IDS Face-to-Face Minutes
August 19, 2020

Meeting was called to order at approximately 10:00 am ET August 19, 2020.

Attendees –

Amitha	Konica Minolta
Gerardo Colunga	HP
Graydon Dodson	Lexmark
Hiroki Ikau	Konica Minolta
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Marc Muldas	Konica Minolta
Alan Sukert	Xerox
Michael Rhines	Qualcomm
Anthony Suarez	Kyocera
Michael Sweet	Lakeside Robotics
Bill Wagner	TIC
Uli Wehner	
Steve Young	Canon

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2020-08-19-IDS-F2F.pdf.

- Minute Taker
  - Alan Sukert taking the minutes

2. Agenda:
   - Introductions, Agenda Review
   - Discuss results of latest Hardcopy (HCD) international Technical Community (iTC) Meetings and potential HCD collaborative Protection Profile (cPP) v1.0 content
   - Review of new ETSI IoT Security Standard
   - HCD Security Guidelines 1.0 Status
   - Status of other HCD Security Standards Efforts
   - Wrap-Up / Next Steps
3. Went through the PWG Intellectual Property policy.
4. Went through the minutes of the HCD iTC meetings held on 5/28/2020, 6/11/2020, 6/25/2020, 7/9/2020, 7/23/2020 and 8/6/2020. Some of the key points from this discussion were:
   - Al went through the current status of the HCD cPP and HCD Supporting Document (SD). The first internal draft of the HCD cPP was sent out for HCD iTC review on 7/21 and comments were due on 8/15. This initial draft contained the following content:
     - o HCD PP v1.0 as approved by NIAP and JISEC
     - o HCD PP Errata #1 created by JISEC
     - o All NIAP Technical Decisions against the HCD PP as of 7/21/2020
     - o All changes to HCD PP v1.0 approved by the HCD Technical Committee before it became the HCD iTC

     We received 46 comments against the HCD cPP draft.

Al then went through the process that will be used to review the comments received against both the HCD cPP and HCD SD. Essentially, the process involves the following steps:

a. We use GitHub to post the drafts that are reviewed.
b. Reviewers use the GitHub “Issues” feature to post their comments.
c. A sanity check is performed by one of the Editors on each comment just to make sure it is a valid comment.
d. Once the sanity check is performed the comment is entered on a master spreadsheet.
e. The comments are then individually triaged by the HCD iTC Chair and Editors. The triage could result in the comment being immediately assigned to an editor to address if the comment is such that it does not require additional iTC action.
   However, some comments may have to be brought to the full HCD iTC for discussion, and if a consensus cannot be achieved, a vote using the voting process per the HCD iTC Terms of Reference document. Once the decision is made the Editors will implement the decision.

- Al then discussed the issue that encompassed most of the HCD iTC meetings since the last IDS Face-to-face. The details of this issue can be found in the IDS Conference Call minutes for the meetings between 6/11/2020 and 7/23/2020 so they won’t be repeated here. In general, the issue was what Conformance Claim would be use for the HCD cPP. It basically came down to two options:

  - Option 1: No EAL Claim but include Security Assurance Requirements (SARs) for EAL2
  - Option 4: No EAL Claim but include SARs for EAL1

  Option 4 is what the current HCD PP has as its Conformance Claim as well as the Network Device cPP. The push for Option 1 was because many European countries require EAL2 certifications which forced some vendors to do multiple certifications – one against the HCD PP so they could get on NIAPs Product Compliant List and one against an older PP that had an EAL2 Conformance Compliance so they could meet the European requirements. Jerry Colunga noted that EAL claims are allowed in Conformance Claims but the problem is that NISAP will not approve any cPP that has an EAL Conformance Claim, and NIAP approval of HCD cPP v1.0 is something that is essential.

  After two months of discussion the iTC could not reach a consensus so we put it up to a vote, with each organization only having one vote. Of the 31 organizations that were represented on the HCD iTC, 22 voted and the final tally was:
  Option 1: 7
  Option 4: 15
  So, Option 4 was the one we went forward with.

- Al then went through the current planned timetable for the HCD cPP/SD. The plan is very aggressive, but the key milestones are:

  - Second internal draft for the HCD iTC for review on 10/20/2020; internal reviews completed by 11/16/2020
  - First public review draft available for public review on 2/1/21; public review completed by 3/19/21
  - Second public review draft available for public review on 5/17/21; public review completed by 7/1/21
  - Final draft available for public review on 8/28/21; public review completed by 9/30/21
  - Publishing of HCD cPP/SD v1.0 by Thanksgiving 2021

  Al noted that the HCD SD first draft was delayed because of the time to get the decision of the Conformance Claim, so it is running about 2 weeks behind the HCD cPP on the above schedule.

- Al finish this part of the agenda with his continuing thoughts on what should go into HCD cPP v1.0 beyond what is now in the first HCD cPP draft. Al’s view was that HCD cPP v1.0 should contain the following additional SFRs:

- Split TLS (and maybe SSH) requirements into separate server and client requirements
- Reflect any new NIAP/JISEC Technical Decisions
- Support for FIPS 140-3
- Removal of all SHA-1 support
- Removal of support for TLS 1.0 and TLS 1.1
- Support for TLS 1.3 (If requirements are included in ND cPP/SD in time)
- Anything that the HCD iTC as a group determines over the next 6-9 months is an "absolute must have" in v1.0; anything less has to go in v1.1 or later. Possible candidates include:
    - Expansion of network-fax separation to "no bridging"
    - Syncing with ENISA and the new proposed European cybersecurity certification scheme (EUCC)
    - Syncing with applicable updates to ND cPP and FDE cPP
    - Syncing with any applicable NIST SP updates

One comment was around inclusion of the Inclusion of ALC_FLR (Flaw Remediation). The problem is that NIAP will not accept Flaw Remediation unless the assurance activities for ALC_FLR are changed to meet NIAP's requirements of them being "achievable", "repeatable", "testable" & "consistent", Ira noted that the Mobile Device iTC is looking into including ALC_FLR into their cPP, so we should follow what they are doing.

Al next briefly went through the review the IDS did of the new ETSI EN 303 645 V2.1.1 (2020-06) Cyber Security for Consumer Internet of Things Standard. The full standard is included below:

en_303645v020101p-1.pdf

The scope of the standard is Consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and was meant for consumer devices like smartphones, TVs, smart appliances, etc.

However, the definition of Consumer IoT consumer IoT device in the standard is a "network-connected (and network-connectable) device that has relationships to associated services and are used by the consumer typically in the home or as electronic wearables". A single function printer or MFP that is designed and sold strictly for home use (and many printer vendors do sell printers of that type) would meet that definition and could be classified by someone as a Consumer IoT product so this standard could be made to apply. So, going through the standard was not considered a waste of time.

The meeting slides provide a summary of some of the key requirements in each of x Requirements Categories of the standards. A couple of the more interesting requirements pointed out at the meeting were:

- Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user
- There were many requirements involving constrained devices. This standard defined a constrained device as "device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use"

- There were many software upgrade requirements, more than any other category, that seemed to be patterned after the Microsoft type of upgrade model. Requirements like:
  - Automatic mechanisms should be used for software updates.
  - The device should check after initialization, and then periodically, whether security updates are available.
  - The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update
  - The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period
- Hard-coded critical security parameters in device software source code shall not be used (this one should be a "shall": for every HCD development)
- Cryptographic algorithms and primitives should be updateable ("cryptoagility") – didn't know about "cryptoagility" until this standard
- Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage – there were a lot of requirements that used vague terminology like "appropriate to the properties of the technology, risk and usage"; we speculated lawyers will have a field day with showing compliance phrases like that
- The consumer IoT device should verify its software using secure boot mechanisms – interesting that this new concept of boot security made its way into the standard
- Several data protection requirements reflect the influence of GDPR
- Finally, liked the Installation and Maintenance requirements, even though they were not "shalls", because they were the right things to suggest:
  - Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability
  - The manufacturer should provide users with guidance on how to securely set up their device
  - The manufacturer should provide users with guidance on how to check whether their device is securely set up

Finally, Al mentioned some comments from an EE Times article about how this standard might be enforced. Basically, the article mentioned three ways:

- Direct enforcement under the EU Cybersecurity Act
- Indirect enforcement by showing the standard was followed to mitigate liability if a security breach happens. That is, by showing evidence that a company followed a standard in the case of a security breach the company might get a lesser fine or even get no fine as opposed to if the company did not follow the standard
- As a consumer marketing tool by showing that an IoT product is more secure by showing customers proof that the company followed the standard in developing the product

5. Ira then went through a set of slides on his proposed schedule and content for his HCD Security Guidelines; the slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/ids-hcdsec-status-20200819.pdf. Some key points Ira made were:

- The initial draft was created in Jan 2020 which includes Appendix A that has a survey of the commonly used protocols from Layers 2-7. The plan for finishing the guidelines is:

  - HCDSEC Interim draft in Q3 2020 to include Section 4 Network Security (minimum requirements)
  - HCDSEC Interim draft in Q4 2020 to include Section 5 Local Security and Section 6 System Architecture
  - HCDSEC Prototype draft in Q1/Q2 20 to include the remaining sections (Section 7 Conformance, Section 8 Internationalization Considerations, Section 9 Security Considerations and Section 10 References)
- Ira is working now on Section 4. The key concepts for Section 4 will be:
  - The network protocols will be defined in terms of functional groups of protocol requirements (e.g., End-to-End Security for TLS, SSH, etc.).
  - Ira will define multiple scalable HCD requirements (i.e., essential security versus value-add security)
  - He will emphasize “secure by default” configuration (e.g., admin password setup and firewall default blocking)
  - Some of the things he will describe in Section 4 will be:
    - Firewall Types - Static (heuristic, without signatures or updates) vs. Dynamic (rule-based, with signatures and updates)
    - Antivirus and IDS Scanner Types - Static (heuristic, without signatures or updates) vs. Dynamic (rule-based, with signatures and updates)
- Ira then gave multiple examples of the types of requirements that would be in Section 4 A couple of examples are:
  - Conforming HCDs MUST implement and enable at least a Static Firewall on open network interfaces
  - Conforming HCDs SHOULD support IEEE 802.1AR for datalink authentication
  - Conforming HCDs SHOULD support TLS/1.3 for end-to-end transport security
  - Conforming HCDs SHOULD support SSH for end-to-end transport security
  - Conforming HCDs SHOULD support SNMPv3 over TLS in an isolated process for necessary remote HCD configuration.

6. For the final topic Al went through was the NIAP Cybersecurity Framework, one of the standards activities Ira had mentioned in his discussion over a year ago. Al had analyzed this framework for Xerox in Sep 2019 so he thought he’d revisit it now and share it with the IDS.

   The NIAP Cybersecurity Framework is a risk-based approach to managing cybersecurity risk that consists of three parts:

   - Framework Core -- Set of cybersecurity activities, desired outcomes, and applicable
   - Framework Implementation Tiers -- Provide context on how an organization views cybersecurity risk and the processes in place to manage that risk
   - Framework Profiles -- Represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The actual NIST Cybersecurity Framework document is included below

     NIST.CSWP.04162018.
     pdf

   The Framework Core is divided up into:

- **Functions**: Organize basic cybersecurity activities at their highest level
- **Categories**: Subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities (e.g., "Asset Management," "Identity Management and Access Control)
- **Subcategories:** Further divide a Category into specific outcomes of technical and/or management activities.
- **Informative References:** Specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory

  There are 5 Functions, 23 Categories, 108 Subcategories and 6 Informative References.

The key is the five Functions – Identify, Protect, Detect, Respond and Recover. These five functions are defined as follows:

- **Identify** - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
- **Protect -** Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect** - Develop and implement appropriate activities to identify the occurrence of a cybersecurity event
- **Respond** - Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
- **Recover** - Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

Everything is really geared around how the five functions are met. The concept is very similar to the Capability Maturity Model (CMM) that was in vogue about 20 years ago in that large enterprises like Ford or AT&T or IBM would be assessed against the NIST Cybersecurity Model so see how mature the enterprise was in terms of managing their cybersecurity risks. So, the NIST Cybersecurity Framework provides a quantitative way of measuring against the five Functions using the 23 categories and 108 subcategories how well cybersecurity risks are managed.

The Implementation Tiers are like the Maturity Levels in the CMM; they tell how mature the organization is in terms of managing cybersecurity risk in terms of how institutionalized cybersecurity risk management is within the organization, the four Tiers in this model are:

- Partial
- Risk Informed
- Repeatable
- Adaptive

The meeting slides include a Reference slide that has a reference to the NIST Cybersecurity Framework web site where more information can be found, as well as references to cyrptoagility, constrained devices, and ENISA standards,

7. **Wrap Up**

- Next IDS Conference Call will be on September 3, 2020.
- Next IDS Face-to-Face Meeting will be during the next PWG Virtual Face-to-Face Meeting November 10-12, 2020

Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 12:00 noon ET on August 19, 2020.