The Printer Working Group

Imaging Device Security

February 06, 2020

PWG February 2020 Virtual Face-to-Face

Agenda

When	What
9:00 – 9:05	Introductions, Agenda review
9:05 – 9:50	Discuss results of latest HCD TC Meetings and potential HCD cPP content
9:50 – 10:30	TLS 1.2 / TLS 1.3 Discussion
10:30 – 10:50	Review latest HCD Security Guide 1.0 Draft
10:50 – 11:00	Wrap Up / Next Steps

Intellectual Property Policy

"This meeting is conducted under the rules of the PWG IP policy".

- Refer to the IP statements in the plenary slides

Officers

- Chair:
  - Alan Sukert (Xerox)
- Vice-Chair:
  - TBD
- Secretary:
  - Alan Sukert (Xerox)
- Document Editor:
  - Ira McDonald (High North) – HCD Security Guide

HCD Technical Community Status

12/10/19 HCD PP TC Conference Call

- Collaboration tool Updates
  - Set up the environment at the Github (Target : End of 2019)
  - Transfer the HCD PP to Github (Target: early 2020)
  - Next meeting is planned on next week.
- Update the HCD iTC progress
  - HCD iTC is not endorsed yet by CCMC.
  - Kwangwoo reminded the CCMC Voting to ITSCC and CCMC Chair.
- HCD cPP development milestone
  - We decided to follow the existing milestone that was proposed by last month.
    - 1~6 month: 1st Working Draft (Starting from 2020)
    - 7~12 month: 2nd Working Draft
    - 13~18 month: SMEs Review (call for comments and comment resolution) v0.8.x
    - 19~23 month: Public Review (call for comments & comment resolution) v0.9.x
    - 24 month: HCD cPP v1.0 (Final Version)

12/10/19 HCD PP TC Conference Call

- HCD cPP development milestone
  - Review the iTC/cPP Process paper
    - Focus on the figure 3: Process Flow Diagram for cPP Development
- Sub WG Establishment
  - TLS 1.3: Ira McDonald (Draft: June 2020)
    - Feb 2020 - set up the TLS 1.3 session
  - Hardware-anchored integrity verification: Jerry Colunga (Draft: June 2020)
  - SED & HDD Encryption: Alan Sukert (Draft: June 2020)
    - Need to align with FDE cPP
  - Ira can support the resource for the all items.

12/10/19 HCD PP TC Conference Call

- Roundtables
  - If you cannot access the Causeway, please contact to Kwangwoo (kwangwoo.lee@hp.com)
  - https://collaborate.ccusersforum.org/wg/HCD_TC/dashboard
  - HCD iTC SMEs status
  - Industry SMEs (36), Lab SMEs (20), Certification Body SMEs (4), Other SMEs (6)

1/10/2020 HCD PP TC Conference Call

- Collaboration tool Updates
  - Set up the environment at the Github (Target: End of 2019)
    - Done. Alan got the environment setup.
  - Transfer the HCD PP to Github (Target: early 2020)
    - 25% done. Actually, Alan started to transfer the HCD PP into the cPP template that Brian Wood set up
    - Asciidoc is not easy to work with
  - Invited talk (Brian Wood/CCUF Team Tools WG)
    - Brian Wood shared the set of tools to help HCD iTC write and manage our cPP using the CCUF Team Tools Working Group website (https://itc-wgtools.github.io/).
    - Brian demo'd how HCD iTC can use GitHub to document issues against drafts of the HCD cPP. He showed how to write issues against a document template.
    - See YouTube video for more details:
      - iTC Tools & Templates (CCUF Team Tools WG) @16th CCUF Workshop
        - https://youtu.be/eBwTwYS5TRE
      - CCUF Team Tools WG @15th CCUF Workshop
        - https://youtu.be/6Gdb4qNn0tg

1/10/2020 HCD PP TC Conference Call

- HCD cPP development milestone
  - We decided to follow the existing milestone that was proposed by last month.
    - 1~6 month: 1st Working Draft (Starting from 2020)
    - 7~12 month: 2nd Working Draft
    - 13~18 month: SMEs Review (call for comments and comment resolution) v0.8.x
    - 19~23 month: Public Review (call for comments & comment resolution) v0.9.x
    - 24 months: HCD cPP v1.0 (Final Version)
      - Target date: 2022 1Q
  - Review the iTC/cPP Process paper
    - Focus on the figure 3: Process Flow Diagram for cPP Development

