IDS Face-to-Face Minutes
November 04, 2020

Meeting was called to order at approximately 10:00 am ET November 04, 2020.

Attendees –

Amitha	Konica Minolta
Cihan Colakoglu	
Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Marc Mulders	Konica Minolta
Alan Sukert	Xerox
Anthony Suarez	Kyocera
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/2020-11-04-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 potential HCD collaborative Protection Profile (cPP) v1.0 content
   - HCD Security Guidelines 1.0 Status
   - CCC and 3D Printing Presentation
   - Wrap-Up / Next Steps
3. Went through the PWG Intellectual Property policy.
4. Went through the minutes of the weekly HCD iTC meetings held since the last IDS Face-to-Face (F2F) Meeting on August 19th. Some of the key points from this discussion were:

   - The first internal drafts of the HCD cPP and HCD Supporting Document (SD) were reviewed by the full HCD iTC – 68 comments were received against the HCD cPP draft and 28 comments were received against the HCD SD draft.

     At the HCD iTC meetings since the last ISD F2F the HCD iTC reviewed and addressed all 68 of the comments against the first internal HCD cPP draft and all 28 of the comments against the first internal HCD SD draft. The final tally of the comment resolutions was as follow:

     For the first HCD cPP draft:

     - 59 comments were ‘Accepted’ to be fixed for the next draft
     - 4 comments were ‘Accepted in Principle’ to be fixed in some later draft

- 5 comments were 'Deferred' to be addressed a later time, possible in a later version of the HCD cPP

For the first HCD SD draft:

- 12 comments were 'Accepted' to be fixed for the next draft
- 9 comments were 'Accepted in Principle' to be fixed in some later draft
- 6 comments were 'Deferred' to be addressed a later time, possible in a later version of the HCD cPP
- 1 comment was 'Not Accepted'

- A major issue that arose during the review of the comments against the HCD cPP draft was a proposal by Ricoh concerning non-field replaceable non-volatile storage. The proposal was that non-field replaceable non-volatile storage be allowed to store key material in clear text rather than encrypted as long as the HCD had some type of "purge" function that would allow the key material to be deleted when the HCD was ready to be decommissioned or moved to another location

  Issue was that the Essential Security Requirements (ESR) document approved by the Common Criteria Development Board (CCDB) contained the following requirement:

  "The HCD shall encrypt user document data and/or the HCD critical data (for confidentiality protection) stored on the nonvolatile storage device if it uses nonvolatile storage device for the purpose of storing those data. **To support encryption, the HCD shall maintain key chains in such a way that keys and key materials are protected. Note that the initial data of the key chain stored on the nonvolatile storage device without protection do not meet the requirement**". The bolded text implied, depending on how you interpreted what "protected" meant, that the ESR would not allow such a proposal, so if we agreed on this proposal the ESR would have to be changed. Since any change to the ESR would have to be approved by the HCD Working Group (the Korean and Japanese Schemes that sponsored the HCD iTC) and then the Common Criteria Development Board, ESR changes cannot be taken lightly.

  Part of Ricoh's rationale for this proposal was that one of the assumptions in the Security Problem Definition in the draft HCD cPP is that the appropriate physical security is in place in the Operational Environment. If that is the case that that should protect any non-field replaceable non-volatile memory from being removed while the device is in operation.

  Since the full HCD iTC could not reach any type of consensus, at Ira's suggestion a subgroup was formed to come up with a recommendation to the full iTC on what to do with the Ricoh proposal. The subgroup's recommendations, which will be discussed at the next HCD iTC meeting, are:

  - 'Defer' the proposal since it would require an ESR change to implement
  - Have the HCD iTC vote on whether to agree to accept the Ricoh proposal. If the vote is to accept the proposal then ask the HCD WG to change the ESR to allow this proposal to be included in the HCD cPP and implemented in an HCD.

- Al went through briefly a related issue brought up by JBMIA on protecting the passphrase or other mechanisms used to generate encryption keys. The good news was that the SFRs needed to do such protected had already been included in the HCD cPP draft.
- Al discussed the work of the HCD iTC's Network Subgroup. This subgroup is looking at what to do in the HCD cPP/SD for the SFRs and assurance activities for the four secure protocols – IPsec, TLS, SSH and HTTPS, although the subgroup's charter has recently been expanded to look at additional SFRs and assurance activities for dependencies of the four secure protocols. Currently the Network Subgroup is leaning towards recommending to the full iTC the following:

- Both TLS and SSH should split requirements into separate client and server requirements
- It is recommended that IPP should be considered for later versions of the HCD cPP/SD beyond v1.0.
- Use the IPsec, TLS, SSH and HTTPS requirements taken from ND cPP/SD v2.2e **as the basis** for the SFRs/assurance activities in HCD cPP/SD v1.0
  - However, in long term goal is to establish cross-functional teams to develop packages for each of the four Secure Protocols that can be referenced by any cPP or SD that needs to use any of the protocols
  - Need to determine if that also includes any of the FIA_X509_EXT.* SFRs/Assurance Activities related to certificate evaluation
- Regarding DTLS, the current Network SG position is that HCD cPP/SD v1.0 will not include requirements for DTLS unless vendors indicate that they need to support it. Ira polled the HCD vendors and the general feeling was that except for two vendors that did not want DTLS, mots vendors would want DTLS as long as it was made a selection. One important caveat was that this was based on the RFC for DTLS being published, which Ira indicated would soon occur.

- Because of the delays in getting the first internal drafts of the HCD cPP and HCD SD out for review, Al went through the changes in the schedule that the delays had caused. As of now, the current schedule for the next set of internal drafts is:

  2nd Internal Draft
  - Release of 2nd Internal Draft HCD cPP delayed until week of 10/26/2020
  - Comments due by Nov 23rd
  - Comments resolved by Dec 15th
  - Updates to HCD cPP to be completed by Jan 6, 2021
  - Release of 2nd Internal Draft HCD SD delayed until 11/09/2020
  - Comments due by Dec 7th
  - Comment resolution date now scheduled for Dec 23rd, but may be moved to early Jan
  - Updates to HCD SD now scheduled to be completed by Jan 13, 2021

  Added 3rd Internal Draft of both HCD cPP and HCD SD for some time in Jan 2021 (date TBD)
  - Will only review changes; not full text

  Date of 1st Public Review Drafts still scheduled for 2/2/21

  Al was asked the question as to how reasonable were these dates in terms of “can they be met”. The answer that was given was “I’d give it a 50-50 chance”.

- Al finish the HCD iTC discussion with his thoughts on what remaining issues the HCD iTC faced in getting HCD cPP/SD v1.0 out. Some of the more significant issues Al mentioned were:
  - Getting a Security Problem Definition document publicly reviewed and approved; it is an important step in the cPP Development Process the iTC has failed to do that has to be done.
  - Start adding new SPRs and Assurance Activities into the HCD cPP and SD drafts. The question was asked whether this had to happen before the first public draft in February 2021; the consensus of the meeting attendees was that new content could still be added even in the first public draft, but that full content for v1.0 had to be in the second public draft.
  - Support for FIPS 140-3
  - Removal of all SHA-1 support and support for TLS 1.0 and TLS 1.1

- "Hardware-anchored integrity of hardware/software" and "secure boot"
- Other areas that might be considered "absolutely necessary" for HCD cPP/SD v1.0 such as:
    - Expansion of network-fax separation to "no bridging"
    - Syncing with applicable updates to ND cPP and FDE cPPs
    - Syncing with any applicable NIST SP updates
    - Inclusion of any applicable NIAP TDs to HCD PP and ND & FDE cPPs
    - Syncing with ENISA and the new proposed European cybersecurity certification scheme (EUCC) and NIST Cybersecurity Framework
    - Changes to ISO/IEC 15408 if they come out in the v1.0 time frame

5. Ira then went the latest draft of the HCD Security Guidelines which can be found at: https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20201101-rev.docx

   https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20201101-rev.pdf

   The changes Ira made were all in Chapter 4, HCD Network Security. Ira took the meeting attendees through a high-level look at the changes made in Chapter 4. Ira created new subsections in Chapter 4 as follows:

   - **Network Interface Defenses** which discusses Antivirus Scanners, Denial of Service Defenses, Firewalls and Network Intrusion Detection Scanners
   - **Datalink Security** which covers MACsec and WPA
   - **End-to-End Security** which covers IPsec, SSH and TLS/DTLS
   - **Job Security** which covers IPP and Common Log
   - **Configuration Management** which covers SNMPv3 over TLS, SSH and NETCONF

   The types of requirements that are in these subsections are:

   - Conforming HCDs that implement SSH MUST restrict the commands that can be executed to those needed for maintenance of the HCD that cannot be supported through other standard protocols.
   - Conforming HCDs MUST implement TLS 1.2 [RFC5246], for compatibility with current Internet and Enterprise network infrastructure.
   - Conforming HCDs SHOULD support SNMPv3 over TLS [RFC5590], [RFC5591], and [RFC5593] in an isolated process for necessary remote HCD configuration.

6. For the final topic Al went through the presentation he and Paul Tykodi gave to the INCITS Digital Technology Technical Committee on October 20th. The presentation was entitled "**Common Criteria and How It Could Be Applied to 3D Printing**". The goal of the presentation was to show the TC how Common Criteria certification methodology could be applied to create a Protection Profile for 3D printers in a similar way to how the HCD PP was created for hardcopy devices and thus 2D printers. The slides Al presented at the meeting were part of the full presentation given to the INCITS TC; the full presentation is available at https://ftp.pwg.org/pub/pwg/ids/Presentation/CCC and 3D Printing v3.pdf.

   Since the INCITS TC had no knowledge of what Common Criteria was Al gave a brief overview of Common Criteria, what Common Criteria certification is, basic terminology such as what a Target of Evaluation (TOE) is, what a SFR and SAR are, etc. and then focused on what a Protection Profile and Security Target (ST) are and what they contain. The key of this section of the presentation was to indicate that the goal of a Common Criteria certification was not to determine that a product was secure, but rather that a TOE met its specification as stated in the Security Target which conformed

to a Protection Profile for the class of products that particular TOE belonged to. In this case, the PP was for hardcopy devices.

The presentation then went into detail on the Security Problem Definition (SPD) for 2D printers taken from the HCD CPP, since a 2D printer is just a type of hardcopy device. The presentation actually started by defining what a hardcopy device was and the normal use cases for a HCD – printing, copying and scanning plus security-related functions like auditing, configuring security functions, verifying software upgrades and self-testing to find malfunctions. The presentation then went into detail of the four key components of the HCD SPD:

- Threats
- Assumptions
- Security Policies
- Security Objectives

The most critical to what was to follow for the 3D printing portion was the five key threats to HCDs:

- Unauthorized Access to user document data stored in the HCD (primarily in non-volatile storage)
- Unauthorized Access to TSF (TOE Security Functions) data stored in the HCD (this is data such as login credentials and encryption keys)
- Unauthorized Access to User and TSF data transmitted to/from the HCD over a network
- Unauthorized Software Update
-
- Failure of the TSF

The presentation then went through the key assumptions and security polices (see the Meeting Slides or the full presentation) and then the Security Objectives of the TOE and the Operational Environment. The key security objectives of the TOE are:

- User Identification and Authentication
- User Authorization
- Access Control
- Administrator Roles
- Software Update Verification
- Self-Test
- Auditing
- Communications Protection
- Storage Encryption
- Image Overwrite
- Protection of Key Material
- Purge Data
- PSTN Fax-Network Separation

Then came the central portion of the presentation – answering the following question: Could the Common Criteria Certification process that was used to certify 2D Hardcopy Devices be used to perform a similar security certification for the Digital Thread for Additive Manufacturing? The Digital Thread for Additive Manufacturing is a 5-step process for created a 3D printed object that in some ways is similar to a software development process. The steps in the Digital Thread are:

- Product Inception
- Design/Scan and Analyze

- Build and Monitor
- Test and Validate
- Deliver and Manage

From a security perspective the Additive Manufacturing industry as a whole is concerned about the following:

- Cybersecurity Threats
    - Espionage
    - Tampering / Hacking / Mischief / Extortion / Terrorism
    - Privacy
    - Intellectual Property / Trade Secrets
- Data Integrity along the entire Digital Thread
- Protect Data Confidentiality
- Ensure/Protect Data Integrity
- Verify Data Integrity
- Protect Intellectual Property

Starting with that, the key, as was stated in the very beginning of the presentation, is that the whole certification process is fundamentally about assets – what assets should be protected, what are the threats against those assets that need to be protected, and what can be done to mitigate or minimize those threats.

So, looking at the details of the Digital Thread, several assets became important from a security perspective that might need to be protected:

- CAD file created to mode the object to be printed
- Models/simulations created for the object to be printed
- STL/3MF file created from the CAD file that the 3D printer uses to actually print the object (like a raster file for a 2d printer)
- Build simulations
- Slicer software used to slice the material to be printed into thin layers for ease of printing
- Software to control the 3D printer and the computer storing the CAD and STL/3MF files

The key to answering the question once you have a possible set of assets that need to be protected is what is the SPD in the case of a 3D printer. Al and Paul couldn't readily determine what the assumptions and security policies might be, but based on the details of the digital path and the nature of the assets the threats in the 3D printing world could be very similar to at least 3 of the key threats to HCDs, specifically:

- Unauthorized Access to user document data stored in the HCD (primarily in non-volatile storage)
- Unauthorized Access to User and TSF data transmitted to/from the HCD over a network
- Unauthorized Software Update

The possible threats Alan and Paul identified for the Digital Thread (there certainly could be others) were:

- Unauthorized access to the CAD file and model/simulations while stored on the computer hosting the CAD file/models/simulations (even if it is the 3D printer)
- Unauthorized access to the STL/3MF file created from the CAD file while stored in either on the computer hosting the CAD file or on the 3D printer itself
- Unauthorized access to the STL/3MF file while in transit between the computer hosting the CAD filer and the 3D printer if stored on separate computers

- Unauthorized access to the build simulation and slicer software stored on the 3D printer
- Unauthorized software upgrade of either the computer hosting the CAD file or the 3D printer

Regarding security objectives of the TOE, some possible ones for 3D printers via the Digital Thread could be:

- User Identification and Authentication
- Access Control
- Software Update Verification
- Self-Test
- Communications Protection
- Storage Encryption (note that there already is an encryption spec for 3D printers)
- Protection of Key Material

Based on all of the above Al and Paul felt there was enough similarity between the 2d printing and 3D printing in terms of assets and threats that a PP could be constructed for 3D printers. The recommendations to the INCITS Digital Manufacturing TC were:

- Create of a 3D Printing Technical Community (TC) to work this problem in coordination with the HCD international TC
- Determine who the customers/audience for this TC would be
- Generate an approved 3D Printing Protection Profile. Our initial thought is that it could be a PP-Module based off of the HCD collaborative PP that is currently being developed for publication sometime in 4Q 2021
- Recognize this will take time; realistically we are probably talking end of 2022 at the earliest before we would have a PP
- Once we have a 3D Printing PP we can start certifying 3D Printers against that PP

The INCITS Digital Manufacturing TC was very receptive to the presentation and agreed to study this further. It will be interesting to see where this goes.

7. **Wrap Up**

- Next IDS Conference Call will be on November 12, 2020.
- Next IDS Face-to-Face Meeting will be during the next PWG Virtual Face-to-Face Meeting February 9-11, 2021

Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 12:00 noon ET on November 04, 2020.