IDS WG Meeting Minutes
October 6, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on October 6, 2022.

Attendees

Smith Kennedy	HP
Ira McDonald	High North
Alan Sukert	
Mike Trent	Xerox
Brian Volkoff	Ricoh
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the HCD iTC Meetings since our last IDS WG Meeting on 9/22/22
   - Continuing the review of the Security Page on the PWG web site at the request of the PWG Steering Committee (SC) started at the 9/8/22 IDS WG Meeting
   - Special topic on the new updates to the Common Criteria Standards (ISO 15408 and ISO 18405)
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 provided a quick summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 9/22/22:
   - Al stated that all comments against the Final Drafts of both the HCD cPP and HCD SD have been adjudicated and the editors are now addressing all the comments. As of now, it is expected that both documents will be ready for final review to ensure comments were properly addressed and publishing by the end of the month.

     The goal was to have Version 1.0 of the HCD cPP and HCD SD published by the time the International Common Criteria Conference is held in mid-November. Unless something totally unexpected occurs, it looks like that is likely to happen.
   - The next steps will be to set up and implement the Interpretation Team and to start planning what the next steps are. In response to a question from Ira, Al indicated that the HCD iTC planned to do incremental Errata and content releases and then bundle the incremental releases into a major release at some point. The HCD iTC has to determine the time frame for the incremental and major release, but the next release after Version 1.0 of the HCD CPP/SD will be Version 1.1. There are some key things that need to go into a version of the cPP and SD as soon as possible such as TLS 1.3.

     Ira mentioned that the Network Device (ND) iTC has posted drafts of ND cPP/SD Version 3.0 which includes TLS 1.3 and the SSH Package from the CCUF Crypto WG. The HCD iTC should look into what the changes in Version 3.0 are to determine what could/should be implemented in Version 1.1 or future versions of the HCD cPP and HCD SD.
4. We then continued review of the Security Page on the PWG web site at http://www.pwg.org/security. The focus of this review was what additions could be added to the page to reflect IDS. It was another good discussion and the key comments from the discussion were:
   - When it is completed the HCD Security Guidelines should certainly be reflected on the page as an important deliverable.

- Ira indicated that the Hardcopy Device Health Assessment Trusted Network Connect Binding (HCD-TNC) spec should be added to the Network isolation and trust line in the Basic Security Features List. He also suggested that there should be a link to the latest TPM spec for the 'Trusted Platform Module' entry on the Basic Security Features List. Al expanded this to suggest that links should be provided wherever possible on the list.
- It was suggested that once Version 1.0 of the HCD cPP and HCD SD are published, a bullet discussing Common Criteria collaboration with a link to the published HCD cPP/SD should be added to the Basic Security Features List.
- There was a discussion on what the purpose of the Security Page was. Ira felt the purpose was essentially to tell the reader what the current print security landscape is and how the PWG fits into this landscape; Smith felt that the purpose was more to show what the PWG was doing in the various key security areas associated with printing.
- Some of the additional items suggested included:
  - Add S/MIME to the Confidentiality and data integrity bullet on the Basic Security Features List
  - Don't include document numbers; just titles
  - Add IPPS RFC to the list
  - Change "Automatic firmware/software updates" to "Secure firmware/software updates" and add System Services to this bullet
  - Add the IPP Implementers Guide to the appropriate bullet on the list
- Smith then stated that the Basic Security Features List was designed to reflect the basic list of security functions that a printer should have. He asked if there was a way to compare this list with what is in the HCD cPP.

  Al indicated that there was. In the Security Problem Definition which forms the front end of the HCD cPP there is a list of Security Objectives that are the key security functions that an HCD should have. All the SFRs in the HCD cPP must be traced back to one or more of these Security Objectives. Al was asked to compare the list of Security Objectives in the HCD cPP with the Basic Security Features List on the PWG Security page and report to the SC what the differences are.

5. Al then presented this week's special topic on the changes to the two Common Criteria Standards – ISO 15408 and ISO 18405. The slides Al used were actually from the Common Criteria User's Forum's Fall 2021 Workshop in Oct 2021 with updates of current status and can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/CCUF_ISO Update_20211014_kwlee.pdf.

