IDS WG Meeting Minutes
July 11 and 25, 2024

These two IDS WG Meetings were started at approximately 3:30 pm EDT on July 11, 2024 and 3:15pm EDT on July 25, 2024.

Attendees – July 11, 2024

Jerry Colungo	HP
Smith Kennedy	HP
Jeremy Leber	Lexmark
Alan Sukert	
Bill Wagner	TIC

Attendees – July 25, 2024

Smith Kennedy	HP
Jeremy Leber	Lexmark
Alan Sukert	
Brian Volkoff	Ricoh

Agenda Items – Both Meetings

1. The topics to be covered during this meeting were:
   - Latest updates on the HCD iTC and HIT
   - Special Topic on Connectivity Standards Alliance (CSA)
2. Both meetings 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 by discussing the results of the HCD iTC and HIT Meetings since the May PWG Virtual Face-to-Face IDS Session on May 8th:
   - The #1 priority for the HCD iTC is to be compliant with the CC:2022 version of the Common Criteria as soon as possible. A subgroup has been formed to address this issue that had its first meeting on July 8th. At that meeting the subgroup listed the following tasks that needed to be done to achieve CC:2022 compliance:
     - Determine which items in the CC:2022 Errata should be included in the HCD cPP and HCD SD.
     - 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.

       One thing to specifically look at are the requirements associated with AVA_VAN because of the extensive use of AVA_VAN in EUCC.
     - Make sure the dependencies in the HCD cPP SFRs are consistent with the dependencies in CC:2022 for SFRs that are in both the HCD cPP and CC:2022.
   - The second priority of the HD iTC is to ensure the HCD cPP/SD are sync'd with ND cPP/SD v3.0e.
   - Kwangwoo Lee is working with the Japanese Scheme to finally get its Endorsement Statement for HCD cPP v1.0e. It will be in the form of an updated Position Statement.

- Another important task is to monitor the efforts by the CCDB and CCMC to establish mutual recognition with EUCC. This is time-critical given that EUCC will be formally implemented within the EU starting in Feb 2025, at which any product certifications in the EU will have to be done against the EUCC requirements.

  EUCC places a heavy emphasis on AVA-VUN (Vulnerability Assessment) as part of its evaluation activities, so that is one area the HCD cPP/SD must be sure it is in sync with EUCC. Establishing mutual recognition by Feb 2025 will be very difficult because of the EUCC requirements governing mutual recognition and the relatively short transition time.

- Regarding the HCD cPP v1.0e certification, the Lexmark MFD certification by the Canadian Scheme is progressing on schedule and should be done sometime around the end of August or early September. When the MFP certification is completed, the certification of the HCD cPP v1.0e that the MFD was certified against will follow shortly after.

- HIT Status:

  - The main issue the HIT is focusing on is HIT-IT #25: RFI on SBT_EXT_EXT.1 Root of Trust - immutability and valid protection mechanisms. The issue is:

    FPT_SBT_EXT.1 states that Root of Trust is implemented in immutable code or a HW-based write-protection mechanism. HCD cPP provides no further description or additional detail on the definition for the Root of Trust in terms of its protection. “Appendix G: Glossary” also fails to provide further information on this matter.

    SD includes a requirement that the TSS shall describe how the Root of Trust is immutable. However, HCD cPP is not clear on how the immutable code or HW-based write-protection is defined. The SD does not provide clear guidance on the level of assurance the evaluator shall take into consideration to confirm a compliant Root of Trust protection mechanism.

    The discussion initially centered around a definition of what is immutability in this context. The HIT decided to use the definition of immutability from NIST SP 800-193. A Technical Recommendation (TR) has been created in GitHub by the HIT for this immutability definition to be eventually submitted after HIT approval to the full iTC for consideration.

    Discussions on the other aspects of this issue are continuing in the HIT. HCD-IT #25 is the HIT’s #1 priority.

  - There are two new issues the HIT is processing:

    a. HCD-ITC-Template #361 - Multiple immutable roots of trust

       Would it be acceptable to have multiple immutable roots of trust, any one of which could be used to verify firmware integrity?

       For example, in one-time programmable effuses, we would have:

       - RSA public key 1
       - RSA public key ..
       - RSA public key n
       - LMS/XMSS public key 1
       - LMS/XMSS public key ..
       - LMS/XMSS public key n
       - which algorithm to use

       The "which algorithm to use" value would determine whether to use RSA or LMS/XMSS for the firmware signature verification. We would try each public key for that algorithm and proceed if any one successfully verifies the signature.

We would invalidate keys in the field by remotely zeroing them out. According to the proposed solution for issue #25, "making changes" to the root of trust would require "manufacturing or service tools directly connected to a locally(physically) present platform or device" (i.e. not remote), but this implementation would not be "making changes" to the root of trust, per se, but rather switching from one truly immutable root of trust to another.

b. HCD-ITC-Template #360 FCS_IPSEC_EXT.1.10 RFI

Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:
a. Test 1: If the first selection is chosen, the evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this cPP is used, and that the length of the nonces meet the stipulations in the requirement.
b. Test 2: If the second selection is chosen, the evaluator shall check to ensure that, for each PRF hash supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this cPP is used, and that the length of the nonces meet the stipulations in the requirement.

Issue:
Tests 1 and 2 appear to be TSS requirements rather than testing activities.

- The rest of the meeting was some general information. For example, Ohya-san is the new chair of the JBMIA.

4. Al then presented his special topic for the day, which is a look at the Connectivity Standards Alliance (CSA). The slides for this special topic can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/CSA.pdf. The special topic covered most of the time at both the July 11th and July 25th meetings.

   The reason Al brought up the CSA was that Smith Kennedy mentioned it at a previous IDS 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 2 for more information.
   - CSA has a certification process shown on Slides 4 and 5 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 8-10 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
- **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 11-16 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 two meetings were:
  - The requirements in Slide 11 are generally Configuration Management requirements dealing with items like authentication of changes, secure configuration, and inventory of the system IoT components.
  - 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.
  - 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.
  - 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 mandatory Secure Boot requirement just like the HCD cPP v.10e has, although clearly the one for IoT device sis much simpler.
- Regarding software updates, Al was glad this spec included the 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 to see the mandatory requirement that software updates for the IoT Device are to 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 that it is there at all is what is important. There is also a non-mandatory requirement to restrict access to audit logs to authorized personnel only which again is important for the fact that it is there.
- The remaining requirements of Slide 16 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 17 – 21 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:
  - 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.
  - All the mandated components of the Secure Development Process listed on Slide 18 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.
  - The vulnerability management requirements on Slide 19 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.

- 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.
- Finally, the Minimization requirement to keep data collection to the minimum data necessary for the intended functionality is another good requirement that was included in the spec.

5. **Actions:** None

Next Steps

The next IDS Meeting will be the IDS Session at the August PWG Face-to-Face Meetings scheduled for Wednesday, August 7th at 10:00 EDT.

The next IDS WG Meeting will be on August 22nd at the normal time of 3:00 PM EDT / 12:00 Noon PDT.