# IDS WG Meeting Minutes
# October 28, 2021

This IDS WG Meeting was started at approximately 3:00 pm ET on October 28, 2021.

**Attendees**

| | |
|---|---|
| Graydon Dodson | Lexmark |
| Erin Huber | Xerox |
| Ira McDonald | High North |
| 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 10/18 and 10/25 Hardcopy Device international Technical Community (HCD iTC) Meetings
   - Ira McDonald's Liaison Report on TCG and IETF Activities
   - Preview of the 11/4 IDS Session at the Nov PWG Virtual Face-to-Face (F2F)
   - 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. Al began with a summary of what was covered at the 10/18 and 10/25 HCD iTC Meetings. For the most past the main thing covered at the two meetings was addressing comments against the 1st Public Draft of the HCD collaborative Protection Profile (cPP). Al indicated that to date there have been 85 comments submitted against this 1st Public Draft, of which 57 have been addressed in some way.

   The biggest issue facing the HCD iTC right now is how to handle Cryptographic Erase in the HCD cPP. The issue revolves around the following statement in the Security Problem Definition (SPD) portion of the HCD cPP in the Organizational Security Policies section under the Image Overwrite (Optional) section:

   Such customers desire that the image data be made unavailable by overwriting it with other data or by destroying its cryptographic key.

   JISEC, the Japanese Scheme, submitted a comment against the 1st Public Draft of the HCD cPP to remove this sentence. JISEC does not want Cryptographic Erase (CE) to be included in any of the discussions of Image Overwrite in either the SPD or in the FDP_RIP.1/Overwrite SFR that is the SFR addressing image overwrite. JISEC's rationale is that CE, which is what self-encrypting nonvolatile storage devices like Self-Encrypting Drives (SEDs) use to make data on the drive irretrievable, is already adequately covered in the HCD cPP via the two "key destruction" SFRs – FCS_CKM_EXT.4 which requires that the encryption keys in these drives be destroyed when no longer required and FCS_CKM.4 which provides the requirements as to how these encryption keys are to be destroyed.

   Several members of the HCD iTC disagree and feel that these two SFRs do not adequately address the inclusion of CE in the HCD cPP. The bottom line, however, is that there is general agreement that HCD cPP v1.0 has to include support for both methods for making user, job and confidential data stored on a disk irretrievable – the more common "image overwrite" mechanism where the data is overwritten by characters for at least one pass (typically vendors use 3 or more passes) and the CE method for SEDs and similar self-encrypting nonvolatile storage devices. An interesting side

discussion here is that Ira rightly pointed out that "overwrite: is not the proper term here; what we are really doing is removing the data so it should have been called "image removal".

Al then went into the source of this issue which is NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization. This document is now the US Government standard, including the DoD, for how to "sanitize" any type of media. NIST SP 800-88 defines sanitization as "a process to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort". There are three basic types of sanitization methods:

- **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques
- **Purge** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques
- **Destroy** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data

For Hard Disk Drives, the main **Clear** method described in NIST SP 800-88 is "Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools", which for HCDs is the "Image Overwrite" mechanism. It should be noted NIST SP 800-88 only requires one pass but does optionally allow multiple passes,

Since technically SEDs cannot do the "Image Overwrite" mechanism they cannot use the Clear method. However, NIST SP 800-88 for the **Purge** method allows "If the device supports encryption and the technical specifications described in this document have been satisfied, the Cryptographic Erase (also known as CRYPTO SCRAMBLE EXT) command". Al noted that "Cryptographic Erase through the Trusted Computing Group (TCG) Opal Security Subsystem Class (SSC) or Enterprise SSC interface" is also allowed which Ira provided some background on.

During the discussion of this topic a couple of interesting points were made:

- When discussion the section in the SPD, we questioned whether Image Overwrite should really be an optional requirement since customers almost universally require it on all HCDs. It isn't a required function now on Single Function Printers which is why it is still optional, but the question is whether in the future it should be required.

The bottom line to this discussion is that the HCD iTC has to find a way to address this issue. The iTC may spawn a small subgroup to determine how best to resolve the issue.

4. Ira then presented his Liaison Report on what is currently happening within the Trusted Computing Group (TCG) and Internet Engineering Task Force (IETF), The slides for Ira's report can be fond at https://ftp.pwg.org/pub/pwg/ids/Presentation/pwg-ids-november-2021-ira-tcg-ietf-v1.pptx. Some of the highlights from Ira's report are:

   a. TCG

      - TCG has formal relationships with Global Platform (GP), ETSI (see https://www.etsi.org/) , and ATIS (see https://www.atis.org/) and informal relationships with several other organizations including US-NIST.
      - One of the more interesting specs TCG is working on is ***TCG MARS 1.0 Mobile Profile***. MARS is a new 20 command structure that will be able to do cryptographic functions such as digital signatures and key generation/destruction. The reason this may be useful in the future is that hardware Trusted Platform Modules (TPMs) have been found to be very easy to hack. MARS may be able to replace hardware TPMs to provide secure boot in many low-cost products.
      - ***TCG Canonical Event Log Format*** spec will allow a device to store event logs.

b. IETF

- TLS Working Group now has 30 active specifications it is working on
- Some of the key TLS specifications are:
  - **Deprecating TLS 1.0 and TLS 1.1**
  - **IETF TLS 1.3 (errata update)** – there are around 68 errata, none of them technical
  - **IETF Compact TLS 1.3** – this is for browser interfaces
  - **IETF Return Routability Check for DTLS 1.2/1.3** – this provides for a heartbeat check to determine in DTLS is still connected if it hasn't responded for a given time period
  - **IETF Guidance for Ext PSK in TLS** – this is primarily for use of TLS in industrial devices
  - **IETF Secure Element for TLS Version 1.3** – this is for the Global Platform usage in mobile devices
  - **IETF Hybrid Post-Quantum KEMs for TLS 1.2** – this specification is to an attempt make TLS 1.2 faster by combining new Post-Quantum crypto algorithms with the "classic" crypto algorithms like AES
- **Security Automation and Continuous Monitoring (SACM)**
  - Work on SACM basically done
  - **IETF Concise Software Identifiers** – this is to reduce the size of the software ID file
- **Concise Binary Object Representation (CBOR)**
  - Most of the work here is to update CBOR and Concise Data Definition Language *(*CDDL)
  - **IETF Storing CBOR on Stable Storage** – this spec deals with static files
  - **IETF Notable CBOR Tags** – this spec defines 100 registered data types
  - **IETF Packed CBOR** – the goal here is to define how to further compress CBOR
  - **IETF Feature Freezer for CDDL** – This is more like a place where authors can work on new ideas for expanding CDDL
- **IRTF Crypto Forum Research Group (CFRG)**
  - The work the CFRG is extremely important and needs to be followed because the new algorithms that will come out of it will eventually be mandated and will have to be incorporated into the various cPPs. Ira stressed that as many of us as possible, especially if we have any interest in cryptology, should get involved with the CFRG.

5. Al spent the rest of the meeting reviewing the agenda for the November 4th IDS Session at the November PWG Virtual F2F. The agenda for the 2-hour meeting will be:

| When | What |
|---|---|
| 10:00 – 10:10 | Introductions, Agenda review |
| 10:10 – 11:10 | Discuss results of latest HCD iTC Meetings and HCD cPP/SD v1.0 status |
| 11:10 – 11:55 | ENISA Cybersecurity Certification (EUCC) / ISO Update |
| 11:55 – 12:00 | Wrap Up / Next Steps |

Al indicated that EUCC will could have a short-term impact on the HCD cPP but will most likely have a long-term impact on both the HCD cPP and, more importantly, the Common Criteria as a whole.

6. Round Table

   There was no time for the Round Table at the meeting itself, but after the meeting Ira did provide the following:

   - NIST Workshop on EO 14028 – Guidelines for Enhancing Software Supply Change Security Including Standards, Procedures & Criteria, November 8, 2021 at 1:00 PM EST

7. **Actions:** None

**Next Steps**

- November Virtual IDS Face-to-Face – Nov 4, 2021, 10-12 AM ET.
- The next IDS WG Meeting will be November 11, 2021 at 3:00P ET / 12:00N PT. Main topics will be review of the 11/8 HCD iTC Meeting and a more in-depth look at the EUCC.