1/10/2020 HCD PP TC Conference Call

- Sub WG Establishment
  - TLS 1.3: Ira McDonald (Draft: June 2020)
    - Feb 2020 - set up the TLS 1.3 session (30 minutes required)
      - Ira is working on updating the slides he had done in the printer working group (which will be presented later at this meeting)
      - Ira reviewed the ND workgroup's package on TLS 1.3 which is a little confusing because it's actually a markup mostly and not meaningful of a very old version of NDcPP from later 2018 so it's not the current one. But there is a really good content (about 2 pages) on TLS 1.3 on particular ciphersuites and so on and TLS 1.2. Unfortunately, none of that got into the new NDcPP version 2.2. so, it is still very deficient in his opinion in describing details for setting up TLS.
      - Anantha mentioned that the TLS 1.3 WG are waiting on feedback from the wider community before going forward in the process.
    - NDcPP: TLS 1.3 ciphersuite of ND cPP
      - Kwangwoo mentioned that CCDB had their crypto workgroup and they also discussed the NDcPP folks. We need to check whether NDcPP has any plan to update NDcPP's ciphersuite

1/10/2020 HCD PP TC Conference Call

- Sub WG Establishment
  - Hardware-anchored integrity verification: Jerry Colunga (Draft: June 2020)
    - Jerry has a plan to start working on this and should have some updates in our next monthly meeting.
  - SED & HDD Encryption: Alan Sukert (Draft: June 2020)
    - Need to align with FDE cPP
    - Alan will try to have something an update for next month.
- Roundtables
  - If you cannot access the Causeway, please contact to Kwangwoo (kwangwoo.lee@hp.com)
  - https://collaborate.ccusersforum.org/wg/HCD_TC/dashboard
  - HCD iTC SMEs status
  - Industry SMEs (36), Lab SMEs (20), Certification Body SMEs (4), Other SMEs (6)

Updates Since the November IDS Face-to-Face Meeting

Updates Since the November IDS Face-to-Face Meeting

- CCMC finally started its vote on ToR and ESR submitted by HCD WG on January 9, 2020
  - Should take 1-2 months to complete
  - We hope to get approval in time for the March 17-19, 2020 CCUF Workshop so we can have the first HCD iTC meeting there
  - Latest status:
    - Voting still in progress
    - No “reject” votes have been cast officially via CCMC mailing list, but have to wait for official announcement from CCMC Chair since votes could go directly to CCMC Chair

Updates Since the November IDS Face-to-Face Meeting

- HCD iTC editors have set up environment on GitHub to transfer HCD PP v1.1 into cPP (SFRs) and Supporting Document (Assurance Activities) GitHub templates so when iTC is approved "we can hit the ground running"
- Work has started on converting the draft HCD PP v1.1 into a draft HCD cPP v1.0 in GitHub
  - Going very slowly but will try to get it done by the March CCUF Workshop
- Next HCD TC Conference Call is February 13, 2020 (US) / February 14, 2020 (Asia)
- Next HCD TC Face-to-Face will be at the CCUF Workshop in Burlington MA Mar 15-17, 2020

HCD cPP v1.0

- Original Planned Content
  - Planned content for what was going to be in HCD PP V1.1 including HCD PP Errata #1
  - Any NIAP Technical Decisions against the HCD PP
  - The list of issues discussed at the Sep 2019 HCD TC Face-to-Face Meeting in Singapore

HCD cPP v1.0

- Current thoughts on additional content that should be or have to be added
  - TLS 1.3 support and removal of both TLS 1.0 and TLS 1.1
  - Implementation of the CCDB Crypto WG Protocol Packages, especially the TLS and SSH ones
  - ISO Standard 19790- **Information technology — Security techniques — Security requirements for cryptographic modules** (This is the crypto standard FIPS 140-3 points to)
    - FIPS 140-3 becomes mandatory on 9/22/2021
  - "No bridging" requirement vs. just "Network-fax separation"
  - Removal of 3DES and SHA-1
  - Sync with ND cPP v2.2 and any further NC cPP and FDE cPP updates
  - EU Cybersecurity Act / Certification Framework and ENISA
  - Sync with any applicable NIST updates and any applicable NIAP TDs and policy updates

