IDS Face-to-Face Minutes
February 9, 2022

Meeting was called to order at approximately 10:00 am ET February 9, 2022.

Attendees –

Graydon Dodson	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/2022-02-09-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
   - Cybersecurity Executive Order Follow-up
   - HCD Security Guidelines v1.0 Status
   - Trusted Computing Group (TCG) / Internet Engineering Task Force (IETF) Liaison Reports
   - Wrap-Up / Next Steps
3. Smith went quickly through the PWG Antitrust, Intellectual Property and Patent 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 2nd Public Draft of the HCD cPP (Version 0.11 dated 12/14/2021) on 12/14/2021.
   - There have been 76 total comments submitted against the 2nd Public Draft of the HCD cPP. 31 of the 76 comments have been reviewed and addressed by the HCD iTC to date. The tally of these 31 comments addressed is:
     - 28 comments were 'Accepted' to be fixed for the Final Draft of the HCD cPP
     - 0 comments were 'Accepted in Principle' to be fixed eventually in the HCD cPP by the time the HCD cPP v1.0 is published
     - 1 comment was 'Deferred' to be addressed a later time, possibly in a later version of the HCD cPP
     - 2 comments were either not accepted or rejected
   - The 2nd Public Draft of the HCD SD is still in development. There were 29 comments submitted against the 1st Public Draft of the HCD SD and all 29 comments have finally been reviewed and addressed by the HCD iTC. The tally of these 29 comments addressed is:

  - 25 comments were ‘Accepted’ to be fixed for the Final Draft of the HCD cPP
  - 0 comments were ‘Accepted in Principle’ to be fixed eventually in the HCD cPP by the time the HCD cPP v1.0 is published
  - 0 comments were ‘Deferred’ to be addressed a later time, possibly in a later version of the HCD cPP
  - 3 comments were either not accepted or rejected
  - 1 comment is on hold pending discussion with ITSCC (the Korean Scheme).
- Al then reviewed the key issues that were resolved in the 2nd Public Draft of the HCD cPP:
  - Added a note for the optional Organizational Security Policy Purge in Section 3.5.7 indicating that Cryptographic Erase is not included in this optional requirement because it is covered in the mandatory requirement of FCS_CKM_EXT.4 and FCS_CKM.4.
  - Replaced the text of the Application Note for SFR **FPT_KYP_EXT.1 Extended: Protection of Key and Key Material** in the 1st Public Draft to add clarity to what the Application Note was trying to convey.
  - Removed the part of the sentence in the application note in SFR **FCS_KYC_EXT.1.1** (**Key Chaining**) that talks about “keys in areas of protected storage” because keys in areas of protected storage are already discussed in SFR **FPT_KYP_EXT.1 Protection of Key and Key Material** in a superior way.
  - Clarified via an addition to the Application Note that the scope of TST Testing for SFR **FPT_TST_EXT.1 TSF testing** is focused on correct operation of the cryptographic function and detection of malfunctions, since the integrity of the executable code can be guaranteed by SFR **FPT_SBT_EXT Secure Boot**
  - Clarified that the requirement in SFR **FPT_SBT_EXT Secure Boot** to use the chain(s) of trust to confirm integrity of its firmware/software using one or more of the selected methods applies only at boot time.
  - Clarified that support for TLS Mutual Authentication and DTLS Mutual Authentication, whether as a client or as a server, are optional in all cases.
  - Corrected numerous incorrect references, External Component Definitions and header information for several SFRs.
  - Clarified that SFRs **FIA_X509_EXT.1 X.509 Certificate Validation and FIA_X509_EXT.2 X.509 Certificate Authentication** must be selected (they are both Selection-Based Requirements) if ‘X.509 Certificate’ is selected in **FPT_TUD_EXT.1.3 (Trusted Update).**
  - Added AES bit selection option to SFR **FCS_COP.1.1/StorageEncryption.**
- Al provided an update on the issue facing the HCD iTC on how to handle Cryptographic Erase (CE)- see the minutes from the November 4, 2021 IDS Face-to-Face Meeting for the background on this issue.

