRs introduced in CC:2022, Al felt that the next steps should be:
     - Identify one or more National Bodies to sponsor and then create a 3D Printing Technical Community (TC) to develop a Protection Profile (PP) for the Digital Thread (or separately for 3D Printers)
     - Determine who the customers/audience for this TC would be
     - Determine what are the following for the Digital Thread (or for 3D printers alone):
     - Threats
       - Key assumptions that must be upheld

        - Organizational Security Policies that must be upheld
        - Security Objectives
    - Generate an approved Digital Thread/3D Printing Protection Profile. Our initial thought is that it could be a PP-Module based off of the HCD collaborative PP that is currently being developed for publication in 4Q 2022
    - Recognize this will take a minimum of two – four years to complete
    - Once we have a Digital Thread/3D Printing PP we can start certifying 3D Printers or the entire Digital Thread against that PP

7. Ira indicated that nothing had been done on the HCD Security Guidelines since the last IDS Face-to-Face Meeting, so this topic was skipped for this session..
8. When it came time for Ira to present his Liaison report on current standards developments for the Trusted Computing Group (TCG) and Internet Engineering Task Force (IETF), we were out of time for the IDS session. Ira agreed to present his Liaison Report .at a future IDS WG Meeting. Ira did have two points he wanted to make before the meeting ended
    - The industry will not be able to do Post-Quantum Computing without hybrid key exchange
    - BSI is mandating stateless hash-based digital signatures in certificates by 2026/2027. That is something the HCD iTC is going to have to follow.
9. **Wrap Up**
    - The next IDS Working Group Meeting will be on November 30, 2023. Main topics of the meeting will be updated status of the HCD iTC and HIT, debrief of this IDS November Face-to-Face, and possibly a special topic that currently is TBD.
    - Next IDS Face-to-Face Meeting will be during the February 202 PWG Virtual Face-to-Face Meeting February 13-15, 2024 (likely on Feb 15, 2024).

    Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 2:00 PM ET on November 15, 2023.