IDS Face-to-Face Minutes
November 4, 2021

Meeting was called to order at approximately 10:00 am ET November 4, 2021.

Attendees –

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
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/2021-11-04-IDS-F2F.pdf.

- Minute Taker
  - Alan Sukert taking the minutes

2. Agenda:
   - Introductions, Agenda Review
   - Discuss results of latest Hardcopy Device international Technical Community (HCD iTC) Meetings and HCD collaborative Protection Profile (cPP)/Supporting Document (SD) v1.0 status
   - EUCC (ENISA Cryptographic Certification) / ISO Updates
   - Wrap-Up / Next Steps
3. Went quickly through the PWG Antitrust and Intellectual Property policies.
4. Went through the current status of the HCD iTC and its efforts to develop HCD cPP v1.0 and HCD SD v1.0. Some of the key points from this discussion were:
   - The HCD iTC issued the 1st Public Drafts of both the HCD cPP (on 8/30/21) and the HCD SD (on 10/13/21).
   - There have been 85 total comments submitted against the 1st Public Draft of the HCD cPP. 64 of the 85 comments have been reviewed and addressed by the HCD iTC to date. The tally of these 64 comments addressed is:
     - 58 comments were 'Accepted' to be fixed for the 1st Public Draft of the HCD cPP
     - 0 comments were 'Accepted in Principle' to be fixed eventually in the HCD cPP by the time HCD cPP v1.0 is published
     - 4 comments were 'Deferred' to be addressed a later time, possibly in a later version of the HCD cPP
     - 2 comments were either not accepted or rejected
   - Similarly, there have been 4 total comments submitted against the 1st Public Draft of the HCD SD to date. None of the 4 comments have been reviewed by the HCD iTC to date:

- The HCD iTC was finally able to rework JBMIA's proposal for the FPT_KYP_EXT.1 Protection of Key and Key Material SFR after the sixth attempt to completely revise the text to make it in line with the FPT_KYP_EXT SFR from the Full Drive Encryption Encryption Engine (FDE EE) cPP and a revised Application Note and with the Assurance Activities from the FDE EE SD,

- One issue that came up at a recent HCD iTC meeting dealt with a requirement in the Secure Boot SFR FPT_SBT_EXT.1 that the Root of Trust is "implemented in immutable memory". One comment to the HCD cPP 1st Public Draft was to add to this requirement to explicitly include hardware Roots of Trust because current it only addressed software Roots of Trust. Ira pointed out that according to both ISO and NIST there are only hardware-based Roots of Trust, so the HCD iTC shouldn't be talking about software-based ones at all anyway. Al stated he would bring this point up to the HCD iTC at its next meeting.

- The biggest issue facing the HCD iTC right now has to do with how to handle Cryptographic Erase (CE). The background for this issue is that if an HCD has any type of nonvolatile storage device such as a hard disk drive, in processing a print, copy, scan and fax job the device will leave a temporary copy of that job permanently on the drive which could be retrieved from the drive if it was somehow removed from the device. So, the HCD cPP needs to address how user, job and confidential data stored on the device like these temporary image files can be made irretrievable.

  The process of making this image data irretrievable is called sanitization. The US Government Standard governing sanitization is NIST SP 800-88r1. For disk drives there are two main methods for sanitization outside of destruction of the drive – Image Overwrite and Cryptographic Erase. HCDs generally use the "Image Overwrite" mechanism for sanitization since most HCDs have standard nonvolatile drives. However, for HCDs with Solid State Drives or self-encrypting nonvolatile storage devices or Self-Encrypting Drives (SEDs) the "Image Overwrite" mechanism will not work because you can't point to the exact location where the image files are stored – you have to use Cryptographic Erase where the encryption key for the image file is destroyed.

