IDS Conference Call Minutes
June 13, 2019

This IDS Conference Call was stated at approximately 3:00 pm ET on June 13, 2019.

Attendees

Cihan Colakoglu	Kyocera
Gerardo Colunga	HP
Erin Huber	Xerox
Smith Kennedy	HP
Brian Smithson	Ricoh
Alan Sukert	Xerox
Bill Wagner	TIC
Rick Yardumian	Canon

Agenda Items

1. The topics to be covered during the Conference Call were:
   - HCD PP Version 1.1 Status
   - HCD iTC Status (from the minutes of the June 3rd Hardcopy Device (HCD) Technical Community (TC) Teleconference)
   - Support for Other Standards Activities Related to HCD Security

   Note: We wanted to cover HCD Security Guide Status, but Ira could not make this meeting, so this topic was deferred to the next Conference Call.
2. The main points discussed at the Conference Call were as follows:
   - We went through the minutes from the June 3rd HCD TC Conference Call. Key points were:
     - We reviewed the 9 HCD TC comments submitted to the HCD Working Group's draft Essential Security Requirements (ESR) document. Of the 9 comments 6 were submitted to the HCD WG for its consideration.
     - The vote by the Common Criteria Development Board (CCDB) of the draft Terms of Reference (ToR) document for the proposed HCD international TC (iTC) is still going on and will be completed by the end of June. No word on the voting results to date. If the CCDB approves the ToR it will be sent to the CC Management Committee (CCMC) for its approval; once the CCMC approval of the ToR is obtained, we can form the HCD iTC.
     - Still waiting for confirmation from NIAP that if we update the HCD PP we will have to incorporate the NIAP TLS Package. This is a "showstopper" for submitting HCD PP v1.1 to NIAP and JISEC for approval. Until we have confirmation one way or the other HCD PP v1.1 submittal is on hold.
   - Al mentioned Ira McDonald's list of current standards activities with some relevance to HCD security that we discussed at the last IDS Conference Call. Al indicated that if anyone on the call wanted to be involved in any of these standards activities they should go ahead and do so and update the IDS WG with status as appropriate. The list of standards activities that Ira McDonald provided was as follows:

     (1) IETF (Internet Engineering Task Force) - FREE!

     - TLS (Transport Layer Security) WG
       -- https://datatracker.ietf.org/wg/tls/charter/
       -- vendors, cryptographers, and gov't agencies worldwide

- * SACM (Security Automation and Continuous Monitoring)
  -- https://datatracker.ietf.org/wg/sacm/about/
  -- heavy TCG and US gov't participation - "son of SCAP"
- * RATS (Remote ATtestation ProcedureS) - brand new!
  -- https://datatracker.ietf.org/wg/rats/about/
  -- device and entity attestation - heavy TCG, GP, ARM, USG participation
- * SAAG (Security Area Advisory Group)
  -- https://www.ietf.org/mailman/listinfo/saag
  -- heads-ups on new and ongoing security work
- * IRTF CFRG (Internet Research Task Force Crypto Forum RG)
  -- https://datatracker.ietf.org/rg/cfrg/about/
  -- pre-eminent group of cryptographers and security experts!

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

- * TPM (Trusted Platform Module)
  -- https://trustedcomputinggroup.org/work-groups/trusted-platform-module/
  -- voting TPM 2.0 r1.55 out for public review *and* publication
- * TNC (Trusted Network Communications)
  -- https://trustedcomputinggroup.org/work-groups/trusted-network-communications/
  -- heavy collaboration w/ IETF NEA, SACM, RATS, and others
- * EmSys (Embedded Systems)
  -- https://trustedcomputinggroup.org/work-groups/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
  -- https://trustedcomputinggroup.org/work-groups/mobile/
  -- mobile phones, telecom networks, 4G and 5G w/ ETSI, 3GPP, GP, etc.

(3) US NIST - FREE!
- * LWC (Lightweight Cryptography)
  -- https://www.nist.gov/programs-projects/lightweight-cryptography
  -- for resource-constrained devices (including mobile phones)
- * TC (Threshold Cryptography)
  -- https://csrc.nist.gov/Projects/Threshold-Cryptography
  -- multi-party signatures and encryption algorithms - hot stuff!
- * CF (Cybersecurity Framework)
  -- https://www.nist.gov/cyberframework
- * PQC (Post-Quantum Crypto)
  -- https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
- * SWID (Software Identification Tags)
  -- https://csrc.nist.gov/Projects/Software-Identification-SWID
  -- see also https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/
  -- underlies runtime integrity and remote attestation work
- * SWA (Software Assurance)
  -- https://www.nist.gov/itl/ssd/software-assurance
  -- series of F2F workshops (Wash, DC) and NIST publications

- Bill asked about Scheme support for the proposed HCD iTC. As of now we know that Japan, Korea and Sweden have committed resources to support this iTC, NIAP indicated it supports the iTC but cannot provide any resources for it and Canada appears to be supporting the iTC but hasn't made any type of "official" position.

Actions: No actions from this Conference Call

Next Steps

- The next IDS Conference Call is scheduled for Jun 27, 2019 at 3:00P ET / 12:00N PT. If we don't have anything to discuss the meeting will be canceled.
- We will have an IDS Conference Call on Jul 11, 2019 at 3:00P ET / 12:00N PT to review the results of the June 8th HCD TC Conference Call.

This IDS Conference Call was completed at approximately 3:30 pm ET on Jun 13, 2019.