HCD PP Version 1.1 Status

HCD PP Version 1.1 Status

Plan as of April 10th:

- Implement TD0393 to create the “final” HCD PP v1.1 text by end of April
- Submit to NIAP and JISEC for their review and approval as soon as possible thereafter

HCD PP Version 1.1 Status

- One question/concern:
  - In announcing TLS Package 1.1 NIAP indicated that “As new and updated PPs/PP-Modules are published, they will make use of this TLS package, where applicable.”
  - If we get HCD PP v1.1 approved by NIAP and JISEC, does that mean we automatically include TLS Package 1.1 by reference in place of FCS_TLS_EXT.1 that is currently in the HCD PP?

  Note: Per NIAP the answer is “YES”
- Based on this the HCD TC hasn’t yet decided whether or not to submit HCD PP v1.1 to NIAP/JISEC

HCD iTC Status

HCD iTC Status

- CCDB at its Oct 2018 Meeting chartered a CCDB Working Group (WG) containing the Korean and Japanese schemes. Goal was formation of the HCD iTC at the April CCDB meeting in Rome
- HCD WG is creating the following documents to be submitted to the CCDB for review at the April CCRA meeting:
  - Essential Security Requirements (ESR)
  - Terms of Reference (ToR)
- At the same time the HCD TC as creating its own versions of the same two documents plus a "Key Persons" document that will be referenced by the ToR

  Goal is to fold the HCD TC documents into the HCD WG versions that are submitted to the CCDB

HCD iTC Status - Essential Security Requirements

- HCD TC members are reviewing the HCD WG draft ESR and will submit comments
  - Deadline for review: May 24th, 2019
- HCD WG are welcome any improvement for the ESR if it is "helpful to increase the security level of hardcopy devices"
- To help the review, I created a comparison by section of the latest draft ESR created by the HCD TC to the latest draft ESR provided by the HCD Working Group.

HCD iTC Status - Essential Security Requirements

- Some key differences between the two versions are:
  - Definition of what a Hardcopy Device is and associated use cases
  - Protection of TSF Protected and Confidential Data vs. Protection of HCD Critical Data
  - “HCD shall support testing of some subset of its security functionality to help ensure that the subset is operating properly.” vs. “The HCD shall test some subset of its security functionality to ensure that the security functionality is not compromised by the detectable malfunction.”
  - HCD TC version has the following ESR not in HCD WG version:

    HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications

HCD iTC Status - Essential Security Requirements

- Some key differences between the two versions are:
  - HCD WG version has the following two ESRs not in HCD TC version:

    The HCD shall ensure logical separation of the PSTN and the LAN if it provides a PSTN faxing function.

    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 so 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

HCD iTC Status – Terms of Reference

- HCD TC shared the draft version of HCD iTC ToR to HCD WG (ITSCC, JISEC). HCD WG reviewed the draft ToR that was provided by HCD TC and had one major comment:
  - Wanted more details on the voting and decision process than the simplified process we borrowed from the OSPP iTC
- HCD TC resolved the comment by including from original draft; HCD WG accepted revised ToR and submitting it to the CCDB.
- CCDB ToR voting is not initiated yet. To make a progress, ITSCC (Korean Scheme) will remind the CCDB Chair about it. Also, HCD TC will continuously check the CCDB/CCMC voting progress

HCD iTC Status – “Key Persons” List

- HCD TC (Kwangwoo Lee) requested several HCD stakeholders to invite the SME(s) list of HCD iTC. According to the feedbacks of each organization, HCD TC created a draft Hardcopy Device International Technical Community – Key persons and affiliations
  - Made key roles ‘TBD’
- Document submitted to HCD WG and accepted. Will be forwarded to CCDB.
- The Status of Subject Matter Experts
  - Industry SMEs: 30 members 14 organizations
  - Lab SMEs: 15 members 9 organizations
  - Certification Body SMEs: 4 members 3 schemes (KR, JP, SE)
    - Waiting the official feedback from 2 schemes (US, SE)
  - Other SMEs: 4 members (IEEE-ISTO PWG experts/Biometric iTC expert

HCD CPP v1.0

HCD cPP v1.0

- Issues that should be considered for HCD cPP v1.0
  - HCD PP v1.1 comments that are open or deferred
  - Parking Lot issues from the development of HCD PP v1.0 (see backup slides)
  - Impact of recently approved NIST SP 800-131A and NIST SP 800-56B updates as they relate to:
    - Sunset of cipher suites with SHA1
    - Sunset of cipher suites with RSA Key Generation with keys < 2048 bits
  - Inclusion of requirement to include TLS 1.3 and removal of requirement to include TLS 1.1
  - Implementing the high-level requirements that are in the ESR approved by the CCDB
  - Updating Assurance Activities

HCD cPP v1.0

- Issues that should be considered for HCD cPP v1.0
  - NIAP TLS Package
    - Splitting up of separate requirements for TLS as a client and TLS as a server.
    - Elimination of support for any ‘SHA’ TLS cypher suites except for TLS_RSA_WITH_AES_128_CBC_SHA
    - The selection of TLS supporting ‘mutual authentication’ and ‘session renegotiation and the TLS requirements for each of the two if either is supported.
    - New requirement for TLS as a client if any ECDHE or ECDHA cipher suites are selected in FCS_TLSS_EXT.5.
    - Inclusion by reference of FIA_X509_EXT.1 (X.509 Certificate Validation) and FIA_X509_EXT.2 (X.509 Certificate Authentication) from NDcPP (see backup slides)
      - Support for OCSP

HCD cPP v1.0

California "Password" Law

- As of Jan 1, 2020 each connected device must ensure that either:
  - The preprogrammed (aka "default") authentication password is unique to each device manufactured or
  - The device contains a security feature that requires a user to generate a new means of authentication (i.e., a new authentication password) before access is granted to the device for the first time

NIST SP 800-171

- As of Jan 1, 2018 requires among other things that we
  - Prohibit password use for a specified number of generations
  - Allow temporary password use for system logons with an immediate change to a permanent password

HCD cPP v1.0

- More Issues that should be considered for HCD cPP v1.0
  - Privacy issues (e.g., GDPR)
  - Use of TPMs and SEDs and SSDs
  - Securing the default configuration
  - Integrating the work of the CCDB Cryptographic Working Group’s cryptographic catalog
  - Impact of FIPS 140-3 which essentially points to ISO 19790
  - Implementing the latest NIST cryptographic algorithms and guidance
  - More specific requirements around the concepts of secure boot, roots of trust, etc. under the umbrella of a “trusted computing environment”
  - Dedicated security components

HCD iTC and HCD cPP v1.0

- Potential Schedule for creation of HCD cPP v1.0
  - CCMC approval of creation of HCD iTC – July 2019
  - First HCD iTC F2F Meeting – Sep 2019
  - First draft of HCD cPP v1.0 – Apr 2020
  - Updated draft of HCD cPP v1.0 – Oct 2020
  - HCD cPP v1.0 submitted for approval by HCD iTC membership – Feb 2021
  - HCD cPP v1.0 submitted to CCDB for approval – Mar 2021
  - HCD cPP v1.0 published – Apr 2021

HCD Security Guide Status

Next Steps

- Submit HCD PP v1.1 to NIAP/JISEC and get it approved
- Implement the transition from the HCD TC → HCD iTC
  - Determine and install “officers”
  - Set up meeting cadence, iTC membership, etc.
  - Have the first iTC meeting
- Reconcile any gaps between the HCD WG version and the HCD TC version of the ESR
- Start work on HCD cPP v1.0
  - Develop plan for development, review and release of HCD cPP v1.0
  - Determine content scope
  - Initiate “transition” of HCD PP v1.1 into first draft
  - Update and review drafts as necessary to create “final” version
  - Get iTC review and approval for “final” version
  - Release HCD cPP v1.0

Support for Other Standards Activities Related to HCD Security

Potential Standard Body “Targets”

- IETF (Internet Engineering Task Force) - FREE!
  TLS (Transport Layer Security) WG
  -- vendors, cryptographers, and gov't agencies worldwide

- SACM (Security Automation and Continuous Monitoring)
  -- heavy TCG and US gov't participation - "son of SCAP"

- RATS (Remote ATtestation ProcedureS) - brand new!
  -- device and entity attestation - heavy TCG, GP, ARM, USG participation

- SAAG (Security Area Advisory Group)
  -- heads-ups on new and ongoing security work

- IRTF CFRG (Internet Research Task Force Crypto Forum RG)
  -- pre-eminent group of cryptographers and security experts!

Potential Standard Body "Targets"

(2) TCG (Trusted Computing Group) - $15K/year for corporations
-- Ricoh, Canon, Google, Qualcomm, Samsung, Infineon, NXP, etc. members

- TPM (Trusted Platform Module)
  -- voting TPM 2.0 r1.55 out for public review *and* publication

- TNC (Trusted Network Communications)
  -- heavy collaboration w/ IETF NEA, SACM, RATS, and others

- EmSys (Embedded Systems)
  -- SGs on Network Equipment, IoT, Industrial, Vehicles, etc.
  -- home of former Hardcopy Device WG

- MPWG (Mobile Platform WG) and TMS (Trusted Mobility Solutions) WG
  -- mobile phones, telecom networks, 4G and 5G w/ ETSI, 3GPP, GP, etc.

Potential Standard Body “Targets”

(3) US NIST - FREE!

- LWC (Lightweight Cryptography)
  -- for resource-constrained devices (including mobile phones)

- TC (Threshold Cryptography)
  -- multi-party signatures and encryption algorithms - hot stuff!

- * CF (Cybersecurity Framework)

- PQC (Post-Quantum Crypto)

- SWID (Software Identification Tags)
  -- underlies runtime integrity and remote attestation work

- SWA (Software Assurance)
  -- series of F2F workshops (Wash, DC) and NIST publications