IDS WG Meeting Minutes
October 14, 2021

This IDS WG Meeting was started at approximately 3:00 pm ET on October 14, 2021.

Attendees

Graydon Dodson	Lexmark
Erin Huber	Xerox
Alan Sukert	
Bill Wagner	TIC
Brian Volkoff	Ricoh
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the discussions at the 10/4 and 10/11 HCD iTC Meetings
   - Status of the HCD Security Guidelines
   - Review of the Oct 13-14 CCUF Workshop
   - Round Table Discussion
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. Since one of the topics covered at the CCUF Workshop was a presentation by Kwangwoo Lee, the HCD iTC Chair, on the status of HCD iTC; a screen-shot of Kwangwoo's slides can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/HCD iTC Update 10-14-21.pdf. Al went through Kwangwoo's slides for the HCD iTC portion of the meeting. The key points from Kwangwoo's slides were:
   - The membership slide showed that PWG is represented in the HCD iTC (Al is considered the PWG representative in the HCD iTC)
   - Two key events have occurred since the last IDS WG Meeting –
     - The 1st Public Draft of the HCD Supporting Document (SD) was completed on 10/8/21 and sent out for public review
     - The review period for the 1st Public Draft of the HCD cPP ended on October 8th. However, we have only received comments from the Korean and Japanese Schemes so far. Kwangwoo would like comments from other Schemes especially NIAP whose approval of the eventual published HCD cPP and HCD SD is needed, so he put out a request to other Schemes for comments post-Oct 8th. Therefore, we might see additional comments to the HCD cPP.
   - The schedule calls for the review period for the 1sp Public Draft of the HCD SD to be from 10/13 – 11/15. The schedule also currently calls for the 2nd Public Drafts to be available by 12/1/21. It will depend on how many comments we get against the HCD SD as to whether we can meet the current schedule. But right now, we are on a rough track to have the HCD cPP and HCD SD v1.0 published around the end of April 2022.
   - Kwangwoo displayed an interesting chart showing the comments against the various drafts of the HCD cPP and HCD SD in a way not seen before. Al commented that the chart showed 20+ comments so far against the 1st Public Draft of the HCD cPP, but that is really the number of GitHub issues against that draft; the number of actual comments is much larger because most of GitHub issues have multiple comments in them (e.g., the GitHub issue from the Japanese Scheme had 31 separate comments, although fortunately they were all minor editorial in nature).

- The last slide of interest was one that for the first time shows how the PWG IDS fits into the whole process of creating the HCD cPP and HCD SD. The slide shows that the PWG IDS interfaces with the HCD iTC to provide SME support to the HCD iTC in developing the HCD cPP/SD.

4. Ira wasn't present at the meeting so there was no status presented on the HCD Security Guidelines.
5. Al spent the rest of the meeting going through some of the other presentations from the CCUF Workshops; screen-shots of selected slides from the presentations described below can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/CCUF Workshop Slides.pdf. The presentations covered and some key messages were as follows:

   a. Different Approaches to Life Cycle Requirements – Rasmas Araby, @tsec

      - This presentation was about the NESAS Audit Methodology. NESAS (The Network Equipment Security Assurance Scheme), provides an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry. NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as using 3GPP (not sure what 3GPP is) defined security test cases for the security evaluation of network equipment.
      - The NESAS Audit Methodology involves four basic steps – a **Preparatory Step** where the equipment vendor defines security-related processes and procedures; an **Internal Step** where the equipment vendor assess conformity to NESAS requirements; the **Independent Audit** of the vendor process and finally the Audit Team's writing and validation with the vendor of **audit report**. This is standard audit methodology.
      - The focus of the NESAS Audit is on the vendor's development and life-cycle processes, so in many ways it is much like an EAL3 Common Criteria certification. The key areas the NESAS audit looks at are general requirements, design, implementation, building, testing, release and operation. NESAS Audits include a combination of documentation review and on-site review.
      - One interesting aspect is that the NESAS Audit must be completed in no more that 3 months, and the speaker said that is a fixed max time limit. The comment was made at the IDS Meeting that we wished CC Audits were that timely in being completed.
      - The goal of the on-site portion of the audit is to basically determine that (1) the vendor has documented processes that are being used on a day-to-day basis, (2) that the vendor has sufficient resources (personnel, equipment, skills, etc.) and (3) that the vendor's staff is sufficiently trained on the processes.
      - The presenter's last slide made some comparisons between the NESAS Audit methodology and other assessment schemes. The limited duration and the fact there is no type of certificate or international recognition are obvious differences, The presenter did list as a difference "similar to activities for CC ALC but focused on development activities rather than specific version of TOE". Al thought that was an incorrect comparison because ALC doesn't focus on TOE; it does focus on life-cycle activities independent of TOE.

   b. Introducing the methodology and guidance for Secure-Sub-System evaluation using Eurosmart ITSC's 3S in SoC PP, Monique Bakker and Markus Hinklemann

      - This presentation dealt with creating a new PP from an existing PP. The subject matter dealt with SoCs (System on a Chip), or as Al called it a "computer on a chip".
      - The concept was that there was an existing PP (Secure IC PP) that the SoC PP Subgroup wanted to use as a starting point to create a PP "which defines all aspects of using and protecting the security functions being integrated into the SoC". This PP would be able to support different external memory configurations of an embedded component in the SoC (e.g., Secure Memory vs. Internal Memory) and different functional packages.

- The new PP (Security Sub-System in System-on-Chip PP) would be for a TOE consisting of a component embedded in a Host SoC and would use the threats of the Secure IC PP as a starting point and add additional threats for the embedded component. Al indicated that this is an interesting approach that possibly could be applied to generating a 3D Printing cPP from the HCD cPP.

