The Printer Working Group

Imaging Device Security

May 6, 2021

PWG May 2021 Virtual Face-to-Face

Agenda

When	What
10:00 – 10:10	Introductions, Agenda review
10:10 – 11:05	Discuss results of latest HCD iTC Meetings and HCD cPP/SD v1.0 status
11:05 – 11:15	MASS DOT Discussion with IDS WG
11:15 – 11:35	HCD Security Guidelines v1.0 Status
11:35 – 11:55	TCG/IETF Liaison Reports
11:55 – 12:00	Wrap Up / Next Steps

Antitrust and Intellectual Property Policies

"This meeting is conducted under the rules of the Antitrust and PWG IP policies".

- Refer to the Antitrust and IP statements in the plenary slides

Officers

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

HCD international Technical Community (iTC) Status

HCD international Technical Community (iTC)

- Since last IDS F2F on February 10, 2021 HCD iTC meetings have been held on:
  - February 15 & 22
  - March 1, 8, 15, 22 & 29
  - April 5, 12, 19 & 26
  - May 3

HCD cPP/SD Status

- Released 2nd internal draft of the HCD cPP v1.0 on 11/17/2020
  - Received 26 additional comments against 2nd draft HCD cPP version
  - All comments but one have been adjudicated by the HCD iTC
  - Tally so far for new comments:
    - 13 Comments Accepted
    - 0 Comment Accepted in Principle but will be addressed in a later v1.0 draft
    - 10 Comments Deferred to be addressed by the HCD iTC at a later point in time
    - 2 Comments Not Accepted

HCD cPP/SD Status

- Released 2nd internal draft of the HCD SD v1.0 on 11/19/2020
  - Received 48 additional comments against that draft HCD SD version
  - Not all comments have been adjudicated by the HCD iTC
  - Tally so far for new comments:
    - 29 Comments Accepted
    - 0 Comments Accepted in Principle to be addressed in a later v1.0 draft
    - 1 Comment Deferred to be addressed by the HCD iTC at a later point in time
    - 1 Comment Not Accepted

HCD cPP/SD Status

- Released draft of the HCD SPD on 4/13/2021
  - Received 7 comments against that draft HCD SPD
  - All comments have been adjudicated by the HCD iTC
  - Tally for comments:
    - 7 Comments Accepted
    - 0 Comments Accepted in Principle to be addressed in a later v1.0 draft
    - 0 Comment Deferred to be addressed by the HCD iTC at a later point in time
    - 0 Comment Not Accepted

Current HCD cPP/SD Issues
Addressing HW-Anchored Integrity Verification

- Is a requirement the HCD iTC had included in the Essential Security Requirements (ESR) document
- Deals with Hardware Roots of Trust and how to verify the integrity of the boot process for an HCD
- Need to determine what requirements/assurance activities need to go into the HCD cPP/SD to address this ESR requirement
- Status to date:
  - Have determined what Threats, Organizational Security Policies and Security Objectives need to go into the Security Problem Definition to address this ESR requirement
  - Working on what corresponding Security Functional Requirements and associated Assurance Activities need to go in the HCD cPP/SD for this ESR requirement

HCD cPP/SD Status
Key Closed Issues

- Agreed that all nonvolatile storage will be encrypted
- Agreed to include the SFRs/Assurance Activities from the latest Network Device cPP/SD version for the following:
  - Secure protocols TLSC/TLSS, DLLSC/DTLSS, SSHC/SSHS, HTTP, IPsec
  - FCS_COP.1/DataEncryption (AES Data Encryption/ Decryption)
  - FCS_CKM.1 Cryptographic Key Generation
  - FCS_COP.1/SigGen (Signature Generation and Verification)
  - FCS_COP.1/Hash (Hash Algorithm)
  - FCS_COP.1/KeyedHash (Keyed Hash Algorithm)
  - FCS_RBG_EXT.1 Random Bit Generation
  - FIA_X509_EXT.1 X.509 Certificate Validation, FIA_X509_EXT.2 X.509 Certificate Authentication and FIA_X509_EXT.3 X.509 Certificate Requests
  - FCS_CKM.2 Cryptographic Key Establishment

