IDS Face-to-Face Minutes
August 19, 2021

Meeting was called to order at approximately 10:00 am ET August 19, 2021.

Attendees –

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Ira Kaplan	Brother
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/2021-08-19-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
   - Executive Order on Cybersecurity
   - HCD Security Guidelines 1.0 Status
   - TCG/IETF Liaison Reports
   - Wrap-Up / Next Steps
3. Went quickly through the PWG Antitrust and Intellectual Property 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 3rd Internal Drafts of both the HCD cPP (on 6/9/21) and the HCD SD (on 6/29/21).
   - There have been 184 total comments submitted against all three drafts of the HCD cPP to date. All 184 comments have been reviewed and addressed by the HCD iTC. The tally of these 184 comments is:
     - 132 comments were ‘Accepted’ to be fixed for the 1st Public Draft of the HCD cPP
     - 5 comments were ‘Accepted in Principle’ to be fixed eventually in the HCD cPP by the time HCD cPP v1.0 is published
     - 37 comments were ‘Deferred’ to be addressed a later time, possibly in a later version of the HCD cPP
     - 10 comments were either not accepted or rejected

- Similarly, there have been 79 total comments submitted against all three drafts of the HCD SD to date. 75 of the 79 comments have been reviewed and addressed by the HCD iTC. The tally of these 75 reviewed comments is:
  - 64 comments were 'Accepted' to be fixed for the 1st Public Draft of the HCD SD
  - 1 comment was 'Accepted in Principle' to be fixed eventually in the HCD SD by the time HCD SD v1.0 is published
  - 10 comments were 'Deferred' to be addressed a later time, possibly in a later version of the HCD SD
  - 0 comments were not accepted
- A key Essential Security Requirements (ESR) document requirement is "The HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications" which was added at the request of the HCD iTC. The HCD iTC formed a Hardware-anchored Integrity Verification subgroup to address this requirement. This subgroup finally completed its work in August 2021 after 9 months of effort. The main outputs that came out of the Subgroup were:
  - A Secure Boot Security Functional Requirement (SFR) – FPT_SBT_EXT.1 – and the accompanying Assurance Requirements[1] that addresses the concept of both Chain of Trust and Root of Trust and allows for multiple Chains of Trust, each with its own hardware-anchored Root of Trust.
  - The necessary additional wording in the appropriate sections in the HCD cPP, such as in the Security Problem Definition, that are needed to support the concept of Chain of Trust and Root of Trust.
  - Inclusion of the necessary crypto SFRs to support the methods of verifying the integrity of firmware/software at boot time - hash, digital signature, message authentication (to include both HMAC and CMAC).
  - Inclusion of the necessary crypto SFR to properly address protection of symmetric keys stored in protected memory.
- An interesting issue that the HCD iTC resolved was a request from the Korean Scheme regarding the audit log. In previous drafts of the HCD cPP the requirements to store the audit log in the device and to require the audit log to be readable via one of the interfaces on the device (either the Control Panel on the device itself or via a web interface to the device) were optional requirements; the Korean Scheme strongly felt these requirements should be mandatory requirements. After the Japanese and US Schemes both indicated they agreed with the Korean Scheme's position, the HCD iTC agreed to make all the audit log requirements regarding storage of the audit log on the device and reading the audit log via an interface on the device mandatory requirements in the HCD cPP.
- Some of the issues that the HCD iTC are working on now are:
  - The proposal to add the NTP SFR from the ND cPP is still on hold while vendors determine whether they can support "secure NTP", since the NTP SFR from the ND cPP requires updating the time via either authentication using a message digest algorithm or a trust communication channel using either IPsec or DTLS.
  - The HCD cPP and JBMIA (The Japanese Business Manufacturing Association) are still working on JBMIA's request to change the wording of the FPT_KYP_EXT.1 Protection of Key and Key Material SFR in the HCD cPP and the corresponding Assurance Activities in the

[1] An SFR define the requirements (i.e., the "what") that have to be met; the Assurance Activities define the documentation and test criteria that are used to determine that the requirements defined in the SFR have actually been met

HCD SD to be more like the wording in the corresponding FPT_KYP_EXT.1 SFR in the Full Drive Encryption Engine (FDE EE) cPP and Assurance Activities for this SFR in the FDE EE SD. JBMIA's concern was that wording for the FPT_KYP_EXT.1 SFR in the current HCD cPP drafts did not not indicate how to protect the keys. The SFR in the FDE AA cPP better specifies various criteria that the stored protected keys can meet to fulfil this requirement. Currently the HCD iTC and JBMIA are finalizing the wording for the Application Note in the SFR.

- The HCD iTC still has issues that have to be worked on. Among them are:
  - What to do with the "Deferred" comments – move them into a parking lot for future versions or resolved them for v1.0.
  - Perform internationalization of the standards and specs referenced in SFRs in the HCD cPP.
  - Decide on whether to remove support for TLS 1.1, SHA-1, cipher suites with RSA Key Generation with keys < 2048 bits, and all RSA and DHE Key Exchanges (Note that the HCD iTC already agreed to remove support for TLS 1.0). This issue becomes important because NIST and other standards bodies have already deprecated these items in their specs and standards.

    During the session several ideas were brought up how the HCD iTC should handle this issue. Ira brought up the suggestion that instead of just removing them the HCD cPP could just indicate via an Application Note that they have been deprecated and should not be used. Al indicated he liked that idea and would bring it to the HCD iTC, but that he would also check to see how the Network Device (ND) iTC was handling this issue.
  - The other big issue that the HCD iTC has to address is updating the specs and standards the SFRs reference. The current thought is that the HCD iTC has to proceed very carefully with this, because updating spec/standard references can have very unintended consequences. For example, updating a spec may require vendors to support a new crypto algorithm they can't implement, or worse no longer support an algorithm or cipher suite that want to support. So, the HCD iTC will probably not update spec/standard referenced in the HCD cPP/SD unless absolutely necessary or are forced to do so by either he Japanese or Korean Schemes.
- Regarding new content, at this point it is unlikely the HCD iTC will include any new SFRs beyond what is already in the pipeline. That especially includes inclusion of support for TLS 1.3. The reason for this is that the HCD iTC does not want to be the first iTC to provide an TLS 1.3 implementation in a cPP, so we are waiting for the ND iTC to implement TLS 1.3 in an update to the ND cPP. However, the ND iTC is still trying to resolve the latest set of comments from the US Scheme against the latest draft TLS 1.3 package and are nowhere near completing that task.

  Ira made an interesting point that several European countries require support for TLS 1.3 and may not accept certification of MFDs that do not support TLS 1.3. He suggested that instead of just stating we support TLS 1.2 we state that we support "TLS 1.2 or later". Again, Al will see how the ND iTC is handling this situation.

  So, at this point the only real reason the HCD iTC would likely consider include any new SFRs is if they are requested by either the Japanese or Korean Schemes (although a request from NIAP (the US Scheme) would be seriously considered also). Any NIAP Technical Decisions against the current HCD PP or against SFRs or Assurance Activities in the ND cPP/SD or FDE EE cPP/SD that we used for the HCD cPP/SD would also have to be incorporated, regardless of what that meant. Finally, the HCD iTC would have to respond to suggestions by JBMIA and changes to ISO or NIST standards and specs.
- Al had prepared an updated schedule in May 2021. After two months it became clear that even this updated schedule needed a revision. Al proposed a new revised schedule that called for the following updated key milestones:

- 1st Public Draft Submitted for Review: Aug 30, 2021
- 2nd Public Draft Submitted for Review: Dec 13, 2021
- Final Draft Submitted for Review: Apr 4, 2022
- Final Documents Published: May 13, 2022

Ira pointed out that the schedule only allowed 10 days for the final update of comments from the review of the Final Draft; he felt that was much too short. Al said he would relook at the Final Draft schedule.

- Al finished the HCD iTC discussion with some additions to the HCD iTC lessons learned he presented at May 2021 IDS Face-to-Face Meeting. These additional lessons learned were:
  - The importance of establishing and maintaining a Work Plan with schedules from the creation of the iTC throughout its lifecycle
  - Make sure every work product an iTC produces is available publicly to every iTC member at all times
  - Make sure the team's rules of operation are written down, well understood by all team members and **followed.** The two times the HCD iTC got in trouble is when we didn't follow our voting rules.
  - Make sure there are minutes for all team meetings; you have no idea how often you need to go back and use minutes from previous meetings to see what was discussed or to avoid arguments as to what happened. Minutes also need to be done in a timely manner

5. Al then briefly went through a presentation he gave at a previous IDS Working Group meeting on the recent Executive Order Improving the Nation's Cybersecurity issued by the White House on May 12, 2021. The reason for discussing the Executive Order was that he felt there were provisions in this document that could have significant impact on the software community because its provisions would apply to any contractor that does business with the Federal Government. Some key topics covered by this Executive Order are:

   - Cybersecurity policy must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).
   - Within 60 days of the date of the Executive Order the Office of Management and Budget, in consultation with other named federal agencies, will make recommendations for contract language changes regarding sharing of threat information among federal agencies.
   - A government contractor that provides software or services would be required to report cyber incidents to the relevant federal agencies based upon a sliding scale of risk assessment, with the highest risk requiring notice within 3 days of discovery.
   - Within 45 days (June 28), Homeland Security, in consultation with other named federal agencies, is directed to recommend changes to the FAR including the nature of the cyber incidents that would require reporting, the government contractors and service providers that would be covered, the time periods for reporting based on "a graduated scale of severity," and "appropriate and effective protections for privacy and civil liberties."

     What is interesting about the Cyber Incident Reporting is that the definition of "incident" that the Executive Order uses is based on the standard security concepts of jeopardizing Confidentiality, Integrity and Availability.
   - The key points in the Enhancing Software Supply Chain Security portion of the Executive Order are:
     - NIST is required to develop and publish guidelines by Nov 8th on how software suppliers are to handle supply chain security. Once NIST issues these guidelines it will be interesting to see what organizations like NIAP do with these guidelines.

- The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices. Al mentioned that Common Criteria might provide a good mechanism for demonstrating this conformance with software practices.
- The guidelines will cover important and familiar security-related issues like (1) multi-factor, risk-based authentication and conditional access; (2) employing encryption for data; (3) ensuring the integrity of the code; (4) check for known and potential vulnerabilities and remediate them; (5) providing a purchaser a Software Bill of Materials (SBOM) for each product; (6) participating in a vulnerability disclosure program that includes a reporting and disclosure process; (7) attesting to conformity with secure software development practices and (8) ensuring integrity and provenance of open-source software used within any portion of a product.

- There are other topics in the Executive Order like establishing a Cyber Safety Review Board and Improving detection of cybersecurity vulnerabilities and incidents on federal government networks. “The devil will be in the details” in terms of how this Executive Order gets implemented over the next several months.

  Towards that end Ira provided a couple of links below on how this Executive Order is actually being implemented:

  - Department of Commerce and NTIA (National Telecommunications and Information Administration) announcement of minimum requirements for Software Bills of Materials (SBOMs) on software deliveries to the government - https://www.ntia.doc.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials
  - NIST announcement of two key publications to enhance software supply chain security called for by May 2021 Executive Order for Cybersecurity - https://www.nist.gov/news-events/news/2021/07/nist-delivers-two-key-publications-enhance-software-supply-chain-security
  - Announcement of NIST recommended minimum standards for vendor or developer verification (testing) of software based on the May 2021 Executive Order for Cybersecurity - https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or

6. Ira then covered the latest status on the HCD Security Guidelines. The latest version from May 2021 can be found at https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20210504.docx. The updates were mainly in Section 4, Network Security and Section 12.2, Datalink Security.

   Ira’s plan is to:

   - Post an Interim Draft in Sep 2021 with additional content in Section 4
   - Post another Interim Draft in Q4 2021 to include content in Section 5 Local Security (OS, Hypervisors, Peripherals, Apps) and Section 6 System Architecture (Firewall, AV, Process Isolation)
   - Post a full Prototype Draft in Q2 2021

   A question was asked whether the guidelines would include content about Bluetooth. Ira indicated that it would, but that it would clearly suggest that Bluetooth not be enables or that it be used as a proxy with no direct access.

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:

   - Nothing really significant was reported regarding TCG standards activities.

- Regarding IETF standards activities, some key items Ira stressed were:
  - There is a new spec on “Secure Negotiation on Incompatible Protocols in TLS” that now is looking at the concept of what protocols are incompatible with an implementation rather that what protocols are compatible with an implementation.
  - The “Hybrid Key Exchange in TLS 1.3” spec is looking at the concept of using multiple cypher suites for key exchange in TLS 1.3.
  - The “Compact TLS 1.3” spec is for TLS 1.3 for computers used in IoT applications like automobiles.
  - The IRTF Crypto Forum Research Group (CFRG) does research on crypto algorithms. Ira noted that this forum is the main forum that provides a window into what is going on within the “university world” in terms of cryptographic research.

8. **Wrap Up**

- Next IDS Conference Call will be on Sep 2, 2021
- Next IDS Face-to-Face Meeting will be during the next PWG Virtual Face-to-Face Meeting November 9-11, 2021

Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 11:55AM ET on August 19, 2021.