  JISEC (the Japanese Scheme) wants the Image Overwrite discussions in the Security Problem Definition and in the FDP_RIP.1/Overwrite SFR to only include the "Image Overwrite" mechanism. JISEC feels Cryptographic Erase is covered by the two Key Destruction SFRs (FCS_CKM.4 & FCS_CKM_EXT.4) already in the HCD cPP. Some HCD iTC members disagree and feel Cryptographic Erase is not adequately covered by the two Key Destruction SFRs

  ITSCC (the Korean Scheme) feels Image Overwrite and Cryptographic Erase are two different things and agrees with JISEC's position. ITSCC's suggestion is that the HCD iTC create additional optional requirements specifically for Cryptographic Erase. To address this issue the HCD iTC created a subgroup to address the Cryptographic Erase requirements which had it's first meeting on 11/3/21.

- When discussing some of the remaining issues that need to be addressed by the HCD iTC, one of the issues was whether the HCD cPP v1.0 would include removal of support for Cipher suites with RSA Key Generation with keys < 2048 bits as required by NIST SP 800-56B and NIST SP 800-131A. Ira pointed out that in 2022 NIST is going to require that Cipher suites with RSA Key Generation will require keys >= 3072 bits, so maybe some type of App Note stating that fact should be included in the HCD cPP.

- Al indicated that in terms of new content, a new factor that may impact what goes into HCD cPP v1.0 is the new ENISA Cryptographic Certification (EUCC) which he will talk about in much more detail later.

- Al provided a status update on the schedule as follows:
  - 1st Public Draft Review for HCD cPP: Completed on 10/8
  - 1st Public Draft Review for HCD cPP: Scheduled for Completion on 11/15

- 2nd Public Draft Submitted for Review: Planned for 12/1 on Master Schedule; Al thinks it will more likely be around the beginning of January 2022
- Final Draft Submitted for Review: Planned for 3/14/22 on Master Schedule; Al thinks it will be closer to mid-end April 2022
- Final Documents Published: Planned for 4/15/22 on Master Schule; Al thinks is will probably be late 2Q 2022.

- Al then listed these items as ones to consider for inclusion in the HCD cPP/SD Post-v1.0:
  - Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
  - Inclusion of NTP if it doesn't make v1.0
  - Inclusion of ALC_FLR.* if it doesn't make v1.0
  - Incorporate, as applicable, the changes to ISO 15408, particularly any relevant new SFRs in the updated Part 2
  - Support for SNMPv3
  - Support for Wi-Fi and maybe Bluetooth
  - Support for NFC
  - Support for Security Information and Event Monitoring (SIEM) and related systems
  - Expand to address 3D printing
  - Support for new crypto algorithms
  - Updates due to changes from ISO, FIPS or NIST Standards/Guidelines, NIAP TDs, or CCDB Crypto WG
  - Indirect updates based on new technologies or customer requests
- Al finished the HCD iTC discussion with some more additions to the HCD iTC lessons learned he presented at May and August 2021 IDS Face-to-Face Meetings. These additional lessons learned were:
  - Even after the third attempt at creating a PP for the same class of products, it still amazes me how bad we are at estimating how long it takes to develop a PP
  - Along the same lines, it's always the topics that you think will be the easy ones to resolve that most often turn out to be the biggest stumbling blocks, so never assume any comment or topic will be an "easy" one to resolve
  - Minutes of meetings are crucial when developing something like a cPP or SD, because you often need to know what was decided or discussed at a previous meeting
  - All iTC documentation including minutes should be available on-line to everyone
  - iTCs have to be flexible because sometimes unexpected requirements come from both the expected sources and sometimes surprise sources
  - Use of a good document management/version control tool from the start is essential

5. Al then briefly went ta discussion of the ENISA Cybersecurity Certification (EUCC). The reason for discussing EUCC was that he felt that EUCC will have significant impact on the HCD cPP, the CC and possible HCD vendors because of many of the provisions that are included within EUCC. Some key topics covered by Al's discussion were:
   - ENISA's goals are to:
     - Serve as a candidate EU cybersecurity certification scheme
     - Successor to existing schemes operating under the SOG-IS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement)

  - Base it on the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045
  - Cover the certification of any type of Information and Communications Technology (ICT) Product, Service or Process
- A couple of Key Definitions:
  - ICT product: an element or a group of elements of a network or information system
  - ICT service: a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems
  - ICT process: a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service
- EUCC's scope is essentially "Cybersecurity Certification of ICT products according to ISO/IEC 15408 and the Common Criteria (CC)" and covers the assessment of vulnerabilities of cryptographic implementations into the security functionalities of an ICT product in accordance with the requirements of the evaluation criteria and methodology defined in the CC
- Al noted that the security objectives of EUCC in many ways mirror the security objectives of a HCD – protection of stored data, protection of data in transit, access control, auditing, secure updates, availability and security by design.
- EUCC maps every SFR in CC Part 2 and SAR in CC Part 3 to one of the Security Objectives. However, EUCC;s biggest impact is that it requires by default that every evaluation must include a Vulnerability Assessment via SAR Class AVA and must include SAR family ALC_FLR Flaw Remediation.

  The ALC_FLR requirement has already been passed down as an edit to all iTCs. The HCD iTC decided that unless directed by either the Japanese of Korean Schemes we will not include one of the ALC_FLR SARs in HCD cPP v1.0 but it will definitely be in the next update.
- EUCC is based on the use of EALs per CC Part 3. Vulnerability Assessment is based on two assurance levels – Substantial and High. The definitions of the two assurance levels are determined by the assurance activities associated with them as follows:
  - Requires that European cybersecurity certificate that refer to assurance level 'substantial' shall provide assurance that:
    - ICT products, services and processes meet corresponding security requirements, including security functionalities
    - Have been evaluated at a level intended to minimize known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources
    - Evaluation activities to be undertaken include:
      - At least a review to demonstrate the absence of publicly known vulnerabilities
      - Testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities
  - Requires that European cybersecurity certificate that refer to assurance level 'high' shall provide assurance that:
    - ICT products, services and processes for which that certificate is issued meet the corresponding security requirements, including security functionalities
    - Have been evaluated at a level intended to minimize the risk of state-of- the-art cyberattacks carried out by actors with significant skills and resources
    - Evaluation activities to be undertaken shall include at least the following:
      - Review to demonstrate the absence of publicly known vulnerabilities

    - Testing to demonstrate that the ICT products, services or processes correctly implement the necessary security functionalities at the state of the art
    - Assessment of their resistance to skilled attackers, using penetration testing
- EUCC includes a detailed process for handling vulnerabilities found in an ICT product after a certificate for that product is issued. What Al found interesting is the strict time limits associated with the process, such as:
    - If the vendor detects a possible vulnerability in the ICT product they have to notify the CB (that is the Scheme that certified the ICT product) within one business day of the possible vulnerability
    - Once the vendor determines that it is a vulnerability, they have to notify the CB of that fact within 5 business days
    - The CB has a max of 90 days to determine an agreed-upon fix date for the vulnerability
- Just like the vulnerability process EUCC has a "Non-Compliance" process again with what seemed like unreasonable fixed dates associated with it for "detected vulnerabilities or irregularities concerning the security of the certified ICT product that may have an impact on its compliance with the requirements related to the certification".
- EUCC has divided what CC calls "Assurance Maintenance" into four different activities – Certificate Maintenance, Assurance Continuity (that's the parallel to Assurance Maintenance), Re-Assessment and Re-Evaluation.
    - The Certificate Maintenance Process can be initiated by either the manufacturer or provider of the ICT product or any other party. The CB validates whether some evaluation tasks are necessary before its review and decision, and if so the ITSEF (that's the Evaluation Lab) performs them. Based on CB review, the results of the continuous maintenance process can be anything from continuing the certificate without change up to suspending the certificate pending remedial action by the manufacturer or provider of the ICT product to even withdrawing the certificate,
    - The Assurance Continuity process is essentially identical to the Assurance Maintenance process performed against products certified against the CC.
    - Re-evaluation is essentially a new certification of the ICT product that reuses the results from the initial certification as the basis for the new certification.
    - Re-assessment is a new concept not in the CC. What it involves is the manufacturer or provider of the ICT product asking for the TOE to be re-assessed because the threat environment has changed. Only a vulnerability analysis is done and only on the new threat model and any vulnerabilities that arise from the new threats. The result is a re-assessment report for the TOE.
- EUCC requires that each CB be peer reviewed once every 5 years using a sample of 5% of the ICT products/services/processes certified with a least one ICT product that had been certified in the last year.
- EUCC has a documented patch management process based on four patch levels:
    - Patch Level 1: where the TOE is part of a bigger ICT product, and product parts not affecting the TOE may be patched whenever required
    - Patch Level 2: for minor changes
    - Patch Level 3: application of Assurance Continuity for a major change
    - Critical Process Flow: for changes where an attack is already possible to be exploited or update is critical and needs to be released urgently

This process defines what actions are to be performed by the manufacturer and CB at each Patch Level.