- An interesting difference for this Security Sub-System in System-on-Chip PP is the role of the "Integrator". The "Integrator" is the person who integrates the embedded component onto the SoC but is not the end user of the SoC with the embedded component. Guidance for how the "Integrator" functions is considered to be part of the TOE, which is a very unique aspect to this particular PP and requires that it be part of the overall guidance documentation covered under AGD.

- Finally, vulnerability analysis of the TOE for this new PP will require that the evaluation look into aspects of self-protection, domain separation, initialization and non-bypassibility.

c. Modern, Source-based, Semi-automated Software Testing, Robert Horr

- This was a presentation on a new "modern" test methodology. The main goal of this methodology is to create a way to "all" (known, unknown) errors of "all" paths efficiently. Al commented that from his early days involved with Software Process Improvement and software engineering research that you can never find "all" errors and you can never prove that you have found "all" errors. So, the goal of this test methodology is a little over ambitious and not really achievable.

- One thing Al pointed out that was nice about this test method was the use of test metrics. Al would have more to say about test metrics in a later slide.

- The presenter's test methodology is based on the use of test tools and the use of Fuzz Testing. Fuzz testing (or fuzzing) is an **automated software testing technique** that attempts to find hackable software bugs by randomly feeding invalid and unexpected inputs and data into a computer program in order to find coding errors and security loopholes. Al indicated it started up maybe 6-10 years ago and was going to be the "next big thing" in testing methodologies but never gained much widespread use. Al also didn't know much about the test tools being used in terms of how new they were or how widespread their use was.

- It is interesting that this test methodology is designed to work in a "bottoms up" manner, where it starts by finding memory leaks first, then finding memory access failures, then finding logical errors and then finally finding design errors. Al mentioned that this is the opposite of the standard approach where you start with requirements and design errors and then move on to coding errors.

- Regarding test metrics, two of the metrics being used are cyclomatic complexity (number of independent execution paths) and code coverage (number of executed independent execution paths). Al mentioned that when he was listening to the presentation he had a flashback because he was working with cyclomatic complexity when he was with General Electric over 30 years ago. The idea is that you want cyclomatic complexity to be low (the presenter state no higher than 15) and code coverage to be as high as possible.

d. ISO Update, Kwangwoo Lee

- This presentation gave an update on the updates to ISO/IEC 15408 and ISO/IEC 18045, the two Common Criteria ISO standards.

- There are types of certification approaches – the original "Attack-based Approach" where TOEs are evaluated against EALs and fixed SARs based on Strict/Demonstrable Conformance vs. the "Specification-based Approached" initiated by NIAP where TOEs are evaluated against PPs and Assurance Activities that are unique to each SFR based on Exact Conformance.

- Some of the key changes to the new 4th Edition to ISO/IEC 15408 are:

- It will support both types of certification approaches. In fact, the CCDB has approved the Exact Conformance Addendum.
- Updated the EAL 6 and EAL 7 evaluations
- Revised the general model in Part 1
- Added new SFRs and modified some SFRs in Part 2
- Moved the EAL descriptions that were in Part 3 to a new Part 5 that will also have pre-defined assurance packages. Part 3 will have update assurance requirements
- A new Part 4 will add evaluation methodologies for specific technologies/product types

- There will also be corresponding updates to ISO/IEC 18045 (the "CEM") which is the guide for evaluators.
- The plan was for the 4th Edition to be published at the end of 2021. However, there is a serious roadblock that is preventing that from occurring. Previously editions of both ISO standards were free; anyone could download them from the Common Criteria portal at no cost for use in building PPs or Security Targets.

  However, ISO is copyrighting this new edition of the two CC standards, which means one would have to pay to download them from the CC Portal. This has serious consequences to iTCs trying to use Parts 2. 3 or 5 of the new ISO/IEC 15408 to create a new PP or for vendors/labs trying to create an ST because it would now cost to do that. Al mentioned that when the P2600 WG created the two 2600 PPs, because of IEEE copyright rules they had to buy the copyright for the two PPs from the IEEE for $100K to ensure the PPs would be available for anyone who needed them for CC certifications or to create STs.

  The Common Criteria Development Board is definitely pushing back to the ISO JTC1 and the SC27/WG3 so we will just have to see how this will end up being resolved.

e. Although there were no slides, Al briefly went through a presentation on how the Egyptian government was trying to set up an Egyptian Common Criteria Scheme and join the Common Criteria Recognition Arrangement. What was interesting about the presentation was:

- The Egyptian government wanted to join the CCRA because it felt its national security demanded it.
- They are asking good questions like "Do they have current evaluation capability" or "How will CC evaluations be used by industry/government in Egypt" or "Are there current government policies requiring the use of evaluated products in government systems" or "What types of Protection Profiles will be of most interest to Egyptian government and commercial sectors".
- They have a 3-step approach to getting to the CCRA – (1) Set up the Egypt Certifying Body (CB) and an Egyptian Evaluation Lab; (2) Get the Egyptian Evaluation Lab accredited and (3) Get the Egyptian CB internationally recognized through the CCRA as a Certificate Consuming and eventually a Certificate Authorizing Member.

6. No Round Table
7. **Actions:** None

Next Steps

- The next IDS WG Meeting will be October 28, 2021 at 3:00P ET / 12:00N PT. Main topics will be review of the recent HCD iTC Meetings, HCD Security Guidelines Status Update, preparation for the November 4th IDS Virtual Face-to-Face Meeting, a special topic if there is time and Round Table.
- November Virtual IDS Face-to-Face – Nov 4, 2021, 10-12 AM ET.