IDS Face-to-Face Minutes
August 7, 2024

Meeting was called to order at approximately 10:00 am ET May 8, 2024.

Attendees –

Charles Armstrong	Canon
Matt Glockner	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
Michael Ziler	Microsoft

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2024-08-07-IDS-F2F v1.pdf.

- Minute Taker
    - Alan Sukert taking the minutes.

2. Agenda:
    - Introductions, Agenda Review
    - Discuss status of HCD iTC, HIT and plans for future HCD cPP/HCD SD releases
    - Connectivity Standard Alliance
    - Wrap-Up / Next Steps
3. Alan went quickly through the PWG Antitrust, Intellectual Property and Patent policies.
4. Alan went through the status of the HCD iTC, the HIT and potential content of the next releases of the HCD cPP and HCD SD.

    Some of the key points from the HCD iTC Status discussion were:

    - The Errata – HCD cPP v1.0e and HCD SD v1.0e – was finally published on March 4, 2024. It contained fixes for the following issues:
        - HCD-IT #2
        - HCD-IT #4 – HCD-IT #7
        - HCD-IT #9
        - HCD-IT#12
        - HCD-IT #16
        - HCD-IT #18 – HCD-IT #19
        - HCD-IT #21 & HCD-IT #22

        Slides 10 and 11 provide more detail on these issues.
    - The HCD iTC has now received Endorsement Statements for the HCD cPP v1.0e from the Canadian and Korean Schemes and from NIAP. JISEC (the Japanese Scheme) finally posted its endorsement as part of an updated Position Statement. However, NIAP's endorsement came with the following important caveat:

NIAP's endorsement is a formal statement that products successfully evaluated against the HCD cPP V1.0E that demonstrate exact conformance to the cPP, meeting the below identified conditions, and in compliance with all NIAP policies, will be placed on the NIAP Product Compliant List:

- Each applicable cryptographic support security functional requirement (FCS_) must include at least one selection conforming to Commercial National Security Algorithm (CNSA) Suite V1.0 or V2.0
- SHA-256 may be selected in FCS_PCC_EXT.1 and may be included in FCS_COP.1/Hash and FCS_COP.1/KeyedHash for that function; and
- **SHA-1 may not be selected**

This version succeeds the HCD PP V1.0 **which will sunset effective 23 October 2024**

Slides 8 and 9 provide the list of algorithms that comprise CNSA Suite v1.0 and v2.0.

- From a HCD Interpretation Team (HIT) perspective, now that the Errata has been published the priorities, in order, are:
    - Resolving the remaining Priority 1 Issues
    - Resolving any remaining Priority 2 Issues
    - Assigning priorities to issues with no priority assigned
    - Addressing any new issues that are raised against the Errata

  Slides 15-18 provide a list of the current open Priority 1 issues, open Priority 2 issues and open issues with no assigned priority that the BHIT must resolve.

- The other main topic the HIT will have to decide is whether the HIT will issue any more standalone HCD cPP or HCD SD v1.0.x releases after the Errata release to address the Priority 1 issues at least (or do we pass them on the HCD iTC to include in the next full release of the HCD cPP and HCD SD)

  If the HIT does decide to do standalone releases, how many of these releases will occur likely depends on the comments we get from:
    - The review of the HCD cPP from the other Schemes and
    - Future certifications against HCD cPP v1.0 or HCD SD v1.0 from the applicable Evaluation Lab or applicable Scheme

- Slides 13 – 16 provided details on the remaining Priority 1, Priority 2 and unprioritized issues that the HIT still must process.
- For the HCD iTC itself, the priorities for 2024 (and probably 2025), in order, are:
    a. CC:2022 Transition Policy – Ensuring the HCD cPP and HCD SD are compliant with CC:2022 (CCDB deadline for certifications against prior CC version)
        - A subgroup was formed and is actively working this issue
        - The subgroup developed the following list of items to review:
            - Determine which items in the CC:2022 Errata should be included in the HCD cPP and SD (either v1.0e or v2.0)
            - Determine which new SFRs included in CC:2022 Part 2 should be included in the HCD cPP and create the appropriate Assurance Activities in the HCD SD for these SFRs
            - Determine what changes to SFRs in CC:2022 Part 2 that have counterparts in the HCD cPP should be made in the HCD cPP counterparts

        - Review CC:2022 Parts 3 -5 to determine if any content in these parts should be included in either the HCD cPP or HCD SD
        - Assuring that the HCD SD's requirements for AVA_VAN are consistent with EUCC for AVA_VAN.1 – AVA_Van.3, which are the levels for "Substantial" assurance in the EUCC, is important

      The goal is to determine the minimum changes needed to conform with CC:2022

   b. Syncing with Network Device cPP/SD v3.0
   c. Syncing with the output from the CCDB Crypto Working Group – SFR Catalog planned for release by end of 2024
   d. Implementing HIT Technical Decisions
   e. Implementing AVA_VAN requirements to sync with EUCC
   f. NIAP PQC Requirements (CNSA 2.0) – currently on hold by NIAP
   g. Parking Lot Issues
   h. Any New Issue

- In terms of HCD cPP/SD release planning, the current plan is for the following releases:
    - V2.0 – 2026:
        - Will contain the results from the CCDB Crypto WG's SFR Catalog, Syncing with ND cPP/SD 3.0, and CC:2022 Compliant efforts
    - V3.0 - 2027 – 2028:
        - Will likely contain some CNSA 2.0 components and content from the other priorities
- Al then listed, based on the above HCD-iTC priorities, what Al thought would be the potential content of v2.0:
    - Updates for the relevant changes in CC:2022
    - Incorporate SFRs from the CCDB Specification of Functional Requirements for Cryptography once it is published and we get a transition plan
    - Update for the relevant changes in ND cPP v3.0e
    - Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
        - Standardizing on ND 3.0 Implementation
    - Incorporate the NIAP Functional Package for SSH so can claim conformance to it
    - Inclusion of AVA_VAN to sync with EUCC
    - Incorporate Priority 1 and other HIT Issues into HCD cPP/SD versions
    - Changes due to requests from JISEC, ITSCC, NIAP, Canada and possible other Schemes due to on-going certifications against HCD cPP/SD v1.0e
- The list of changes that could go in V3.0 or later releases is essentially the same as shown in previous sessions with some differences and additions:
    - NTP
    - Full implementation of CNSA 2.0
    - Support for Cloud Printing
    - Incorporate NIAP Functional Package for X.509 when it becomes available
    - Support for post quantum and other new crypto algorithms

  - Any other new NIAP Packages
  - Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, and NIAP TDs
  - Updates to Address 3D printing and the Digital Thread to Additive Manufacturing
  - Support for Artificial Intelligence
  - Support for Wi-Fi
  - Any new CCDB Crypto WG or CCUF Crypto WG Packages or Specifications
  - Support for Security Information and Event Monitoring (SIEM) and related systems
  - Support for SNMPv3
  - Support for NFC
  - Updates based on new technologies, customer requests or government mandates
  - Syncing with Other iTCs such as DSC iTC and FDE iTC
  - Syncing with newer versions of ND cPP/SD
- Key next steps for the HCD iTC are:
  - Continue HIT activities for maintaining HCD cPP/SD v1.0e and issue the necessary TDs/TRs and Errata to address all documented RfIs
  - Complete HCD cPP/SD v1.0e certification by Canadian Scheme
    - Current plan is to be done sometime in Sep 2024
    - Will also include certification of HCD cPP v1.0e
  - Fully engage the HCD iTC to work on HCD cPP v2.0 and HCD SD v2.0
  - Start planning for HCD cPP/SD v3.0 and beyond.

5. Al then presented his special topic for the day, which is a look at the Connectivity Standards Alliance (CSA).

   The reason Al brought up the CSA was that Smith Kennedy mentioned it at a previous IDS WG Meeting and Al was curious what it was and decided to look further into it.

   The key points from Al's search into the CSA are:

- Its mission, as stated on its web site, is to "Ignite creativity and collaboration in the Internet of Things, by developing, evolving, and promoting universal open standards that enable all objects to securely connect and interact. We believe all objects can work together to enhance the way we live, work, and play"

  Smith described the CSA as being like the Linux Foundation or ISTO. It is an umbrella organization over other standards organizations that develop standards for the Internet of Things products.

- CSAs key offerings are in the areas of developing IoT technology standards, certifying IoT products and promoting the benefits of global open standards. See Slide 25 for more information.
- CSA has a certification process shown on Slides 26 and 27 that at a high level is somewhat like the CC process. The main steps in the CSA Certification Process are:
  - Become a member of the CSA
  - Request a Manufacturer ID / Vendor ID
  - Select a Compliant Platform or Network Transport

  - Choose a Testing Provider
  - Send Product to be Tested
  - Submit Certification Application
  - Application Pending
  - Upon Approval
- The rest of the CSA discussion covered the CSA IoT Device Security Specification Version 1.0.
  - This spec was published on March 18, 2024. Smith explained that CSA specs like this one are a type of “umbrella spec” that tries to take the “best practices” from other specs such as ETSI standards for IOT devices (which are not voluntary) or NIST standards (which are voluntary).
  - Its purpose is to “Define the requirements that must be met by devices within the initial scope of this Specification to be certified under the Alliance Product Security certification and define the baseline security threshold requirements for an Alliance-based device security certification program defined by the Alliance that can be used to certify the security of IoT Devices,” meaning that it only applies to IoT products used in smart homes – things such as smart refrigerators.
  - The scope of this spec is for certifying the security of consumer IoT Devices, contemplating the use of each such IoT Device in an IoT System for consumer use in the smart home, to meet the level current as of June 2023 required by:
    - international standards (specifically European Telecommunications Standards Institute (ETSI) EN 303 645 [3] and National Institute of Standards and Technology (NIST) IR 8425 [4]); and
    - regulations (specifically Singapore Cybersecurity Labeling Scheme (CLS) [5]); and
    - the markets

    An important caveat is that the spec does not cover home healthcare products
  - Slides 30-32 provide some key definitions included in the specification. The definitions that Al pointed out during the two meetings were:
    - **Best Practice Cryptography -** Cryptographic Algorithms, modes and protocols, key generation and handling, and random number generation required by any government or regulatory body in the applicable market, or markets, in which the IoT Device is intended to be deployed. The choices may be determined by the need for interoperability as required by established specifications as described in section on Best Practices for Cryptography of the PSWG Assessment Guidance – this term shows up in many of the functional requirements
    - **Critical Security Parameters -** Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs), the disclosure or modification of which can compromise the security of an IoT Device.
    - **Cryptographic Algorithms -** Cryptographic primitives and higher-level algorithms that perform functions essential to maintaining cryptographic security.
    - **IoT Device -** A tangible product, composed of IoT Sub-Components, that comprises at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world. PSWG 1.0 is limited to devices intended principally for consumer use in the home (excluding home healthcare devices).

The interesting part of this definition is that a home printer could be considered an IoT device in this context because it has least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., web interface) for interfacing with the digital world. That could make the spec potentially applicable to HCD devices.

  - **IoT System -** A collection of related IoT System Components, including IoT Devices and IoT Associated Services. There is no assumption in this Specification that all the IoT System Components in an IoT System come from the same vendor.
  - **IoT System Component -** An IoT Device, an IoT Associated Service, or other equipment used to create an IoT System instance. An example of other equipment would include a router.
  - **Security Best Practices -** These are the best practices for IoT Device security:
    - Perform a risk analysis and threat model for the IoT Device in light of the expected usage and target deployment context
    - Identify and classify data storage points and data flow assets, and safeguard assets classified as Sensitive Data in a manner that satisfies some or all of the following: availability, integrity, and confidentiality, as applicable to each asset
    - Select appropriate countermeasures to reduce residual risk to acceptable levels
    - Implement the selected countermeasures.

    It is interesting that threat modeling is included in the best practices
  - **Security-Relevant Information -** Information that could identify the combination of the IoT Device and the version of that IoT Device's software and/or hardware.
  - **Sensitive Data -**Data that is of particular concern from a security perspective, including, by way of example and without limitation: safety- and/or control-related commands/functions or parameters; data strings; data attributes; personal identifiable information; data in memory being used for calculations; credentials; keys; protocol header fields; and intellectual property

- Slides 33-38 contain the set of technical requirements included in the specification which Al went through quickly in most cases. The technical requirements Al spent some time on during the meeting were:
  - The requirements in Slide 33 are generally Configuration Management requirements dealing with items like authentication of changes, secure configuration, and inventory of the system IoT components.
- Slide 34:
  - The "**Security Best Practices**" requirement dealing with passwords includes the typical type of strong password requirements.
  - The mandatory "**Preventing Brute Force Attacks"** requirement was very surprising given that this spec was for IoT products for smart homes. The spec did state that in the future its scope might be extended to more IoT products, but preventing brute force attacks is a rare requirement even for more advanced type of products.
  - The **Changing Authentication Values** mandatory requirement that an IoT Device or some other IoT System Component SHALL include a mechanism for simply changing user authentication value user authentication is used is another rare requirement that is a good requirement,
- Slide 35:

  - Al noted that it was good that the spec included the mandatory **Secure Storage of Persistent Data** to ensure that all Sensitive Data stored persistently on the IoT Device SHALL be stored in a secure manner
  - Al noted that the mandatory **Erasure from Device** requirements are like the Purge requirements that were previously in the HCD PP and earlier versions of the HCD cPP and the FPT_WIPE_EXT SFR that replaced Purge in the HCD cPP v1.0 and v1.0e.
  - Al noted that there was a mandatory **Confidentiality Protection** requirement to ensure the confidentiality of Security-Relevant Information and Sensitive Data exchanged with IoT Devices and IoT Associated Services. However, surprisingly the spec has no mandatory requirement ensuring the integrity of the Security-Relevant Information and Sensitive Data stored persistently on the IoT Device.
- Slide 36:
  - Al noted that it is good that the spec includes the mandatory requirements for (1) disabling all interfaces not necessary for the intended use of the IoT Device, (2) validating data input into the IoT Device via network and any other interfaces against malformed input, and (3) not installing functionality not needed for the intended use of the IoT Device be installed, or disable such functionality where non-installation is not practical
  - Al noted that there is a Secure Boot requirement is like secure boot requirement the HCD cPP v.10e has, although clearly the one for IoT devices is much simpler.

    It was noted that the secure boot requirement in the NIST document is not mandatory, and Al and others at the session thought it should be a mandatory requirement. The same comment was made for the “Least Privilege” requirement.
- Slide 37:
  - Regarding software updates, Al was glad this spec included mandatory requirements to support a software update process and ensure the authenticity and integrity of software updates. Al noted that the requirements around automatic software updates are not mandatory, which given the current state for IoT devices is probably the right thing.
  - It was also good to see the mandatory requirement that software updates for the IoT Device be easy for users to install.
  - Al noted that there was a requirement concerning audit logging of security-relevant events and errors that SHOULD include enough details to determine what happened. Even though it is not a mandatory requirement, the fact an audit log requirement is there at all is what is important. There is also a non-mandatory requirement on Slide 38 to restrict access to audit logs to authorized personnel only, which again is important for the fact that it is there.
- The remaining requirements on Slide 38 are non-mandatory requirements dealing with reporting the current security state, what happens if an unauthorized change to the IoT software is detected by the IoT device, resiliency to power and network outages, and use of isolated processing approaches employing both software-based and hardware-based mechanisms.

Slides 39 – 43 contain the set of non-technical requirements included in the specification which Al also went through quickly in most cases. The non-technical requirements Al spent some time on during the two meetings were:

- Slide 39:
  - Regarding the Design Considerations, just like the Security Best Practices it is interesting that Threat Modeling and Risk Analysis are included as one of the required design considerations.

    - It was good to see that a Secure Development Process Related to IoT Device was one of the required processes, platforms, and tools used to develop the IoT Device.

  - Slide 40:
    - All the mandated components of the Secure Development Process listed on Slide 40 are important.
      - Threat modeling has been a technical requirement throughout the spec.
      - The requirement that the IoT Device Manufacturer must employ a secure engineering approach will be interesting to assess, since the spec does not really define what constitutes a “secure engineering approach.”
      - The inventory of IoT Sub-Components requirement falls in line with the big push by NIST and NIAP in defining HBOMS and SBOMs for systems.
      - Finally, requirements around ensuring secure supply chain are another big initiative within NIST and NIAP right now.
  - Slide 41
    - The vulnerability management requirements are another critical area, especially as they pertain to syncing with EUCC as mentioned above. It is interesting that the requirements around Vulnerability Disclosure (establish, publicize, and implement a vulnerability disclosure process) and Assessment (conduct penetration testing or vulnerability testing) are mandatory, but requirements for Vulnerability Response (continually monitor, identify, and respond in a timely manner to security vulnerabilities) are not.
    - The requirement to provide security updates for vulnerability fixes is mandated, but as Ira always says when you include terms like “timely” assessment becomes subjective at best. Smith commented on that by reminding the group that CSA is an umbrella organization, so standards and specs like this one try to take the best requirements from several regulations such as the two regulations mention in the “Scope” slide. For that reason, requirements in CSA standards and specs do tend to be high level and somewhat subjective.
  - Slide 42:
    - Al noted that the mandatory requirements around Consumer Disclosure (provide information to consumers about what personal data (and telemetry data, if any) is being processed, how it is being used, by whom, and for what purposes) and Consent (Obtain consumer consent for personal data processing in a valid manner) almost seem to be patterned after the EU GDPR regulations.
  - Slide 43:
    - The Minimization requirement to keep data collection to the minimum data necessary for the intended functionality is another good mandatory requirement that was included in the spec.

6. **Wrap Up**
   - The next IDS Working Group Meeting will be on August 22, 2024. Main topics of the meeting will be updated status of the HCD iTC and HIT and a special topic that is currently TBD.
   - Next IDS Face-to-Face Meeting will be during the November 2024 PWG Virtual Face-to-Face Meetings November 12-14, 2024 (likely on November 14, 2024).

   Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 11:00 AM ET on August 7, 2024.