The Printer Working Group

TLS/1.2 and TLS/1.3 Highlights

IPP Working Group

Agenda

- Evolution of SSL (Netscape)
- Evolution of TLS (IETF)
- Usage Recommendations for TLS
- Extensions for TLS
- TLS/1.2 Cipher Suites & Profiles
- TLS/1.3 Cipher Suites & IANA Registry
- TLS/1.3 Migration

TLS/1.3 Ciphers & IANA Registry

- TLS/1.3 Mandatory Cipher Suites
  - Current MTI of TLS_AES_128_GCM_SHA256
    - Defined in Appendix B.4 of RFC 8446
  - Recommends support for TLS_AES_256_GCM_SHA384
    - Defined in Appendix B.4 of RFC 8446
  - Recommends support for TLS_CHACHA20_POLY1305_SHA256
    - Defined in RFC 8439
  - Other cipher suites SHOULD only be supported if specified in an implementation supported IETF TLS application profile standard
- IANA Registry Updates for TLS and DTLS https://tools.ietf.org/html/rfc8447
  - For use with TLS/1.2 and TLS/1.3 – updates RFCs 3749, 5077, 4680, 5246, 5705, 5878, 6520, 7301
    - Defines new registration policy and registry annotation mechanism
    - https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml
    - https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml

TLS 1.3 Migration (1 of 3)

- TLS/1.3, RFC 8446, August 2018
  https://tools.ietf.org/html/rfc8446
  - Obsoletes TLS/1.2 (RFC 5246)
- DTLS/1.3, draft-34, November 2019
  https://datatracker.ietf.org/doc/draft-ietf-tls-dtls13/
  - Obsoletes DTLS/1.2 (RFC 6347) – to IETF Last Call
- TLS/1.3 support in browsers
  - All major browsers now support TLS/1.3
- 18 TLS libraries participated in TLS/1.3 prototyping
- All major TLS libraries now have TLS/1.3 support
  - OpenSSL starting with v1.1.1
  - GNU TLS starting with v3.6.3
  - SecureTransport (macOS) starting with macOS 10.14 and iOS 12
  - wolfSSL starting with v3.15.3
  - Facebook Fizz, Boring SSL, JSSE, NSS, and others coming soon

TLS 1.3 Migration (2 of 3)

- Lots of confusion over this new version of TLS
  - https://en.wikipedia.org/wiki/Transport_Layer_Security
  - https://en.wikipedia.org/wiki/Comparison_of_TLS_implementations#Protocol_support
  - https://www.techrepublic.com/article/tls-1-3-is-approved-heres-how-it-could-make-the-entire-internet-safer/
  - https://www.wolfssl.com/differences-between-tls-1-2-and-tls-1-3-2/
  - Customer demand for Clients and Printers to support TLS 1.3 ASAP!
- Testing TLS via Error Checking Tool https://github.com/WestpointLtd/tls_prober
  - TLS mailing list note from Hubert Kario (Redhat) on 13 June 2018

TLS 1.3 Migration (3 of 3)

- Site policies and government regulations influence cipher suite selections and preferences
- Aside from TLS protocol issues, X.509 certificates issues
  - IETF TLS WG is now deprecating MD5 or SHA-1 hashes
  - SHA-2 is now supported by all major browsers
  - CA certs are max-life 3 years / Printer self-certs ~ max-life 10 years
- IPP Everywhere™ v1.1 adds "1.3" version to the TLS key in the TXT record to allow a Client to discover maximum TLS version a Printer supports without connecting
  - ... but the only way to know for sure is to negotiate a TLS connection since the DNS-SD TXT record could be spoofed
- No IPP attributes or values are defined for TLS 1.3
  - Most IPP Clients look for **_ipps** advertisements (TLS) and not for a specific version of TLS
  - TLS version negotiation is handled separately from IPP
  - DNS-SD discovery mechanism is handled separately from IPP

HCD Security Guide Status

HCD Security Guide

- 12/31/19 draft was created by Ira and reviewed at the 1/9/2020 IDS WG Conference Call. The following comments were generated:
  - Cover page - correct document metadata - title and author
  - Section 1 Introduction - line 155 - correct title of HCD PP
  - Section 2.3 Security Terminology - line 227 - delete trailing "d"
  - Section 3.4 Design Requirements
    - - line 330 - change "5100.4" to "5110.4"
    - - line 337 - misspelled "recommendations
    - - line 337 - missing local security and system architecture requirements
  - Section 6 HCD System Architecture - line 359 - missing "isolation" after "channel"
  - Section 10 References
    - - line 403 - delete leading space
    - - line 879 - change [XML] to [W3C-XML] for clarity (global)
    - - line 882 - change [XSD] to [W3C-XSD] for clarity (global)
    - - line 882 - fix [XSD] broken reference format

HCD Security Guide

- 12/31/19 draft was created by Ira and reviewed at the 1/9/2020 IDS WG Conference Call. The following comments were generated:
  - Section 12 Appendix A – Internet Protocol Suite
    - - global - change "used in TCP/IP networks" to either:
    - -- "that can be used in the Internet Protocol Suite" (non-IETF protocols)
    - <or>
    - -- "in the Internet Protocol Suite" (IETF protocols)
    - - global - move all notes on inappropriate protocols for HCDs to section 4
    - - line 1246 - move "SMIv1" and "SMIv2" outside "SNMP" (w/ cross refs)
    - - line 1263 - change "is is" to "is"

HCD Security Guide

- Revised draft incorporating corrections to these comments was issued by Ira on 1/20/2020 at https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20200120-rev.docx

HCD Security Guide

Early comment on 1/20/2020 draft from Mike Sweet:

Text in section 12.7.17 on SSH:

> Note: SSH is inherently dangerous, because implementation or configuration errors can allow privilege escalation and unconstrained remote shell capabilities on target systems. SSH has major security flaws and has often been used for widespread Internet attacks by intelligence agencies and criminal organizations. Therefore, SSH is unsuitable for use in any HCD.

SSH is an Internet Standard and is IMHO the only viable solution for a remote "shell" interface. Honestly I wouldn't want any vendor to try to invent their own "secure" solution (you know what happens then...)

I would much prefer that the PWG talk about *what* the actual security considerations are and not focus on historical issues that have a) been fixed and b) affected specific implementations of SSH and not the protocol itself.

We can debate what the full text should be, but IMHO the focus should be that a) SSH is a common target, b) SSH (like all HCD software) needs to be updated to address security issues, and c) SSH should not provide general access to the device.

Next Steps – Security Guide

- Develop Updated Draft Versions
  - Review content with IDS WG at Conference Calls and F2F Meetings as it is created
- Develop Final Draft
- Obtain PWG Approval

Next Steps – HCD cPP v1.0

- Implement the transition from the HCD TC → HCD iTC
  - Complete transfer of HCD PP v1.1 to HCD cPP v1.0 draft
  - Initiate HCD PP v1.1 → HCD cPP Supporting Document draft
  - Have the first iTC meeting
- Start work on HCD cPP v1.0
  - Develop detailed plan for development, review and release of HCD cPP v1.0
  - Determine detailed list of issues for HCD iTC to review for inclusion in HCD cPP v1.0
  - Initiate work on subgroups and create more subgroups as necessary
  - Generate first full HCD cPP v1.0 draft
  - Update and review drafts as necessary to create “final” version
  - Get iTC review and approval for “final” version
  - Release HCD cPP v1.0

Next Steps – IDS WG

- As some of you might know I am retiring from Xerox as of April 1, 2020
- Have reached out to some as replacements, but if anyone is interested please contact either myself, Smith Kennedy, Jeremy Leber or Ira McDonald

Proposed IDS WG 2020 Goal

- As a parting thought, I believe that a key 2020 goal of the IDS WG should be as follows:

  Expand its “outreach with other standards bodies involved in HCD security issues” to other standards bodies beyond the HCD Technical Community

Next Steps – IDS WG

- Next IDS Conference Calls – March 5, 2020 and March 19, 2020
- Next IDS Face-to-Face Meeting May 5-7 (probably May 7), 2020 at Lexmark in Lexington KY
- Start looking at involvement in other HCD standards activities starting in 2020