IDS WG Meeting Minutes
February 3, 2022

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

Attendees

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Erin Huber	Xerox
Smith Kennedy	HP
Jeremy Leber	Lexmark
Alan Sukert	
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the HCD iTC Meeting since our last HCD iTC Meeting on 1/20/22
   - Preparation for the IDS Face-to-Face Meeting on February 9th
   - Share a discussion on the IDS's future I had with the PWG SC on 1/31
   - Round Table
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 one HCD iTC Meeting (1/24/22) since the last IDS Workgroup meeting on 1/20/22.
   - For the most past the main items covered at this meeting were a review of the FPT_WIPE_EXT SFR and associated Assurance Activities developed by the Cryptographic Erase Subgroup and the set of comments from ITSCC (the Korean Scheme) dealing with requested additions to the Assurance Activities for several of the cryptographic SFRs.

     Regarding the FPT_WIPE_EXT SFR and associated Assurance Activities, the HCD iTC reviewed the latest proposal from the Cryptographic Erase Subgroup and made many comments and suggested changes. In fact, enough changes to the proposal were suggested the Subgroup decided that a special subgroup meeting was needed to process the changes and come up with another proposal to be presented at the next HCD iTC meeting which would be on February 7th. Note: The subgroup did end up meeting on January 26th and did develop an updated proposal.

     Regarding the ITSCC comments against the HCD SD, since most of the HCD iTC (especially Jerry Colunga the HCS SD editor) had not had a chance to fully review the ITSCC comments, it was decided to give the full HCD iTC two weeks until the next HCD iTC meeting on 2/8/22 to review the ITSCC comments. The ITSCC comments were placed on the HCD iTC OnlyOffice public site so everyone could review them before the next HCD iTC meeting.

     The plan is that the full iTC will finish adjudicating the ITSCC comments at the 2/8 meeting. That is important because once the ITSCC comments are adjudicated and implemented the 2nd Public Draft of the HCD SD can be published and distributed for public review.

     Finally, Al did a quick review of the HCD iTC schedule. The HCD cPP is essentially on schedule but 2nd Public Draft of the HCD SD is now about 2 months behind schedule. Al thinks the Final Draft of the HCD cPP has a good chance of being ready by the beginning of April as planned,

although there still are some important issues that need to be resolved which he will discuss at the IDS presentation at the Face-to-Face (F2F) next Wednesday (2/9).

However, assuming the 2nd Public Draft of the HCD SD goes out the middle of February, the plan was to give reviewers one month to review the document. Al's hope is the implementing the ITSSC comments will mean that there will not be too many technical comments against the 2nd Public Draft of the HCD SD. However, Al's best guess is that the HCD cPP and HCD SD will likely get published sometime in July 2022.

Given that the HCD iTC was formed in Feb 2020, that would put the publishing on Version 1.0 some 2-1/2 years after the iTC was formed. Considering the 2600 PPs took 5+ years to be developed and the HCD PP 3+ (almost 4) years to be developed, getting the HCD cPP/SD in 2-1/2 years would not be bad at all.

4. Al then discussed a topic he will be presenting at the IDS F2F Meeting on 2/9. One suggestion back at the 12/16 IDS Meeting was that we follow-up on some of the special topics covered in 2021. Al decided to follow-up on the Cybersecurity Executive Order issued by the White House in May 2021.

   Al showed the meeting attendees a document he put together that showed what had been done to implement this Executive Order in 2021. He will present highlights of this document at the F2F, but he went through some of the highlights at the meeting. Some of the key steps that were done to implement the Executive Order in 2021 were:

   - NIST Published Guidelines Recommending Minimum Standards for Vendor Verification of Their Software Source Codes. These guidelines were based on verification standards using (1) Threat Modeling; (2) Automated Testing; (3) Code-Based (Static) Analysis; (4) Dynamic Analysis; (5) Check Included Software; and (6) Fix Bugs.
   - NIST Published Preliminary Guidelines for Enhancing Software Supply Chain Security as part of NIST SP 800-161 Rev 1. These guidelines describe key cybersecurity supply chain risk management (C-SCRM) practices for managing exposures to cybersecurity risks, threats, and vulnerabilities throughout the supply chain and developing appropriate response strategies presented by the supplier, the supplied products, services, and the supply chain.
   - NIST issued three reports related to cloud security: (1) the Second Draft NIST Internal Report (IR) 8320, "Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases"; (2) Draft NIST IR 8320B, "Hardware-Enabled Security: Policy-Based Governance in Trusted Container Platforms"; and (3) Draft NIST Publication (SP) 1800-19, "Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments."
   - Cybersecurity and Infrastructure Security Agency (CISA) Published Cybersecurity Incident Response and Vulnerability Response Playbooks – an Incident Response Playbook covers incidents that involve confirmed malicious cyber activity and for which a "major incident" (as defined by the Office of Management and Budget) has been declared or not yet reasonably ruled out and a Vulnerability Response Playbook that applies to any vulnerability "that is observed to be used by adversaries to gain unauthorized entry into computing resources."
   - NIST Published Security Guidance for Internet of Things Devices - Establishing IoT Device Cybersecurity Requirements (NIST Special Publication (SP) 800-213) that overviews areas of consideration for organizations when determining the applicable cybersecurity requirements for an IoT device and (2) a revised IOT Device Cybersecurity Requirements Catalog (NIST SP 800-213A) that contains controls similar to NIST SP 800-53.

   Al indicated that he will dive deeper into some of these new areas, especially the NIST SPs for presentation at future IDS WG meetings. The full document Al prepared has numerous other links and much more detail on these and other items that were accomplished such as workshops in support of the Executive Order. The full document is located at https://ftp.pwg.org/pub/pwg/ids/Presentation/Cybersecurity Executive Order Updates.pdf

5. Al then discussed some of the results of a PWG Steering Committee (SC) Tiger Team meeting held on Monday 1/31. The purpose of the meeting was to discuss the IDS Charter Evolution. Although Al couldn't discuss much of what was covered at the meeting, there were a few things covered that were pertinent to the IDS WG.

   One of Al's main points at the meeting was that current the IDS and IPP WGs within PWG are "stovepipes", meaning that they act as separate groups without any contact with each other. Al feels that the two WGs need to be integrated under the PWG umbrella so that they work together and so that there can be cross-pollenization between the two groups.

   Towards that end Smith Kennedy proposed that there could be IPP presentations at IDS Meetings to "break down the walls". The presentations would be on IPP issues that dealt with security, confidentiality, authentication and privacy. Smith suggested areas such as:

   - An IPP overview such as the one he gives yearly to the Mopria alliance
   - A brief summary of areas such as IPP encrypted jobs, job accounting and IPP authentication methods

   Al invited Smith to start with the IPP overview presentation at the next IDS WG Meeting on Feb 17th which he accepted. The other presentations will be done at future IDS WG meetings.

   Al also mentioned that he would like IDS to start looking into following other standards areas beyond the HCD cPP/SD. A couple of key area are cybersecurity – certainly further exploration of what is being done to implement the Cybersecurity Executive Order is needed as well as follow-up on EUCC – and 3D printing, since it is possible that in the near-distant future 3D printing may replace 2D printing if it becomes cheap enough as the main printing method among industry and home users.

6. Finally, Al quickly went through the planned agenda for the upcoming IDS F2F Meeting on Wednesday, Feb 9th. The planned agenda is:

When	What
10:00 – 10:10	Introductions, Agenda review
10:10 – 11:05	Discuss results of latest HCD iTC Meetings and HCD cPP/SD v1.0 status
11:05 – 11:20	Cybersecurity Executive Order Follow-up
11:20 – 11:35	HCD Security Guidelines v1.0 Status
11:35 – 11:55	TCG/IETF Liaison Reports
11:55 – 12:00	Wrap Up / Next Steps

7. **Actions:** None

Next Steps

- February PWG IDS Face-to-Face Meeting will be on February 9, 2022 at 10:00 AM ET.
- The next IDS WG Meeting will be February 17, 2022 at 3:00P ET / 12:00N PT. Main topics will be review of the 2/7 and 2/14 HCD iTC Meetings and Smith Kennedy's IPP Overview presentation.