The Printer Working Group

Imaging Device Security

May 07, 2020

PWG May 2020 Virtual Face-to-Face

Agenda

When	What
10:00 – 10:05	Introductions, Agenda review
10:05 – 11:15	Discuss results of latest HCD iTC Meetings and potential HCD cPP v1.0 content
11:15 – 11:30	HCD Security Guidelines 1.0 Status
11:30 – 11:50	Status of other HCD Security Standards Efforts
11:50 – 12:00	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 Guidelines

HCD international Technical Community (iTC) Status

HCD international Technical Community (iTC)

- HCD iTC formally approved by Common Criteria Management Committee in Feb 2020
- Key HCD iTC Officers:
  - Chairperson – Kwangwoo Lee, HP
  - Deputy Chairperson – Alan Sukert
  - CCDB Liaison - Eunkyoung Yi, Korean Scheme
  - Editors – Alan Sukert; Brian Volkoff, Ricoh; Geraldo Colunga, HP
  - Record Manager – TBD (Kwangwoo Lee acting for now)
- April HCD TC F2F in Burlington MA was cancelled
- Agreed to hold bi-weekly meetings. Meetings have been held on:
  - 02/14/2020
  - 03/20/2020
  - 04/07/2020
  - 04/28/2020

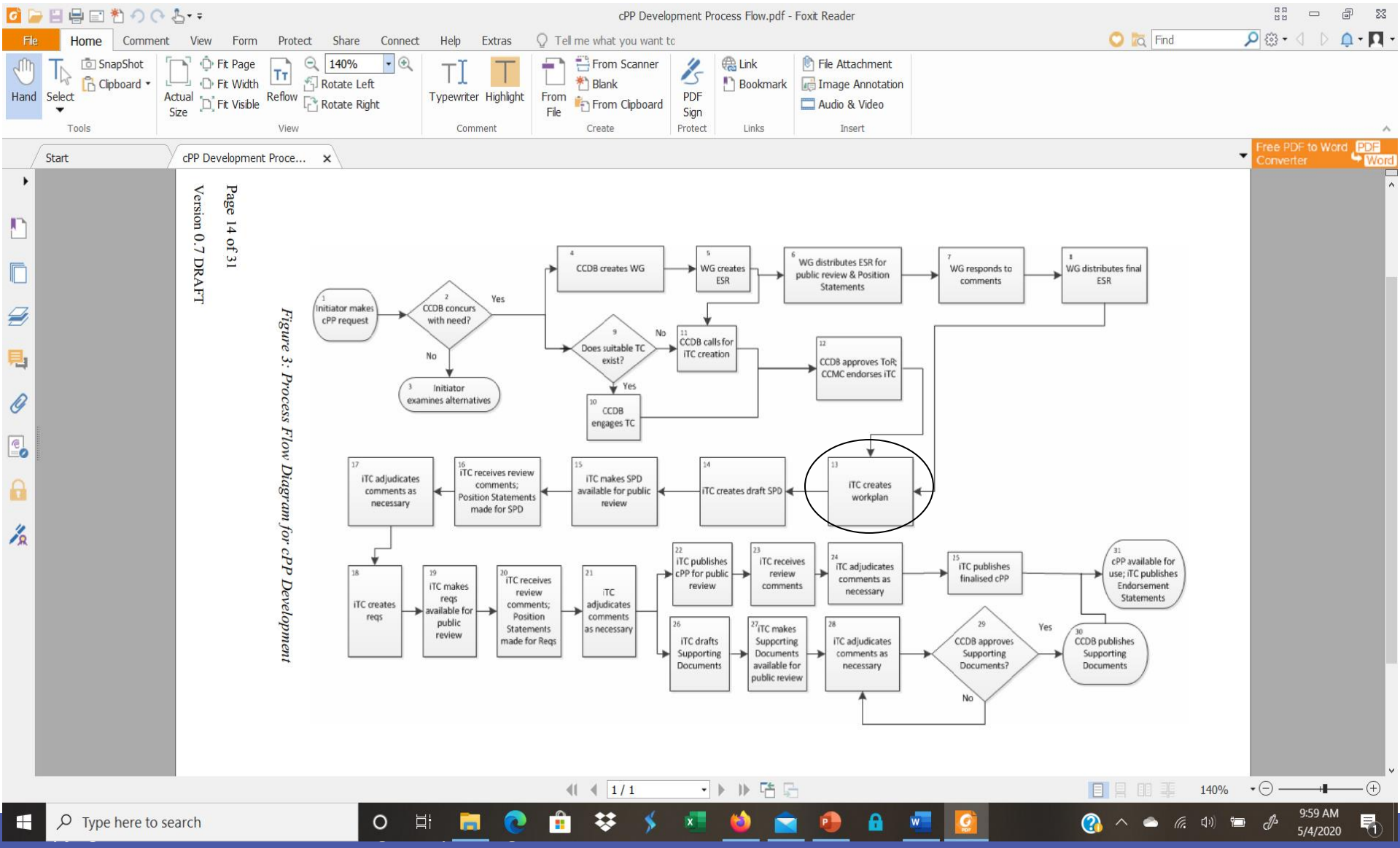
HCD iTC Status

- Essential Security Requirements (ESR)
  - Version developed by HCD Working Group (WG) (Korean and Japanese Schemes) approved by Common Criteria Development Board (CCDB)
  - Version developed by HCD Technical Committee that is slightly different from the HCD WG version
    - Biggest differences are in areas of (1) inclusion of requirement to verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications and (2) requirement to encrypt user data/confidential data stored on any type of non-volatile memory.
  - Next step is to get agreement with HCD WG on a “sync’d” version of the ESR

HCD iTC Status

- Terms of Reference (ToR)
  - Approved by the CCDB after some back-and-forth between the HCD TC and the HCD WG
  - No changes expected at this time although if needed the ToR can be changed
- HCD Key Persons Document
  - Latest version is 0.85
  - HCD iTC SMEs status (71)
    - Industry SMEs (38)
    - Lab SMEs (20)
    - Certification Body SMEs (5)
    - Other SMEs (8)

HCD iTC Status
cPP Development Process Flow



HCD iTC Status

- Collaboration Tool Updates
  - GitHub repositories for HCD iTC set up with templates based on CCUF Tools WG Templates that are in asciidocs
  - Editors group met to sync up the tasks that need to be performed
  - Draft templates structure prepared and shared with editors for detailed changes such as SFRs and Annex.
  - Plan is to use the proposed HCD Protection Profile (PP) v1.1 (which was never approved or issued) as the baseline for HCD collaborative PP (cPP) v1.0 and then add on content as agreed upon by the HCD iTC to form the eventual published HCD cPP v1.0.
    - Take the applicable portions of the HCD PP v1.1 (which are in MS Word) that deal with requirements and put them into the cPP template to form the baseline HCD cPP v1.0
    - Take the applicable portions of the HCD PP v1.0 (which are in MS Word) that deal with assurance activities and put the into the Supporting Documents (SD) template to form the baseline HCD SD v1.0
  - Right now is a "cut and paste" operation; looking at automated tools to streamline the operation

HCD iTC Status

- Editor Status
  - Draft Work Plan has been created and is being reviewed by Kwangwoo before being distributed to iTC members.
  - Brian V. is working on the draft cPP with some detail changes such as SFRs, Annex, and Asciidoc tasks. Brian was to finish this task for everything but the Appendices by the end of last week. The estimated delivery time to team will now be end of this week
  - Jerry is going to do the Support Document. The draft SD will be completed by the next HCD iTC meeting on 5/14
  - Ira requested whether we can have line number for easy review and comment
    - I checked and asciidocs does not support line numbers very easily at all. To add line numbers we'll have to do some type of post-processing if that is possible.

HCD iTC Status

- TLS 1.3: Ira McDonald (Draft: June 2020)
  - AI: Kwangwoo to share the CCUF Trondheim April 2018 slides that presented by Tony Boswell. These slides are described how update on ND cPP/SD versioning
    - https://ccusersforum.onlyoffice.com/Products/Files/doceditor.aspx?fileid=5689766
    - https://ccusersforum.onlyoffice.com/Products/Files/doceditor.aspx?fileid=5684415
  - AI: Ira to check whether NDcPP keep the same timeline & versioning schedule that mentioned in Trondheim
  - Updated Compact TLS

HCD iTC Status

- Hardware-anchored integrity verification: Jerry Colunga (Draft: June 2020)
  - Not so much progress. Jerry will make a progress and share it at the next HCD iTC meeting.
  - AI: DSC has published the candidate cPP (v1.0). Jerry will review DSC cPP v1.0 document.
  - DSC cPP v1.0 draft
    - https://www.commoncriteriaportal.org/communities/docs/cpp_dsc_v10d_DRAFT_20200224.docx
  - Latest DSC Status
    - https://www.commoncriteriaportal.org/files/communities/Status.DSC.pdf
- SED & HDD Encryption: Alan Sukert (Draft: June 2020)
  - No new updates to either FDE AA cPP/SD or FDE EE cPP/SD planned
  - Only Interpretation Team (IT) activity going on with FDE iTC
    - Latest IT activity and NIAP Technical Decisions do not appear to be in areas that impact either HCD CPP or HCD SD.

HCD iTC Status – Additional Questions

- Versioning (version x.y or even x.y.z)
  - HCD iTC needs to determine:
    - What constitutes a major (x) vs. a minor version (y or y.z) in terms of content
    - Frequency of major vs. minor versions
      - Major updates every 12 months vs every 18 months vs. every 24 months?
      - Minor updates every 6 months or 9 months?
- EAL vs PP compliance
  - Some European countries still require EAL certifications
  - HCD PP does not specify an EAL; just specifies PP Compliance
  - HCD cPP template is written around EAL1 so could technically specify EAL1
  - What do we do with the HCD cPP?

HCD iTC Status – Additional Questions

- Exact Compliance
  - HCD PP requires exact compliance because NIAP requires it
  - Should the HCD cPP require exact compliance?
- Copyright
  - Are there any copyright issues we need to be concerned about in developing the HCD cPP and HCD SD?
  - There weren't any in developing the HCD PP but we were only dealing with FIPS and NIST referenced documents. Now we are dealing with ISO/IEC referenced documents.

HCD cPP V1.0 Proposed Content – My Thoughts as HCD iTC Deputy Chair

- KISS – KEEP IT SIMPLE STUPID! Or in other words – don't try to do too much in v1.0; we can't solve everything in two years.
- Just cover the basic requirements that HCD vendors will need in the 2022 time frame.
- We should plan for a v1.1 by the end of 2022 to cover any key SFRs we can't get into v1.0.
- We need to keep in sync with the changes in the Network Device cPP but we can't let the ND iTC control what we do either – there has to be a balance because HCDs are difference in many ways for other network devices
- We have to anticipate what is coming (e.g., FIPS 140-3, sunsetting SHA-1) as much as possible over the next two years in determining what SFRs to add/modify

MY HCD cPP V1.0 Proposed Content beyond what is in HCD PP v1.1

- Support for FIPS 140-3
- Removal of all SHA-1 support
- Removal of support for TLS 1.0 and TLS 1.1
- Implement the TLS and SSH packages coming from the CCDB Crypto Working Group
- **IF rolled out in next 6-12 months via a TLS package or via ND cPP**, support for TLS 1.3
- Implement any new NIAP TDs against the HCD PP
- Implement any ND cPP changes, any new NIAP TDs against the ND, FDE AA or FDE EE cPPs or any FDE AA cPP/FDE EE cPP interpretations that the HCD iTC determines are applicable
- Anything that the HCD iTC as a group determines is an "absolute must have" in v1.0; anything less has to go in v1.1 or later

HCD iTC – Next Steps

- Approve the Work Plan
- Complete the baseline HCD cPP v1.0 and HCD SD v1.0
- Agree on the HCD cPP v1.0 and HCD SD v1.0 Content
- Implement the Work Plan
  - Complete the HCD cPP/SD v1.0 drafts
  - Complete internal reviews/update of the HCD cPP/SD v1.0 drafts
  - Update the HCD cPP/SD v1.0 drafts to address internal review comments
  - Public review of the final HCD cPP/SD v1.0 version
  - Update HCD cPP/SD v1.0 to address final comments
  - Get CCDB approval of HCD SD v1.0
  - Publish HCD cPP/SD v1.0

* - May be more than one draft

Proposed HCD cPP V1.0 Timeline

- Complete the HCD cPP/SD v1.0 drafts – Jul 2021
- Complete internal reviews/update of the HCD cPP/SD v1.0 drafts – Aug - Sep 2021
- Update the HCD cPP/SD v1.0 drafts to internal review comments – Oct 2021
- Public review of the final HCD cPP/SD v1.0 version – Nov – Dec 2021
- Update of final HCD cPP/SD v1.0 to address final review comments – Jan 2021
- Get CCDB approval of HCD SD v1.0 – Feb 2022
- Publish HCD cPP/SD v1.0 – Mar/Apr 2022

HCD Security Guidelines Status

HCD Security Guidelines Status

- HCD Security Guidelines Development Schedule
  - Next Interim Draft Q2 2020
  - Prototype Draft Q4 2020 / Q1 2021
- HCD Security Guidelines Development Plan
  - 1 Intro – complete
  - 2 Terminology – complete
  - 3 Rationale – complete
  - 4 HCD Network Security - first new text
    - Key topics first - e.g., firewall, SSH, TLS, IPP
  - 5 HCD Local Security - second new text
    - Key topics first - e.g., operating systems, local secure peripherals
  - 6 HCD System Architecture - third new text
    - Key topics first - e.g., system isolation, process isolation

HCD Security Guidelines Status

- HCD Security Guidelines Development Plan (cont'd)
  - 7 Conformance - last new text
  - 8 Internationalization Considerations - last new text
  - 9 Security Considerations - last new text
  - 10 References – ongoing
  - 11 Authors Addresses – ongoing
  - 12 Appendix A - Internet Protocol Suite - complete

Latest interim draft from Jan 2020:
https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20200120-rev.pdf

Other HCD Security Standards Activities

Potential Standards Activities 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"

* SAAG (Security Area Advisory Group)

-- https://www.ietf.org/mailman/listinfo/saag

-- heads-ups on new and ongoing security work

* RATS (Remote ATtestation ProcedureS) - brand new!

-- https://datatracker.ietf.org/wg/rats/about/

-- device and entity attestation - heavy TCG, GP, ARM, USG participation

* IRTF CFRG (Internet Research Task Force Crypto Forum RG)

-- https://datatracker.ietf.org/rg/cfrg/about/

-- pre-eminent group of cryptographers and security experts!

Potential Standards Activities To Be Watched

(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.

Potential Standards Activities To Be Watched

(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

Potential Standards Activities To Be Watched

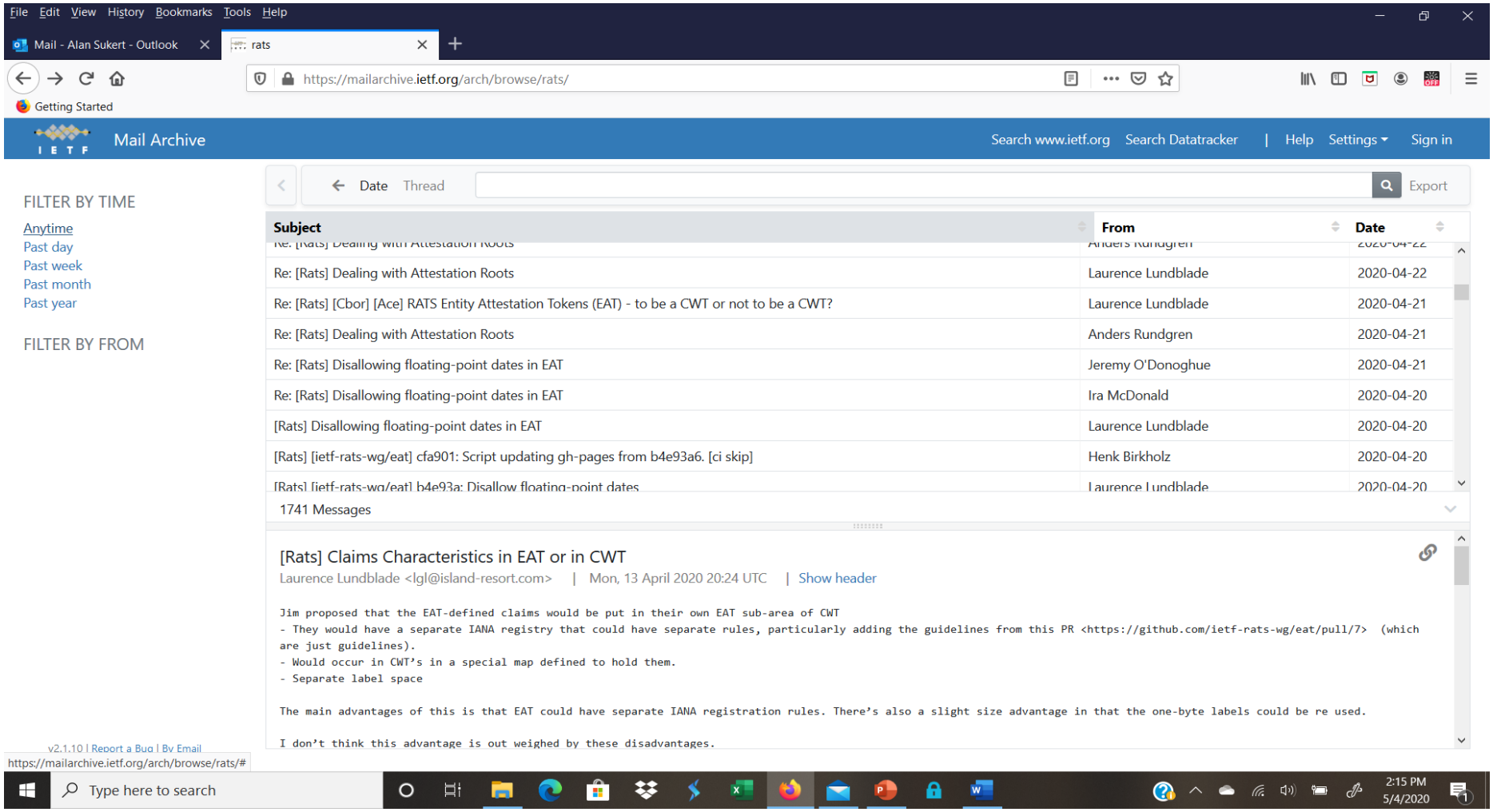
* RATS (Remote ATtestation ProcedureS)

About RATS

In network protocol exchanges, it is often the case that one entity (a Relying Party) requires Evidence about a remote peer to assess the peer's trustworthiness, and a way to appraise such Evidence. The evidence is typically a set of claims about its software and hardware platform. This document describes an architecture for such remote attestation procedures (RATS).

Potential Standards Activities To Be Watched

* RATS (Remote ATtestation ProcedureS)



Potential Standards Activities To Be Watched

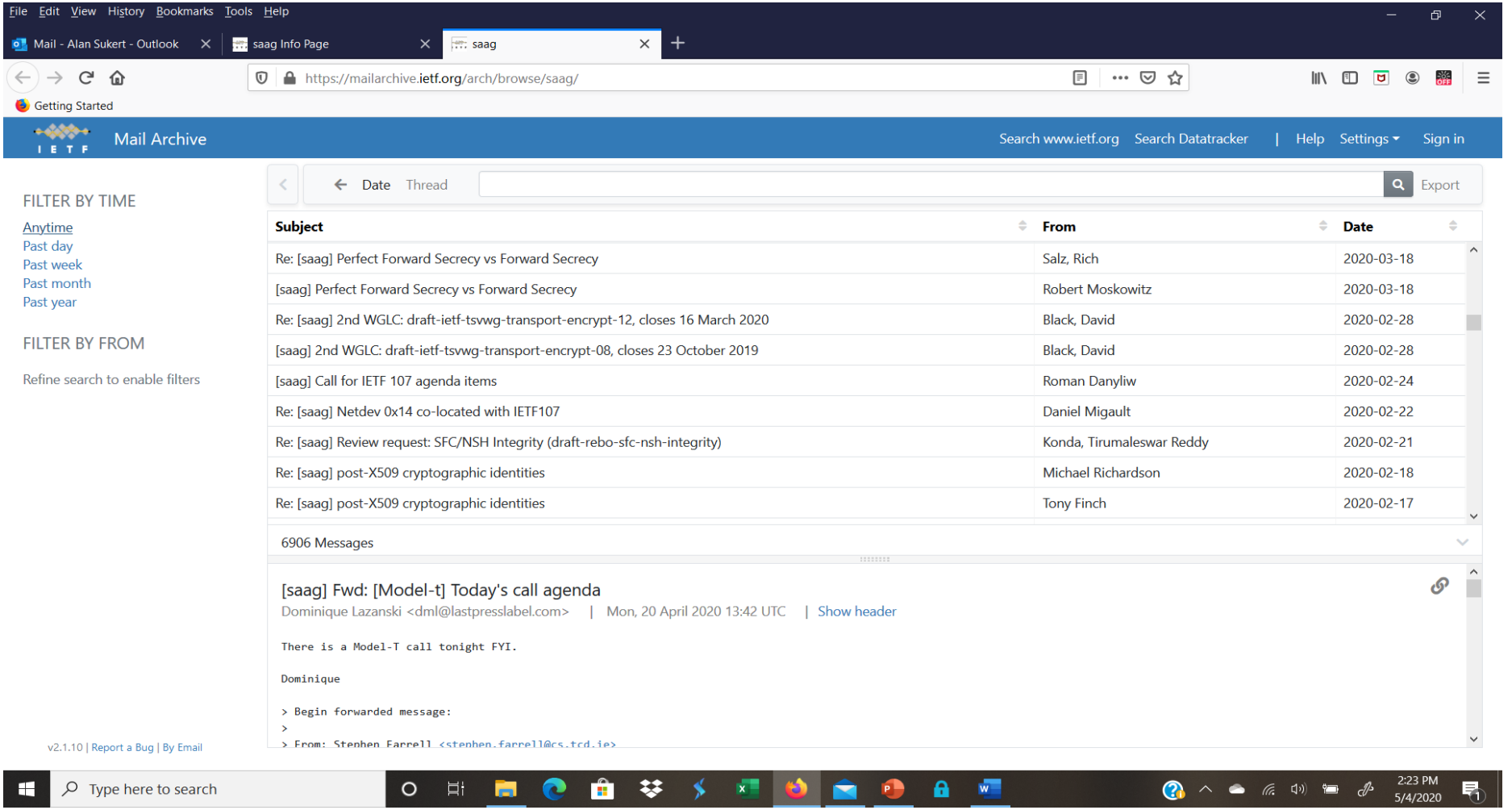
* SAAG (Security Area Advisory Group)

About SAAG

The SAAG List is the IETF mailing list for the Security Area Advisory Group which meets once at each IETF meeting as part of the Security Area.

Potential Standards Activities To Be Watched

* SAAG (Security Area Advisory Group)



Next Steps – IDS WG

- Next IDS Conference Call – May 28, 2020
- Next IDS Face-to-Face Meeting Aug 26-27 (probably Aug 27), 2020 at next Virtual PWG F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG