IDS WG Meeting Minutes
March 31, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on March 31, 2022.

Attendees

Graydon Dodson	Lexmark
Erin Huber	Xerox
Smith Kennedy	HP
Ira McDonald	High North
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 Meetings since our last IDS WG Meeting on 3/3/22
   - Quick status of the HCD Security Guidelines
   - Presentation by Al Sukert on NIST SP 800-203A, IoT Device Cybersecurity Guidance for the Federal Government: *IoT Device Cybersecurity Requirement Catalog*
   - 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 then provided a summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 3/3/22.
   - Much of the time has been spent at the HCD iTC meetings since the last IDS WG Meeting reviewing comments against the 2nd Public Drafts of the HCD collaborative Protection Profile (cPP) and Supporting Document (SD), although comments against the 2nd Public Draft of the HCD SD are not due to the HCD iTC until April 15th.
   - The main issue covered by the HCD iTC over the past month has been finalizing the new FPT_WIPE_EXT SFR and its associated Assurance Activities (AAs). The FPT_WIPE_EXT SFR and AAs have undergone several revisions, both internally by the subgroup that created this SFR and AAs and because of comments raised by members of the HCD iTC. The last comment against the FPT_WIPE_EXT SFR and AAs came from Kwangwoo Lee who was concerned about how the SFR and AAs would handle the case where an HDD was divided into partitions and User and TSF data was only stored in certain partitions while other partitions contained code. The non-data partitions could not be wiped because then the HCD could not be booted.

     The HCD iTC determined a way to address the partitioning issue by modifying the AAs to accommodate partitioning. At that point the HCD iTC thought we had a final solution to the FPT_WIPE_EXT SFR. However, this past week ITSSC (the Korean Scheme) submitted a set of comments against this latest version of the FPT_WIPE_EXT SFR and AAs which the HCD iTC will review at its next meeting on 4/4.
   - Kwangwoo Lee spent the last part of the 3/28 Meeting reviewing the updated HCD iTC Work Plan. Since the HCD cPP 2nd Public Draft was released n 12/14/21 and comments were received by 1/31/22 while the HCD SD 2nd Public Draft was just released on 2/24/22 and the comments are due yet to 4/15, Kwangwoo feels that schedule should be linked to the HCD SD schedule at this point. So, the updated HCD iTC Work Plan is as follows:

- Review comments and update HCD cPP and HCD SD: 4/15 – 5/13
- Submit Final Draft of HCD cPP and HCD SD: 5/16
- Review HCD cPP/SD Final Drafts: 5/17 – 6/20
- Review comments against HCD cPP/SD Final Drafts and update documents: 6/21 – 6/30
- Publish HCD cPP v1.0 and HCD SD v1.0: 7/5/22

Ira mentioned that the Network Device iTC was planning to release its next update in June 2022; it also had agreed to not implement TLS 1.1 and require TLS 1.3. Al indicated that a recent meeting Kwangwoo Lee had indicated that as of now TLS 1.3 was not going to be in HCD cPP/SD v1.0 because it was too late to intersect the schedule. **Side Note not discussed at the IDS Meeting: With the new HCD iTC schedule it may now be possible to include TLS 1.3 if we can get a final version of it from the ND iTC by 5/1**.

Steve asked about the issue of NIAP Policy 5. Al responded that the current status is that since NIAP is not a sponsor Policy 5 doesn't apply so the certification sponsor or the crypto module supplier will have to perform the necessary crypto testing that would have been covered by the CAVP certificate. However, NIAP indicated they will provide a Position Statement once the HCD cPP is published. If NIAP approves the HCD cPP and allows HCDs certified against the HCD cPP to appear on the NIAP PCL, they may allow Policy 5 to be applied in those instances. Al indicated he would broach that issue with Jon Rolf, the new NIAP Director.

4. Ira indicated that is trying to have an update to the HCD Security Guidelines for the May PWG IDS Face-to-Face Meeting.
5. Al then went through a presentation he put together on NIST SP 800-203A, IoT Device Cybersecurity Guidance for the Federal Government: *IoT Device Cybersecurity Requirement Catalog*; IOT Device Cybersecurity Requirements Catalog provides a link to NIST SP 800-203A. The presentation slides are located at https://ftp.pwg.org/pub/pwg/ids/Presentation/NIST SP 800-203A.pdf. This NIST SP is a direct result of the Cybersecurity Executive Order 2021-14028 issued May 12, 2021.

   One of the subjects of this Executive Order was "*Enhancing Software Supply Chain Security*" which included the following request:

   - Includes the requirement that NIST shall initiate pilot programs to educate the public on the security capabilities of software development practices and Internet of Things (IoT) devices. As part of implementing that pilot NIST published two guidance documents relating to IoT devices in November:
     - Guidance relating to Establishing IoT Device Cybersecurity Requirements (NIST Special Publication (SP) 800-213) and
     - A revised IOT Device Cybersecurity Requirements Catalog (NIST SP 800-213A).

     The publications are targeted to information security professionals, system administrators, and others in organizations tasked with assessing, applying, and maintaining security on a system
   - The purpose of NIST SP 800-203A is to help Federal Organizations determine device cybersecurity requirements for IoT devices they seek to use with federal information systems and other systems operated by the federal government.

     A couple of important definitions:

     - IoT devices in-scope for NIST SP 800-203A have 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, Long-term Evolution (LTE), Zigbee, Ultra-Wideband (UWB)) for interfacing with the digital world. They can function on their own, although they may be dependent on specific other devices (e.g., an IoT hub) or systems (e.g., a cloud) for some functionality

  - Device cybersecurity requirements are device cybersecurity capabilities and non-technical supporting capabilities needed to integrate an IoT device into a system.
  - Device cybersecurity capabilities are cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software)
- NIST SP 800-213A defines a set of 7 device cybersecurity "capabilities". Each capability contains one or more :sub-capabilities" and each sub-capability can contain one or more requirements that may be necessary to achieve that sub-capability. It is important to stress that NIST SP 800-203A provides a catalog of potential requirements that a Federal Agency can require an IoT device under that Agency's purview to meet. However, NIST SP 800-203A is a guidance document and not a standard, so nothing in the document is required.
- The 7 Device Cybersecurity capabilities specified in NIST SP 800-203A are:
  - **Device Identification:** The capability to identify the IoT device for multiple purposes and in multiple ways to meet organizational requirements
  - **Device Configuration:** The capability to configure the IoT device through logical and/or physical interfaces to meet organizational requirements
  - **Data Protection:** The capability to protect IoT device data to meet organizational requirements
  - **Logical Access to Interfaces:** Ability to require authentication to, and/or identification of, the IoT device, and to establish authentication and identification configuration and display requirements
  - **Software Update:** Ability to update IoT device software, and to have support mechanisms for such updates
  - **Cybersecurity State Awareness:** The capability to generate data indicating different types of events related to the use of the device to meet organizational requirements
  - **Device Security** - The capability to secure the IoT device to meet organizational requirements
- Al went through the sub-capabilities of each of the seven Device Cybersecurity capabilities and then quickly went through the "Requirements that may be necessary" for each of the sub-capabilities. Some of the key points from the discussion were:
  - The sub-categories for the **Device Identification** capability are:
    - **Identifier Management Support** - Ability for device identification. Requirements dealt with identification of the device.
    - **Device Authentication Support** - Ability to support local or interfaced device authentication. Requirements dealt with ability to support differentiation between authorized and non-authorized users and entities.
    - **Actions Based on Device Identity** - Ability to perform actions that can occur based on or using the identity of the device. Was interesting that a requirement was included to verify the identity of other devices as well as the IoT device to identify itself as an authorized entity to other devices.
    - **Physical Identifiers** - Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access. No requirements were identified for this sub-category.
  - The sub-categories for the **Device Configuration** capability are:
    - **Logical Access Privilege Configuration** - Ability for only authorized entities (e.g., organization personnel, other system elements, enabling systems) to apply logical access privilege settings within the IoT device and configure logical access privilege as

described in Logical Access to Interfaces. No requirements were identified for this sub-category.

  - **Authentication and Authorization** Configuration - Ability for only authorized entities to configure IoT device authentication policies and limitations as described in Logical Access to Interfaces. No requirements were identified for this sub-category.
  - **Interface Configuration** - Ability for only authorized entities to configure aspects related to the device's interfaces as described in Logical Access to Interfaces. No requirements were identified for this sub-category.
  - **Display Configuration** - Ability to configure content to be displayed on a device. There were a lot of requirements for this sub-capability, all related to setting, changing, and restoring device configuration settings. It was interesting that one requirement was the "ability for authorized entities to configure the cryptography use itself, such as choosing a key length"; that is something HCDs do now.

- The sub-categories for the **Device Configuration** capability are:
  - **Logical Access Privilege Configuration** - Ability for only authorized entities (e.g., organization personnel, other system elements, enabling systems) to apply logical access privilege settings within the IoT device and configure logical access privilege as described in Logical Access to Interfaces. No requirements were identified for this sub-category.
  - **Authentication and Authorization** Configuration - Ability for only authorized entities to configure IoT device authentication policies and limitations as described in Logical Access to Interfaces. No requirements were identified for this sub-category.
  - **Interface Configuration** - Ability for only authorized entities to configure aspects related to the device's interfaces as described in Logical Access to Interfaces. No requirements were identified for this sub-category.
  - **Display Configuration** - Ability to configure content to be displayed on a device. There were a lot of requirements for this sub-capability, all related to setting, changing, and restoring device configuration settings. It was interesting that one requirement was the "ability for authorized entities to configure the cryptography use itself, such as choosing a key length"; that is something HCDs do now.
- The sub-categories for the **Data Protection** capability are:
  - **Cryptography Capabilities and Support** - Ability for the IoT device to use cryptography for data protection. The requirements for this sub-category are ones you would expect - execute cryptographic mechanisms of appropriate strength and performance, obtain and validate certificates, verify digital signatures, run hashing algorithms and perform authenticated encryption algorithms.
  - **Cryptographic Key Management** - Ability to manage cryptographic keys securely. Like the sub-category above, the requirements for this sub-category are the standards one you would expect for key management - generate key pairs, store encryption keys securely, change keys securely, and maintain exclusive control of cryptographic keys when used by external systems. However, there is no requirement associated with destruction of keys.
  - **Secure Storage** - Ability for the IoT device, or tools used through the IoT device interface, to enable secure device storage. The requirements for this sub-category deal with secure storage of data at rest on the IoT, support for encryption of data at rest, securely back-up the data on the IoT device and "sanitize" or "purge" specific or all data in the device. Note the "purge" issue is the same one that the HCD iTC is dealing with as discussed above.

  - **Secure Transmission** - Ability to secure data transmissions sent to and from the IoT device. Requirements for this sub-category deal with configuring cryptographic algorithm to protect data in transit, use cryptographic means to validate the integrity of data transmitted (a requirement in the HCD cPP) and using organization-internal normalized formats to protect the data it transmits.

- The sub-categories for the **Logical Access to Interfaces** capability are:
  - **Authentication Support** - Ability to support authentication methods. Requirements for this subcategory deal with support for authentication connecting to the device, remote authentication and use of "authentication method(s) through an out of band path" such as biometrics and Third-party credential checks.
  - **Authentication Configuration** - Ability to require, or not require, authentication to, and/or identification of, the IoT device, and to establish authentication and identification configuration and display requirements. Requirements for this subcategory deal with
  - **System Use Notification Support** - Ability to support system use notifications. Requirements for this subcategory deal with providing messages/banners of successful authentication displayed on the IoT device display until actively acknowledged by the user.
  - **Authorization Support** - Ability to restrict all unauthorized interactions. Requirements for this subcategory deal with identifying authorized users and processes and differentiating between authorized and unauthorized users (both physical and remote).
  - **Authentication & Identity Management** - Ability to establish access to the IoT device to perform organizationally-defined user actions without identification or authentication. No requirements were identified for this sub-category.
  - **Role Support & Management** - Ability to establish unique, privileged, organization-wide, and other types of IoT device user accounts. Requirements for this subcategory deal with access control similar to the access control requirements for HCDs. Al noted in the discussion that the requirements seemed to clearly point to Role-Based Access Control as the preferred access control method.
  - **Limitations on Device Usage** - Ability to establish restrictions for how the device can be used. Requirements for this subcategory deal with limits on concurrent device sessions based on roles, user accounts and other criteria.
  - **External Connections** - Ability to support external connections. Requirements for this subcategory deal with interactions and information sharing with external systems over secure connections to ensure security requirements are met.
  - **Interface Control** - Ability to establish controls for the connections made to the IoT device. The many requirements for this subcategory deal with external interfaces and technologies to an IoT. This sub-category led to an interesting discussion as to whether the writers of this NIST document "knew what they were writing about", especially in the area of communication technologies. Al also commented that wireless requirements was something that the HCD iTC was going to have to include in future versions of the HCD cPP.

- The sub-categories for the **Software Update** capability are:
  - **Update Capabilities** - Ability to update the IoT device software within the device and/or through the IoT device interface. Requirements for this subcategory deal with the secure update of IoT software/firmware, the same as for HCDs. For example, update the software by authorized entities only using a secure and configurable mechanism, restrict software installations to only authorized individuals or processes and verify software updates come from valid sources using an effective method (e.g., digital signatures, checksums, certificate validation, etc.). One of the requirements is the "Ability for

authorized entities to roll back updated software to a previous version (i.e., uninstall an update)". Ira pointed out that this "rollback" requirement would be illegal in Japan and in Europe. Finally, one of the requirements for this sub-capability was "Ability to execute the software update mechanism with fault tolerance such that a failed or interrupted update does not degrade the IoT device's cybersecurity state"; Al noted that the concept of Fault Tolerance was something that maybe should be looked at for HCDs in future versions of the HCD cPP when the field is more mainstream. Ira indicated that this was just a form of "resilience".

  - **Update Application Support** – Ability to update the device's software through remote (e.g., network download) and/or local (e.g., removable media) means. Requirements for this subcategory deal with verifying and authenticating a remote update before installing it and setting update mechanisms functions (e.g., download, installation) to be either automatically or manually initiated for remote updates.

- The sub-categories for the **Cybersecurity State Awareness** capability are:

  - **Access to Event Information** – Ability to access IoT device state information. Requirements for this subcategory deal with accessing information about the IoT device's cybersecurity state and other necessary data and preserving the IoT state information.

  - **Event Identification & Monitoring** – Ability to provide event identification and monitoring capabilities and/or support event identification and monitoring tools interfacing with the device. Requirements for this subcategory deal with identifying cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device and other events for purposes of auditing and for monitoring user sessions and communications traffic.

  - **Event Response** – Ability for the device to respond to organizationally-defined cybersecurity events in an organizationally-defined way. There are several requirements all around generating alerts for specific events, event responses and handling audit failures.

  - **Logging Capture & Trigger Support** – Ability for the device, or an interfaced system, to generate, store, retain, delete, and report on specific device audit events, to run specific audit checks, and report findings in a variety of ways. Requirements for this subcategory deal with capturing information from organizationally-defined cybersecurity events (e.g., cybersecurity state, time) through organizationally-defined means and creating audit logs within the device for organizationally-defined and auditable events.

  - **Support of Required Data Logging** – Ability for the device to capture required information in audit logs. Requirements for this subcategory deal with tracking users interacting with the device, the time they interacted with the device, the time the user logged out of the device, and to list this information in an audit log. A; noted that some of the required information to be tracked, like the outcome of the event, goes well beyond anything that would be tracked for an HCD and, as Ira pointed out, probably would not even be known for most IoTs.

  - **Audit Log Storage & Retention** – Ability to maintain audit logs in accordance with organizational policy. Requirements for this subcategory deal with compliance with organization policies with respect to audit log size, retention and deletion. Al noted that the requirement "Ability to send alerts that the logs are too big for the device to continue to store" is a requirement in the HCD cPP.

  - **Support for Reliable Time** – Ability to use timestamps to record the time an auditing event occurred**.** Requirements for this subcategory deal with having valid timestamps that are compatible with Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) (essentially the same as the FPT_STM.1 SFR in the HCD cPP).

  - **Audit Support & Protection** – Ability for the device to support and protect audit activities and associated data. Requirements for this subcategory deal with ability to send requested audit logs to an external audit process or information system, ability to protect the audit information through the use of encryption and digital signing and ability to prevent any entities from editing audit logs unless the entity is authorized, all requirements that are included in the HCD cPP. Note that this last requirement also includes the requirement to "maintaining the audit logs".
  - **State Awareness Support** – Ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state. No requirements were identified for this sub-category.

- The sub-categories for the **Device Security** capability are:
  - **Secure Execution** – Ability to protect the execution of code on the device. Requirements for this subcategory deal with enforcing organizationally-defined execution policies with respect to executing code and IoT process execution, and levels of IoT device and device user functionality. Ira noted that most of the requirements in this and the other **Device Security** subcategories are well beyond the capability of most IoTs.
  - **Secure Communication** – Ability to securely initiate and terminate communications with other devices. Requirements for this subcategory deal with establishing and terminating secure network communication channels. Ira pointed out that IoTs will almost never interface with Domain Name System/Domain Name System Security Extensions (DNS/DNSSEC) for example.
  - **Secure Resource Usage** – Ability to securely utilize system resources and memory. Requirements for this subcategory deal with supporting shared system resources, providing sufficient resources to store and run the operating environment and use or enforcing hardware-based, write protect to protect certain software/firmware.
  - **Device Integrity** – Ability to protect against unauthorized changes to hardware and software. Requirements for this subcategory deal with performing security compliance checks on system components, detecting unauthorized hardware and software components and other tampering with the IoT device when used or being developed and taking organizationally-defined actions when unauthorized hardware and software components are detected.
  - **Secure Network Onboarding Support** – Ability to use secure network onboarding technologies to connect to the network. Requirements for this subcategory deal with the ability for the IoT device to provide necessary data and/or perform necessary functions to participate in the device-to-network authentication, including identifying and recognizing the network; receiving, storing, and/or using secure network credentials and restricting communications to only authorized entities.
  - **Secure Device Operation** – Ability to operate securely and safely. Requirements for this subcategory deal with the ability to support various modes of IoT device operation with more restrictive operational states such as a "safe mode" and restricting components/features of the IoT device (e.g., ports, functions, protocols, services, etc.) in accordance with organizationally-defined policies. Al noted this last requirement is similar to restricting ports in HCDs.

- NIST SP 800-203A also has a Non-Technical Supporting Capability Catalog that consists of the following categories:
  - **Documentation:** The ability for the manufacturer and/or the manufacturer's supporting entity, to create, gather, disseminate, and store information relevant to cybersecurity of the IoT device prior to customer purchase, and throughout the development of a device and its subsequent lifecycle

  - **Information And Query Reception -** The ability for the manufacturer and/or supporting entity to receive from the customer information and queries related to cybersecurity of the IoT device
  - **Information Dissemination -** The ability for the manufacturer and/or supporting entity to broadcast and distribute information related to cybersecurity of the IoT device
  - **Education and Awareness -** The ability for the manufacturer and/or supporting entity to create awareness of, and educate IoT device customers about, cybersecurity-related information, considerations, features, and other information related to reducing the risks created by the IoT device being implemented within the IoT customer's digital ecosystem

- As a last topic for this topic, Al mentioned that two years ago Al had given a presentation at an IDS WG Meeting on essentially the EU version of this document - ETSI EN 303 645 V2.1.1 (2020-06) Cyber Security for Consumer Internet of Things. Al decided to do a comparison between the Categories of the NIST and EU documents to see what the similarities and differences were. The table below was generated to show the comparison.

Requirements Category	NIST SP 800-203A	ETSI EN 303 645
Device Identification	Yes	No
Device Configuration	Yes	No
Data Protection	Yes[1]	Yes[2]
Logical Access to Interfaces	Yes	No
Software Update	Yes	Yes
Cybersecurity State Awareness	Yes	No
Device Security	Yes	No
Password	Yes	Yes
Vulnerability Management	No	Yes
Secure Parameter Storage[2]	Yes	Yes
Secure Communication[2]	Yes	Yes
Minimize Attack Surface	No	Yes
Software Integrity	No	Yes
Securing Personal Data	Yes[1]	Yes
System Resiliency (Availability)	No	Yes
System Telemetry Data	No	Yes
Data Deletion	No	Yes
Installation and Maintenance	Yes[3]	Yes
Input Data Validation	No	Yes
Data (Privacy) Protection	No	Yes

[3]Covered by Documentation requirements

Al's general observation was that the EU document was more focused on privacy, protecting personal data (not surprising given how important GDPR is in Europe) and the integrity and availability of the software while the NIST document appeared to be more focused on protecting the IoT device itself, its configuration and its interfaces. Given that there are other

NIST SPs that cover Vulnerability Management and Passwords that does factor into this comparison.

6. Round Table:

   There are a lot of important meetings and events coming up in the near future:

   - IACR Real World Crypto Conference, April 13-15. Is Hybrid.
   - Spring 2022 CCDB (Common Criteria Development Board) Meeting, May 17-19. Will be virtual
   - Spring 2022 CCUF (Common Criteria Users Forum) Workshop, May 18-19. Will be virtual. Note: This conflicts with the May PWG Virtual Face-to-Face Meetings; to allow Awl's participation at the CCUF Workshop the IDS Session at the May PWG F2F will be on May 19 at 12:45 PM
   - ISO Spring 2022 Meeting, April 4-7. Will be virtual
   - CCUF Management Group elections, May 25-31, 2022
   - 2022 International Conference on the EU Cybersecurity Act, May 24-25 in Brussels, Belgium. Will be In-Person
   - RSA 2022, June 6-9 in San Francisco, CA. Will be In-Person
   - 2022 International Cryptographic Module Conference (ICMC), Sep 14-16 in Arlington VA. Will be In-Person
   - ISO Fall 2022 Meeting, TBD. Unknown if will be In Person or Hybrid
   - Fall 2022 CCDB Meeting, Nov TBD (probably around ICCC and most likely in Toledo Spain). Unknown if will be In Person or Hybrid
   - Fall 2022 CCUF Workshop, Nov TBD (from past experience it will likely be Nov 10-14 in Toledo Spain). Unknown if will be In Person or Hybrid
   - 2022 International Common Criteria Conference (ICCC), Nov 15-17 in Toledo Spain. Will be In-Person

7. **Actions:** None

Next Steps

- The next IDS WG Meeting will be April 14, 2022 at 3:00P ET / 12:00N PT. Main topics will be review of the 4/4 and 4/11 HCD iTC Meetings, possibly a special topic and round table.