   The main items covered in the presentation were:

   - The work to update the two Common Criteria standards is being done by ISO SC 27 WG 3. ISO 15408 is the standard that actually defines the Common Criteria process, while ISO 18405 is the Common Evaluation Methodology (CEM) which defines the criteria Evaluation Labs use to evaluate a product being certified against ISO 15408.
   - The current version of ISO 15408 and ISO 18405 in use is the 3rd Edition, Version 3.1, Revision 5; the new version of ISO 15408 and ISO 18405 will be the 4th Edition.
   - ISO 15408 is currently composed of three parts:
     - Part 1 is a framework that explains the general Common Criteria process and explains how to generate specifications that can be evaluated by Labs under scheme policies, particularly
       - Protection Profiles (PP) (product-type specification of requirements) and
       - Security Targets (ST) (product-level specification of requirements)
     - Part 2 is the catalogue of Security Functional Requirements (SFRs)

  - Part 3 is the catalogue of Security Assurance Requirements (SARs) and the discussion of the 7 Evaluation Assurance Levels (EALs)

- ISO 18405 (the CEM) describes the core method for evaluating PPs and STs
- The core methodology described in ISO 14508 is based on the "Attack-based Approach". This approach is based on the idea of starting with a threat analysis to determine the threats to the product or class of product to be certified, and then using these threats to determine the proper set of SFRs and the proper EAL necessary to protect the product being certified (know as the Target of Evaluation of TOE) against these threats.

  From a certification perspective the tests are known based on the EAL chosen, although additional testing such as penetration testing is often included. From a conformance perspective, CC certifications under this methodology are usually based on either demonstrable (conformance is equivalent or more restrictive than the statement of security problem definition in the PP to which conformance is being claimed) or strict (the statement of security requirements in the ST is a superset of or identical to the statement of security requirements in the PP to which conformance is being claimed) conformance. However, one positive aspect is that this methodology allows for the inclusion of additional SARs, most notably ALC_FLR.* (Flaw Remediation), so that you would often see certifications listed as EAL2+ because of the inclusion of Flaw Remediation to the SARs for EAL2.
- However, since 2015 NIAP has introduced a new "Specification-based" methodology for CC certifications that has been adopted by the CC Development Board. This methodology is based on Exact Conformance, meaning that the TOE must comply with the SFRs and Assurance Activities specified in the PP to which conformance is being claimed exactly with zero deviances; otherwise, the product fails certification. This methodology no longer relies on EALs; instead, each SFR has its own unique set of Assurance Activities and SARs tailored to the class of products in the PP to which conformance is being claimed. No additional SARs like Flaw Remediation are allowed.

  This methodology is strictly based on what is in the PP and the ST which is extracted from the PP with no deviations as stated above.
- A major goal of the changes to the two standards was to allow ISO 15408 to accommodate both the "Threat-based" and "Specification-based" methodologies. Some of the other major changes were:
  - 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)

  To accommodate these changes ISO 15408 was split from 3 Parts now into 5 Parts. The new format of ISO 15408 will be:
  - Part 1: The general model (same as before) but has been significantly revised
  - Part 2: Still contains the catalogue of SFRs, but with new & changed ones•
  - Part 3: Still contains a catalogue of SARs, but with updated security assurance requirements. However, the description of the EALs has been moved to the new Part 5
  - New Part 4: Adds support in developing evaluation methodologies for specific technologies/product types
  - New Part 5: Contains
    - All pre-defined packages of assurance packages
    - The evaluation assurance level (EALs)

  The CEM (ISO 18405) was also updated as required to reflect the changes to ISO 15408

- Current status, per Ira, is that the new ISO 15408 and ISO 18405 Standards have been published and are publicly available as of August 2022. Al received a different status that the two new standards would be finalized and published in November 2022 because of a copyright issue with ISO over the updated documents. Al noted that the new versions of the two standards have not yet been listed on the Common Criteria Portal. It is suggested that the reader of these minutes check with ISO and the Common Criteria **P**ortal to determine if and when the new Standards are or will be available.

6. **Actions:** Al: Compare the list of Security Features on the PWG Security Page against the list of Security Objectives from the Security Problem Definition in the HCD cPP.

Next Steps

- The next IDS WG Meeting will be October 20, 2022 at 3:00P ET / 12:00N PT. Main topics will be the latest status of the HCD cPP/SD and HCD iTC and a special topic to be determined.