Other Current HCD cPP/SD Issues

- Inclusion of NTP
  - Concern ND cPP requirements for NTP constitute requirement for "secure NTP"
  - Not sure all vendors support "secure NTP"
- FPT_KYP_EXT Protection of Key and Key Material SFR
  - JBMIA wants to change SFR to state requirements for how key and key material are to be protected to meet requirement in the ESR that "*To support encryption, the HCD shall maintain key chains in such a way that keys and key materials are protected*"
  - HCD iTC members currently commenting on the JBMIA proposal
- Audit Log
  - Korean Scheme now feels that (1) it is mandatory that the audit log be stored on device and (2) that it is mandatory, and not optional, that the audit log should be readable by a device interface
  - JISEC and NIAP have concurred with the Korean scheme
  - HCD iTC assessing what actions to take

Other Current HCD cPP/SD Issues

- Issues HCD iTC members are discussing with their companies:
  - Removal of support for TLS 1.0 and TLS 1.1
  - Removal of SHA-1 support
  - Removal of support for cipher suites with RSA Key Generation with keys < 2048 bits
  - Removal of support for all RSA and DHE Key Exchanges
  - Need to still address Internationalization of SFRs
- Additional New Content
  - Highly unlikely ND TLS subgroup will have TLS 1.3 ready in time frame for HCD iTC to pick it up for HCD cPP v1.0
  - Not anticipating picking up any additional new requirements for the HCD cPP/SD at this time unless either:
    - They are suggested by JISEC or ITSCC
    - They are suggested by JBMIA
    - They are required by changes to ISO, FIPS or NIST Standards/Guidelines

HCD iTC Status
Additional Considerations in Developing HCD cPP/SD v1.0

- 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/SDs
- Syncing with ENISA and the new proposed European cybersecurity certification scheme (EUCC) and NIST Cybersecurity Framework

HCD iTC Status
Proposed New HCD cPP/SD Schedule

Phase	Timeframe	Status/Updates
Resolve ESR Issue and Approve SPD	• Resolve ESR issue: 2/26 DONE • Update ESR: 3/1 – 3/12 NOT NEEDED • Update SPD: 3/1 – 3/12 DONE • Submit ESR changes to HCD WG (if needed): 3/15 NOT NEEDED • HCD WG Review and comment: 3/15 – 4/9 NOT NEEDED • Submit SPD for public review: 3/1 • SPD Public review: 3/1 – 3/26 • Update SPD and update cPP/SD: 3/29 – 4/16	• Draft SPD submitted for internal iTC review: 4/12 • Comments Due: 4/26 Potential Updated Schedule • Submit SPD for public review: 5/10 • SPD Public review: 5/10 – 6/4 • Update SPD: 6/7 – 6/18
Internal Draft	Original Proposal Schedule • Submit 3rd internal draft: 4/19 • Review 3rd internal draft: 4/19 – 5/14 • Review comments & update documents: 5/17 – 6/11	• Looking at 3rd Internal Draft of cPP/SD while SPD is undergoing public review • Estimate can have cPP draft by 5/17 and SD draft by 6/1 at the latest
	New Proposed Schedule • Submit 3rd internal draft: 6/1 • Review 3rd internal draft: 6/1 – 6/18 • Review comments & update documents: 6/21 – 7/16	

HCD iTC Status
Updated Proposed HCD cPP/SD Schedule

Phase	Timeframe	Description
Public Review Draft 1	• Submit 1st Public Draft: 7/19 • Review 1st Public Draft: 7/19 – 8/27 • Review comments and update documents: 8/27- 10/22	
Public Review Draft 2	• Submit 2nd Public Draft: 10/25 • Review 2nd Public Draft: 10/25 – 12/3 • Review comments and update documents: 12/3 – 1/14/22	
Final Draft	• Submit Final Draft: 1/17/22 • Review 2nd Public Draft: 1/17/22 – 2/25/22 • Review comments and update documents: 2/28/22 – 3/25/22	
Final Document Published	• Publish Version 1.0: 3/25/22	

HCD iTC Status
Key Next Steps

- Agree on a revised schedule
- Finalize all new content for v1.0
- Add all new SFRs and Assurance Activities into the HCD cPP and SD
  - Goal is to complete this by the first Public Draft
- Submit all internal, public and final draft HCD cPPs and HCD SDs per the agreed schedule
- Review all comments and update the HCD cPP and HCD SD drafts per the agreed schedule
- Publish HCD cPP/SD v1.0

HCD iTC Status
Lessons Learned to Date (My Take)

- Pre-Planning and getting off to a good start is essential
- Define and agree on your rules of conduct early on, then..
- You need to be disciplined in following your rules of conduct once you agree on them
- Things are not going to go as planned or as scheduled, so be prepared to be flexible and to adapt
- Make sure you have strong leadership, but that has to include someone who is willing to ask questions and offer alternatives
- Employ sub-teams as necessary to solve specific problems

MASS DOT DISCUSSION WITH IDS WG

MASSACHUSETTS DEPARTMENT OF TRANSPORTATION (MASS DOT) DISCUSSION WITH IDS WG

Overview

- Mass DOT has a diverse printer environment with a fleet of printers – some new and some as much as ten years old
- Want to develop a process to ensure a standardized hardening of their printers from a security perspective
  - Looking for the best way to deal with how to ensure their fleet of printers are safe and secure.
  - Want to see if Common Criteria could help them do that

MASSACHUSETTS DEPARTMENT OF TRANSPORTATION (MASS DOT) DISCUSSION WITH IDS WG

MASS DOT:

- Wants to do upgrades of their older printers and keep products current
- Biggest need is how to get a baseline (secure) configuration for each of their devices.
- Desire would be for each of its printers to be hardened "out of the box" by default; i.e., they are secure by default.
- From their experience they have noticed that even when public interfaces are specified and in place for a long time, even if they are not correctly specified, they are very difficult to get changed because printer owners are concerned about unknown consequences to customers if configurations are changed.

MASSACHUSETTS DEPARTMENT OF TRANSPORTATION (MASS DOT) DISCUSSION WITH IDS WG

IDS WG Comments to Mass DOT:

- One of the required outputs that comes out of a Common Criteria certification of a printer are guidelines for the secure installation and operation of the printer, including what should be the "secure configuration" of the printer.
- Protection Profile that has been developed for hardcopy devices, including printers, includes the standard uses cases and security features that a printer should have.
- IDS WG is developing the HCD Security Guidelines.
  - Are planned to be at a higher level than a Protection Profile
  - Will contain specific recommendations, but within the larger framework that a hardcopy device can be (and typically is) a node in a network.
  - Guidelines would also discuss centralize administrative management of HCDs.

MASSACHUSETTS DEPARTMENT OF TRANSPORTATION (MASS DOT) DISCUSSION WITH IDS WG

IDS WG Comments to Mass DOT (cont'd):

- Asked what threat model that Mass DOT is concerned about.
- Briefly went through the Security Problem Definition from the Application Software Protection Profile as an example of what a threat model would be and how it related to assumptions and security objectives that would be found in a Protection Profile.

HCD Security Guidelines Status

Liaison Status

Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Virtual F2F – 14-18 June 2021 – Ira to call in**
- **Trusted Mobility Solutions (TMS) – Ira is co-chair and co-editor**
  - **Formal – GP (TEE, SE), ETSI (NFV/MEC), ATIS (5G Security)**
  - **Informal – 3GPP, GSMA, IETF, ISO, ITU-T, SAE, US NIST**
  - ***TCG TMS Use Cases v2 – published September 2018***
- **Mobile Platform (MPWG) – Ira is co-editor**
  - **Formal – GP (TEE, SE), ETSI (NFV/MEC), ATIS (5G Security)**
  - ***TCG Runtime Integrity Preservation for Mobile Devices – Nov 2019***
  - ***TCG Mobile Reference Architecture v2 – work-in-progress***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress***
  - ***GP Trusted Platform Services Client API – work-in-progress w/ TCG***
- **Recent Specifications**
  - **http://www.trustedcomputinggroup.org/resources**
  - ***TCG TSS 2.0 System Level API (SAPI) – review April 2021***
  - ***TCG TSS 2.0 Overview and Common Structures – review April 2021***
  - ***TCG TSS 2.0 Enhanced System API (ESAPI) – review April 2021***
  - ***TCG TPM 2.0 Library r1.64 – review March 2021***
  - ***TCG DICE Attestation Architecture – published March 2021***
  - ***TCG SMBIOS-based Component Class Registry – published February 2021***

Internet Engineering Task Force (IETF) (1 of 4)

- **Next IETF Members Meetings**
  - **IETF 111 San Francisco ??? – 26-30 July 2021 – Ira to call in**
- **Transport Layer Security (TLS)**
  - **Deprecating TLS 1.0 and TLS 1.1 – RFC 8996 – March 2021**
    https://datatracker.ietf.org/doc/rfc8996/
  - **Hybrid key exchange in TLS 1.3 – draft-02 – April 2021**
    https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
  - **Connection Identifiers for DTLS 1.2 – draft-11 – April 2021 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-tls-dtls-connection-id/
  - **Deprecating MD5 / SHA-1 in TLS 1.2 – draft-06 – March 2021 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-tls-md5-sha1-deprecate/
  - **TLS Encrypted Client Hello – draft-10 – March 2021**
    https://datatracker.ietf.org/doc/draft-ietf-tls-esni/
  - **External PSK Usage in TLS – draft-02 – February 201 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-tls-external-psk-guidance/
  - **TLS Protocol Version 1.3 – draft-01 – February 2021**
    https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/
  - **DTLS/1.3 – draft-41 – February 2021 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-tls-dtls13/
  - **Flags Extension for TLS 1.3 – draft-04 – February 2021**
    https://datatracker.ietf.org/doc/draft-ietf-tls-tlsflags/

Internet Engineering Task Force (IETF) (2 of 4)

- **Security Automation and Continuous Monitoring (SACM)**
  - **SACM Architecture – draft-08 – March 2021**
    https://datatracker.ietf.org/doc/draft-ietf-sacm-arch/
  - **Concise Software Identifiers – draft-17 – February 2021 – to IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/
- **Concise Binary Object Representation (CBOR)**
  - **Storing CBOR items on stable storage – draft-01 – April 2021**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-file-magic/
  - **CBOR tags for IPv4 and IPv6 addresses – draft-04 – April 2021**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-network-addresses/
  - **Feature Freezer for CDDL – draft-07 – April 2021**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-freezer/
  - **Map-like data in CBOR and CDDL – April 2021**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-map-like-data/
  - **CBOR Tags for OIDs – draft-06 – March 2021 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-tags-oid/
  - **Additional Control Operators for CDDL – draft-03 – March 2021**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-cddl-control/
  - **Packed CBOR – draft-00 – September 2020**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/

Internet Engineering Task Force (IETF) (3 of 4)

- **Remote ATtestation ProcedureS (RATS)**
  - **YANG Data Model for CHARRA using TPMs – draft-07 – April 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/
  - **Trusted Path Routing – draft-02 – April 2021**
    https://datatracker.ietf.org/doc/draft-voit-rats-trustworthy-path-routing/
  - **Attestation Event Stream Subscription – draft-02 – March 2021**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-network-device-subscription/
  - **RATS Architecture – draft-11 – March 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/
  - **ARM's PSA Attestation Token – draft-08 – March 2021**
    https://datatracker.ietf.org/doc/draft-tschofenig-rats-psa-token/
  - **CBOR Tag for Unprotected CWT Claims Sets – draft-03 – March 2021**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-uccs/
  - **Entity Attestation Token (EAT) – draft-09 – March 2021**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
  - **Use Cases for RATS – draft-03 – January 2021**
    https://datatracker.ietf.org/doc/draft-chen-rats-usecase/
  - **Time-Based Uni-Directional Attestation – draft-04 – January 2021**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-tuda/

Internet Engineering Task Force (IETF) (4 of 4)

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **Hashing to Elliptic Curves – draft-11 – April 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/
  - **Argon2 password hash and proof-of-work – draft-13 – March 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-argon2/
  - **Usage Limits on AEAD Algorithms – draft-02 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/
  - **OPAQUE Asymmetric PAKE Protocol – draft-03 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/
  - **OPRFs using Prime-Order Groups – draft-06 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/
  - **KangarooTwelve – draft-05 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-kangarootwelve/
  - **Hybrid Public Key Encryption – draft-08 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hpke/
  - **FROST: Flexible Round-Optimized Schnorr Threshold Signatures – draft-00 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/
  - **CPace, a balanced composable PAKE – draft-01 – January 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/

Internet Engineering Task Force (IETF) (4 of 4)

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **Hashing to Elliptic Curves – draft-11 – April 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/
  - **Argon2 password hash and proof-of-work – draft-13 – March 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-argon2/
  - **Usage Limits on AEAD Algorithms – draft-02 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/
  - **OPAQUE Asymmetric PAKE Protocol – draft-03 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/
  - **OPRFs using Prime-Order Groups – draft-06 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/
  - **KangarooTwelve – draft-05 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-kangarootwelve/
  - **Hybrid Public Key Encryption – draft-08 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hpke/
  - **FROST: Flexible Round-Optimized Schnorr Threshold Signatures – draft-00 – February 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/
  - **CPace, a balanced composable PAKE – draft-01 – January 2021**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/

Next Steps – IDS WG

- Next IDS WG Meeting– May 27, 2021
- Next IDS Face-to-Face Meeting August 17-19, 2021 (probably August 19th) at next PWG Virtual F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG