IDS Conference Call Minutes
April 16, 2020

This IDS Conference Call was stated at approximately 3:00 pm ET on April 16, 2020.

Attendees

Cihan Colakoglu	Kyocera
Gerardo Colunga	HP
Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Erin Huber	Xerox
Ira McDonald	High North
Alan Sukert	Xerox
Rick Yardumian	Canon

Agenda Items

1. The topics to be covered during this Conference Call were:
   - Results of the 04/07/2020 Hardcopy Device (HCD) international Technical Committee (iTC) meeting.
   - Status of the HCD Security Guidelines
   - Next Steps for the IDS Working Group
2. Al stated that now that he has retired from Xerox, he has joined the PWG as an Individual member and thus will continue per the PWG process as IDS Chair at least in the near future.
3. Al reviewed the minutes from 04/07/2020 Hardcopy Device (HCD) international Technical Committee (iTC) meeting which are included below:

   

   2020-04-07 HCDiTC BiweeklyTeleconferenc

   The key points discussed during review of the minutes were:

   - There was much discussion about the process we are using to convert the HCD PP v1.1 which is in MS Word format into the baseline HCD collaborative PP (cPP) and HCD Supporting Document (SD) versions 1.0 which are in asciidocs format. Basically, what we are doing is “cutting and pasting” the various portions of the HCD PP v1.1 into the appropriate sections of the HCD cPP and HCD SD and then adding the appropriate asciidocs syntax.

     Ira provided the following link to a curated list of a large number of AsciiDoc tools (editors, etc.) - https://github.com/bodiam/awesome-asciidoc - that may be useful to the HCD CPP and SD editors. Ira also the official AsciiDoctor suggestion to use Pandoc to convert MS Word ".docx" files to AsciiDoc (with a list of supported features): https://asciidoctor.org/docs/migrating-from-msword/ the link to Pandoc: https://pandoc.org/.
   - Alan indicated that the three editors – myself, Jerry Colunga and Brian Volkoff – met after the meeting and split up the editing work as follows: Brian will finish creating the baseline HCD cPP v1.0 from the HCD PP v1.1, Jerry will create the baseline HCD SD v1.0 from the HCD PP v1.1 and Al will help the two as needed and focus on other tasks such as creating the work plan.
   - Ira indicated that he attended the ND iTC meeting earlier that day and that TLS 1.3 will not be included in the ND cPP until at least ND cPP v3.x (they are currently at ND cPP v2.2). He feels that for the HCD cPP TLS 1.3 will have to me made part of a standard TLS module that is the

output from the TLS Task Force that can (and will) be used across multiple cPPs that have TLS requirements such as mobile, biometrics, as well as HCD.

Ira also indicated that there is a small update to ND cPP v2.2 coming with just editorial changes. Ira then gave a quick update of the ND iTC subgroup status. The only meaningful updates are that:

- the X.509 subgroup is looking at trustors,
- the TLS subgroup is deferring work on DTLS at the present time and
- the ND NIT (the Interpretation Team) is essentially on hold at this time. Because of this if an ND product in evaluation needs some type of interpretation the ND iTC will work with the applicable evaluation lab to determine an appropriate course of action to keep the evaluation moving forward.

- We are still planning on the aggressive schedule below of having an HCD cPP v1.0 issued within 24 months, which means sometime in 2Q 2022. That means that we will need a 1st working draft probably in 3Q 2020 (that would be basically the baseline draft) and then the 2nd baseline draft which would be the first real draft with the planned content for HCD cPP v1.0 for a more general review in 2Q 2021.
- The HCD PP v1.1 which we never got approved by NIAP is still going to be the basis for HCD cPP v1.0. The key will be determining what additional requirements to add while keeping the scope constrained enough to have a chance to meet the 24-month goal. The keys will be coming up with a prioritized list of what requirements need to go into HCD cPP v1.0 and establishing early on a set of agreed-upon ground rules on how we'll agree on that prioritized list and where the cutoff on the list will be.
- It was mentioned that because of the shutdown due to the coronavirus NIAP has been totally shut down indefinitely. That has impacts in terms of the fact NIAP is responsible for updating the Common Criteria portal and of course any certifications that were in process in NIAP. However, evaluation labs are still working and evaluations that were started under NIAP can still move forward until they get to the point where some type of NIAP action is required.

4. Ira indicated that he has done no work on the HCD Security Guidelines.
5. Al then went into the last topic which was about the next steps for the IDS Working Group. Al would like to expand the outreach of the IDS WG to go beyond just the HCD iTC because there are other standards activities on-going withing the various communities that impact either directly or indirectly HCDs and imaging devices. Al then went through a list of standards bodies that Ira had put together almost a year ago back in April 2019 that the IDS WG must consider looking at - that list is included as Attachment 1 to these minutes.

   Ira went through the various standards bodies listed in the attachment. The two that Ira singled out that we might want to focus on first were:

   - RATS (Remote ATtestation ProcedureS)
   - IRTF CFRG (Internet Research Task Force Crypto Forum RG)

   but he did indicate that all of them were worth pursuing. In the coming weeks we will start investigating some of these and determine which ones we should start following as a WG.

Actions:

There were no actions that resulted from this call.

Next Steps

- The next IDS Conference Call is scheduled for April 30, 2020 at 3:00P ET / 12:00N PT

IDS Conference Call Minutes
April 16, 2020

This IDS Conference Call was completed at approximately 4:05 pm ET on April 16, 2020.

IDS Conference Call Minutes
April 16, 2020

Attachment 1
Potential Standards Efforts to Be Watched

(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