  JISEC (the Japanese Scheme) wanted 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 felt Cryptographic Erase is covered by the two Key Destruction SFRs (FCS_CKM.4 & FCS_CKM_EXT.4) already in the HCD cPP. ITSCC (the Korean Scheme) felt Image Overwrite and Cryptographic Erase are two different things and agreed with JISEC’s position. ITSCC’s suggestion was 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 its first meeting on 11/3/21.

  To resolve the issue the subgroup ended up creating a new Data Wiping SFR FPT_WIPE_EXT and associated Assurance Activities to replace the current FDP_RIP.1/PURGE SFR. This new SFR requires D.USER and D.TSF data stored on non-volatile storage to be made unavailable upon the request of an Administrator using one or more of the following methods: (1) *overwrite,* *(2) block erase,* (3) *Cryptographic Erase,* (4) *[**assignment:** media-specific method(s)].* Note: In this context, "Cryptographic Erase" encompasses any method that destroys the decryption key while leaving encrypted D.USER and/or D.TSF on the storage media. This would include, for example, some ATA commands that only destroy the key.

The HCD iTC is still reviewing the new Data Wiping SFR but hopes to have the SFR finally finished by its next meeting on Feb 13th.

- Release of the 2nd Public Draft of HCD SD was being held up because the HCD iTC needed to address the ITSCC (Korean Scheme) request to add substantive additional testing to Assurance Activities for several cryptographic SFRs. Fortunately, these comments were finally resolved at 2/6 HCD iTC Meeting so the HCD SD 2nd Public Draft could finally be completed, published and distributed for comment9.

- Inclusion of NTP is still an open issue. Al definitely feels that HCD cPP v1.0 should not be issued without inclusion of the requirements for NTP because most customers use NTP to set the time for their HCD devices and most vendors already implement "secure NTP" already. In response to a question from Smith, Al indicated that the issue that is holding up inclusion of NTP to this point is that Japanese vendors were concerned that the NTP SFR that we obtained from the Network Device (ND) cPP required the use of "secure STP" (the actual requirement is "The TSF shall update its system time using [selection: *IPsec, DTLS*] to provide trusted communication between itself and an NTP time source.") and they were not sure that they would be able to implement this requirement. Al noted most vendors he was aware of already implement "secure NTP" already

  Ira mentioned that most vendors use the Network Time Security (NTS) protocol (RFC 8915) that uses TLS and Authenticated Encryption to provide cryptographic security for the client-server mode of NTP. It was noted that NTS now requires support for TLS 1.3. Ira suggested the current NTP requirement could be changed to include NTS as one of the selection options. Al said he would bring that suggestion up when he brings up the topic of NTP again to the HCD iTC for consideration one last time.

  Ira noted that the TLS WG within the ND iTC had decided to ignore the latest set of NIAP comments against the latest TLS 1.3 draft and publish it in the next ND cPP release (Ira didn't know when that release was scheduled). In a later slide Al indicated that TLS 1.3 support would not be in HCD cPP v1.0; given this new information there is now a small but finite possibility, depending on the maturity of the TLS 1.3 requirements by the ND iTC, that we might be able to get TLS 1.3 into the HCD cPP in time to make the Final Draft. Al will check with the ND iTC Lead about this possibility at the next iTC Chair Meeting.

- Another issue the HCD iTC considered was a comment concerning the Secure Boot SFR FPT_SBT_EXT The current SFR requires that the hardware-based Roots of Trust must be stored in immutable memory. The comment asked whether the requirement should address hardware-based Roots of Trust stored in mutable memory as well as immutable memory. The Hardware-anchored Integrity Verification Subgroup looked at this issue and decided that it might be possible to address this issue, but that it would require significant changes to the Secure Boot SFR, addition of at least one new SFR and other changes to the Security Problem Definition and other parts of the HCD cPP. The subgroup felt the required changes were too many to implement at this point in the HCD cPP development, so it was decided to address this issue in future versions of HCD cPP

  Ira mentioned that this could be a problem for vendors getting some HCDs certified that do implement their hardware-based RoTs in mutable memory and this also could pose a problem when trying to revoke certificates. Al indicated that we were aware of the issues but the HCD iTC had to make the decision, and iTCs often have to make these types of decisions.

- 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 with RSA Key Generation with keys < 2048 bits are already being disallowed in most cases, so the HCD iTC is probably going to have to disallow support for that as well as for SHA-1 and all RSA and DHE Key Exchanges anyway.

- Al indicated that right now with the exception of maybe NTP and possibly TLS 1.3, there is no new content planned for the HCD cPP behind what is already in the pipeline. The only things that might change that would be requests from the Japanese and Korean Schemes, NIAP Technical Decisions against the HCD PP or possible comments against the 2nd Public Draft of the HCD SD.
- Al provided a status update on the schedule as follows:
  - 2nd Public Draft of the HCD CPP was released on time (12/14/21) per the updated schedule and comments were received on time (1/31/22) per the revised schedule.
  - 2nd Public Draft of the HCD SD is now planned for release on 2/18/22 and comments are planned to be received by 3/18/22. That is some 2 months behind the revised schedule.
  - Final Draft Submitted for Review: Right now, baring something unexpected, Al thinks the Final Draft of the HCD cPP should be published as scheduled at the beginning of April 2022. The Final Draft of the HCD SD is probably going to be published around the middle of May 2022; it could be published sooner depending on the number of comments that are received.

    Ira commented that in his experience it is that final draft where the most comments are received, especially from other Schemes, because this is the time when they realize they have to review the document. Al agreed with Ira, stating that he has been concerned with the lack of comments from other Schemes, especially NIAP, and is fearful we may get a dump of comments against the Final Draft.
  - Final Documents Published: Right now, per the schedule the HCD cPP/SD are to be published in mid-May 2020. Given that the HCD SD is two months behind the HCD cPP, Al's best guess is that earliest the two documents could be published in mid-July 2022. If Ira's experience comes to pass, it could be even later than that.
- Al then listed these items as ones to consider for inclusion in the HCD cPP/SD Post-v1.0. They were essentially the same ones that he presented at the November 4th IDS Face-to-Face meeting.
- In talking about next steps, Al emphasized that a key "next step" was that the HCD iTC has to start planning for what comes after HCD cPP/SD v1.0. That involves two areas:
  - Determining what will be the schedule for future releases of the HCD cPP/SD versions (for example – minor updates every 6 months and major updates every 18 months)
  - Preparing the infrastructure (people and process/procedures) for establishment of an Interpretation Team to address the inevitable questions, comments, errors, etc. that will crop up as HCD cPP/SD v1.0 begins to be used to actually certify HCDs.
- Al finished the HCD iTC discussion with some more additions to the HCD iTC lessons learned he presented at May, August and November 2021 IDS Face-to-Face Meeting. These additional lessons learned were:
  - You have to be aggressive in the way you attack a problem or you will never get done
  - No matter when you think you've finished solving a problem, you'll find that you're not finished at all
  - Standards work takes a lot of patience
  - You have to rely on a same core group of dedicated volunteers or you'll never get it done

5. Al then presented follow-up information to the Executive Order on Improving the Nation's Cybersecurity topic he had presented at the IDS Session during the PWG August 2021 Face-to-Face Meetings.

As a precursor, this Executive Order was issued by the White House on May 12, 2021. Its goal was to establish a Cybersecurity policy that must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)). The purpose of this discussion was to indicate what steps had been done to implement this Executive Order in 2021 since it had been issued in May 2021.

The key steps that had been taken were:

- NIST defined "critical software" as: *any software that has or has direct software dependencies upon, one or more components with at least one of these attributes:*
    - *Software that is designed to run with elevated privilege or manage privileges;*
    - *Software that has direct or privileged access to networking or computing resources;*
    - *Software that is designed to control access to data or operational technology;*
    - *Software that performs a function critical to trust; or operates outside of normal trust boundaries with privileged access.*
- The National Telecommunications and Information Administration (NTIA) defined the minimum elements of a Software Bill of Materials (SBOM) to be:
    - Required data fields (e.g., "supplier name," "component name," and "cryptograph hash of the component,")
    - Operational considerations - a set of operational and business decisions and actions that establish the practice of requesting, generating, sharing, and consuming SBOMs
    - Support for automation - support relates to whether the SBOM can be automatically generated and is machine-readable.
- NIST published guidelines recommending minimum standards for vendor verification of their software source codes that consists of the following Technique Classes - (1) Threat Modeling; (2) Automated Testing; (3) Code-Based (Static) Analysis; (4) Dynamic Analysis; (5) Check Included Software; and (6) Fix Bugs. Each of these Technique Classes includes one or more specific techniques.
- NIST released the final version of NISTIR 8259B, "IOT Non-Technical Supporting Capability Core Baseline". It complements NISTIR 8259A, "Core Device Cybersecurity Capability Baseline (May 2020), which is NIST's guide to the technical aspects of manufacturing secure Internet of Things ("IOT") devices and products.

    NISTIR 8259B describes four recommended non-technical supporting capabilities related to the lifecycle of cybersecurity management that manufacturers should implement, including (1) documentation, (2) information and query reception, (3) information dissemination, and (4) education and awareness. NISTIR 8259A and NISTIR 8259B are intended to define a baseline set of activities that manufacturers should undertake during the planning, development, and operational life of IOT devices to address the cybersecurity needs and goals of their customers.
- NIST published preliminary guidelines for enhancing software supply chain security - NIST Special Publication 800-161 Revision 1. These guidelines contained three targeted initiatives:
    - Critical Software Definition and Security Measures;
    - Recommended Minimum Standard for Vendor or Developer Verification of Code; and
    - Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software
- NIST issued three guidance documents on Cloud Security
    - 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"
    - Draft NIST IR 8320B, "Hardware-Enabled Security: Policy-Based Governance in Trusted Container Platforms"

-
  - Draft NIST Publication (SP) 1800-19, “Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments.”

  These documents provide guidance on practices, techniques, and technologies for securing data in connection with various cloud services. Al noted that the area of Cloud Security was not mentioned in the original Executive Order, nor was IoT. This just showed the intent to address cybersecurity threats across the entire spectrum of software.

- NIST released a draft Secure Software Development Framework (Draft SSDF) at the end of September 2021 - Draft NIST Special Publication 800-218, Version 1.1. This SSDF framework consists of a core set of high-level secure software development practices that can be integrated into software development life cycles.

- The Cybersecurity and Infrastructure Security Agency (CISA) published two Cybersecurity Incident Response and Vulnerability Response Playbooks – one for incidence response and one for vulnerability response.

  The 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. It provides Federal Civilian Executive Branch (FCEB) agencies with a standard set of procedures to identify, coordinate, remediate, recover, and track mitigations from incidents affecting FCEB systems, data, and networks.

  The Vulnerability Response Playbook applies to any vulnerability “that is observed to be used by adversaries to gain unauthorized entry into computing resources.” It sets forth standard, high-level processes and practices that FCEBs should follow when responding to vulnerabilities that pose significant risk.

- NIST issued a Draft Criteria for Consumer Software Cybersecurity Labeling. This draft describes the baseline technical criteria as a series of attestations, i.e., claims made about the software associated with the label. It organizes these attestations into the following categories: (1) Descriptive Attestations, such as who is making the claims in the label, what the label applies to, and how consumers can obtain other supporting information; (2) Secure Software Development Attestations, such as how the software provider adheres to accepted secure software development practices throughout the software development cycle; (3) Critical Cybersecurity Attributes and Capability Attestations, and (4) Data Inventory and Protection Attestations, including declarations concerning the data that is processed, stored, or transmitted by the software.

- NIST published Security Guidance for Internet of Things Devices consisting of:

  - 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

  - Revised IOT Device Cybersecurity Requirements Catalog (NIST SP 800-213A) that contains controls similar to those in NIST SP 800-53 that can be selected in categories such as Data Protection, Software Update, Cybersecurity State Awareness and Device Security (essentially a NIST SP 800-53 for IoTs)

6. Ira then covered the latest status on the HCD Security Guidelines. Ira had just published the previous day an updated version of the HCD Security Guidelines (Version 13.1 dated 8 February 2022) that can be found at https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20220208-rev.docx (Note: a “clean” version of the update can be found at https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20220208.docx).

   The updates were mainly in Section 5, HCD Local Security. Ira indicated this was not meant to be a thorough review of the changes since some of the updates were incomplete, so he planned to just walk through the changes during this meeting which he proceeded to do.

There were questions regarding the material in Section 5.2, Local Peripheral Interfaces, specifically about Bluetooth and Bluetooth Low Energy (BLE) and the guidance around not enabling either by default. It was pointed out that Bluetooth beacons, which only announce their presence but do not act as two-way interfaces, may be included in HCDs by default. Ira agreed that this guidance and this whole section does need some rework.

There was also a question about Section 5.2.2 on HDMIs and HDMIs were actually on HCD. Ira indicated he would look into this and remove this section if they were not.

Finally, there was some discussion on USBs, although what is in the document now is very preliminary and needs to be significantly expanded.

7. For the final topic Ira presented his Liaison report on current standards developments for the Trusted Computing Group (TCG) and Internet Engineering Task Force (IETF). The key points from Ira's Liaison Report were:

- Regarding TCG standards activities, some key items Ira stressed were:
  - **TCG MARS 1.0 Mobile Profile** – this is out for public review and is the first update in 8 years. MARS, by the way, is designed to support secure boot.
  - **TCG SNMP MIB for TPM-Based Attestation –** it was published January 2022 and supports TPM 2.0
- Regarding IETF standards activities, some key items Ira stressed were:
  - IETF 113 Hybrid F2F (Vienna, Austria) is 21-25 March 2022,
  - IETF 114 Hybrid F2F (Philadelphia, USA) is 25-29 July 2022**.** Ira doesn't expect much live attendance at either meeting. Ira also noted that CDDL 2.0 will be introduced at IETF 114.
  - **IETF Deprecating MD5 and SHA-1 in TLS 1.2 and DTLS 1.2** – It is important that the HCD iTC take note of this
  - Security Automation and Continuous Monitoring (SACM) has been abandoned mostly. IETF Concise Software Identifiers is the only spec left for this Working Group, which is effectively being shut down.
  - **IETF Additional Control Ops for CDDL – RFC 9165** is creating new operators for CBOR (Concise Binary Object Representation).
  - There is a new spec being developed that is I "Last Call" that is for CBOR Tags on file storage.
  - **IETF Notable CBOR Tags – draft-04 – August 2021** – this spec is for more CBOR tags.
  - There is a lot going on under Remote ATtestation ProcedureS (RATS).
    - **IETF TPM-based Network Device RIV – draft-11** and **IETF YANG Data Model for CHARRA using TPMs – draft-12** are I IETF Last Call
    - **IETF Attestation Results for Secure Interactions – draft-01** and **IETF Direct Anonymous Attestation for RATS – draft-00** are WG Adopted.

  The IETF is putting pressure on RATS to move along.

A question was asked what type of certification program was applicable to these IETF specs. Ira indicated that outside of a Common Criteria certification where SFRs that included these specs as requirements were included in the Security Target, the only other applicable certification program he is aware of is the Global Platform certification program, However, this program is only for mobile devices.

8. **Wrap Up**

- Next IDS Working Group Meeting will be on February 17, 2022. Main topics of the meeting will be latest HCD iTC status and an IPP Overview presentation by Smith Kennedy.
- Next IDS Face-to-Face Meeting will be during the May 2020 PWG Virtual Face-to-Face Meeting May 10-13, 2022.

Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 12:01PM ET on February 9, 2022.