- EUCC is expected to become fully operational in 1H 2022, although there will be a transition period. Al indicated that this will have both short-term and long-term impacts on iTCs, possibly on the CC and maybe even on HCD vendors. For example, given all the provisions of EUCC (there are a lot more in EUCC than what was presented here) it is very possible that once EUCC goes into effect HCD vendors may be forced to do two product certifications, one in North America against the CC and one in Europe against EUCC. We are already seeing the impact of the ALC_FLR requirement on the HCD cPP. Finally, we have no idea what provisions of EUCC may eventually get incorporated into ISO 15408 and may be adopted by one of the Schemes outside of Europe such as NIAP. It will be interesting to follow EUCC to see where this all leads.

6. Al's final presentation was on the efforts to update ISO/IEC 15408 and ISO/IEC 18405 (the two CC Standards).
    - The current framework, which is the 3rd Edition, contains the following:
        - A framework (ISO/IEC 15408 Part 1) that explains how to generate specifications that can be evaluated by Labs under scheme policies
            - Protection Profiles (PP) (product-type specification of requirements)
            - Security Targets (ST) (product-level specification of requirements)
        - Catalogues of security requirements
            - Functional security requirements (Part 2)
            - Assurance security requirements (Part 3)
        - How to evaluate a Security Target or PP
            - Core methodology for evaluation (ISO/IEC 18045)
    - What is being developed now is the 4th Edition of the two standards which has the following key updates:
        - Security evaluation approaches allowing both:
            - Specification-based : Exact Conformance added
            - Attack-based : "Traditional EAL approach"
        - Addition of modularity and composition techniques to the model
        - Enhanced specification for packages
        - Updated Security Policy definition
        - Updated to include state-of-the art for the highest levels of evaluation (EAL 6 and EAL 7)
    - The concept of "Specification-based" vs. "Attack-based" evaluations is essentially that the original CC model as defined in the 3rd Edition with EALs (that for example is what EUCC bases its certifications on) uses the "Attack-based" approach, which is based on:
        - Use if Strict/Demonstrable Conformance and EALs
        - TOE type-specific evaluation methods
        - All evaluated TOEs are protected against a given set of threats
        - Allows for additions to assurance activities beyond what is in EALs

        On the other hand, "Specification-based" evaluations, which the HCD cPP/SD use, are based on:

        - :Exact conformance, direct rationale PPs, TOE and SFR-specific evaluation methods

- All evaluated TOEs are compliant to a given list of functional and assurance requirements: nothing more and nothing less
- All tests are set and known beforehand

The new framework of the 4th Edition will be as follows:

- The general model has been significantly revised (Part 1)
- New & changed security functional requirements (Part 2)
- Updated security assurance requirements (Part 3)
- Adds support in developing evaluation methodologies for specific technologies/product types (New part 4)
- All pre-defined packages of assurance packages moved to a (new) part 5
- For example, this is where the evaluation assurance level (EALs) are now found
- (To facilitate use by scheme/MRA policies)
- Updated the common evaluation methodology (ISO/IEC 18045 aka “CEM”)

Current Status is that it was planned to be releases in the end of 2021 bur is being held up over a disagreed over copyright issues with ISO.

7. **Wrap Up**

- Next IDS Conference Call will be on Nov 11, 2021. Main topic of the meeting will be a much deeper dive into EUCC.
- Next IDS Face-to-Face Meeting will be during the next PWG Virtual Face-to-Face Meeting February 8-10, 2022.

Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 11:59AM ET on November 4, 2021.