Security Area Advisory Group

Notes: https://notes.ietf.org/notes-ietf-118-saag

Meetecho (full client): https://meetings.conf.meetecho.com/ietf118/?session=31634

Meetecho (on-site): https://meetings.conf.meetecho.com/onsite118/?session=31634

Roman Danyliw

Paul Wouters

IETF 118

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

Living the IETF Code of Conduct

Reminder of the key points of the Code of Conduct [RFC7154]:

1. IETF participants extend respect and courtesy to their colleagues at all times
2. IETF participants have impersonal discussions
3. IETF participants devise solutions for the global Internet that meet the needs of diverse technical and operational environments

IETF 118 meeting tips

In-person participants

- Make sure to sign into the session using the Meetecho (usually the “Meetecho lite” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*

Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

Agenda

1. Welcome, Administrivia, and Agenda Bashing (5 mins)

2. WG and AD Reports (15 mins, chairs/ADs)

3. Survey of "Newer Cryptography" being used in IETF work (Orie Steele, Chris Wood)

4. Open Mic (remaining time)

Helping out

1. If you are interested in becoming a WG chair, let your ADs know. Experience not always a plus!
2. Become a document Shepherd. Learn about IETF processes while helping advancing documents! Ask your AD if shepherding is right for you!
3. Errata processing - help your WG resolve reported erratas. We also have errata in closed WGs that no one is looking at.
4. Attend (virtual and in person) BoFs

WG Changes since IETF 117

BOF	Detecting Unwanted Location Trackers (DULT) Secure Patterns for Internet Credentials (SPICE)
Chartering	-
New	Key Transparency (KEYTRANS)
Closed	-
Rechartered	-
In Rechartering	OPENPGP, MLS and LAKE

Working Group Summaries

If you have highlights to share, please sent to saag@ietf.org

- ACE
- ACME
- COSE
- DANCE
- EMU
- GNAP
- IPSECME
- JOSE
- KEYTRANS
- KITTEN
- LAKE
- LAMPS
- MLS
- OAUTH
- OHAI
- OPENPGP
- PPM
- PQUIP
- PRIVACYPASS
- RADEXT
- RATS
- SATP
- SCITT
- SecDispatch
- SCIM*
- SUIT
- TEEP
- TIGRESS*
- TLS
- UTA*

* WGs currently in ART (some with responsible SEC ADs) that officially move to SEC when area reorgnizations occur before/at IETF 119

Related Non-SEC Area Activities

Security Topics in Related WGs

- ADD
- ANIMA
- DIME
- DISPATCH
- DMARC
- DPRIVE
- DRIP
- HTTPBIS
- QUIC
- NETCONF
- NTP
- OPSEC
- PERC
- SATP
- SFRAME
- SIDROPS
- STIR
- TAPS

Security Related IRTF

- CFRG
- PEARG
- UFMRG

IAB Programs

- (proposed) WHODIS

External related

- W3C
- IEEE
- ITU
- NIST Lightweight Crypto
- NIST PQC

WG Chair Changes

WG	Departures	Additions
SECDISPATCH	Kathleen Moriarty	Daniel Kahn Gillmor
SUIT	Russ Housley David Thaler	
KEYTRANS		Orie Steele Shivan Kaul Sahib
ACE	Daniel Migault	Tim Hollebeek

New Non-WG Mailing Lists

List Name	Purpose
N/A	

AD Sponsored Drafts

Draft	Sponsor	Status
draft-gutmann-testkeys	Paul	RFC Ed Queue
draft-yee-ssh-iana-requirements	Roman	RFC Ed Queue : EDIT
draft-josefsson-ntruprime-ssh	Roman	Waiting for AD Go-Ahead
draft-pismenny-tls-dtls-plaintext-sequence-number	<tbd>	<tbd>

Errata Processing

	Total Open Errata	Since Last Meeting	
		Closed	Reported
at IETF 118	295	-16	+15
at IETF 117	296	0	+8
at IETF 116	288	-3	+16
at IETF 115	275	-1	+10
at IETF 114	266	-15	+17
at IETF 113	264	N/A	N/A

Need help from: TLS, LAMPS, OAUTH, ACME, and EMU

SEC Area Pointers

Security Area

- https://wiki.ietf.org/en/group/sec

Common SEC AD DISCUSS items

- https://wiki.ietf.org/group/sec/typicalSECareaissues

Where is my document that is with AD?

- https://datatracker.ietf.org/doc/ad/roman.danyliw
- https://datatracker.ietf.org/doc/ad/paul.wouters

What is on the next IESG telechat?

- https://datatracker.ietf.org/iesg/agenda/documents/

Thanks to the SECDIR Reviewers

since IETF 117

- Alexey Melnikov
- Barry Leiba
- Brian Weis
- Carl Wallace
- Chris M. Lonvick
- Dan Harkins
- Daniel Migault
- David Mandelberg
- Deb Cooley
- Derrell Piper
- Donald E. Eastlake 3rd
- Hilarie Orman
- Ivaylo Petrov
- Kyle Rose
- Linda Dunbar
- Magnus Nystrom
- Mališa Vučinić
- Melinda Shore
- Mike Ounsworth
- Ned Smith
- Peter E. Yee
- Radia Perlman
- Rich Salz
- Rifaat Shekh-Yusef
- Robert Sparks
- Russ Housley
- Sean Turner
- Shawn M Emery
- Shivan Kaul Sahib
- Stephen Farrell
- Tero Kivinen
- Valery Smyslov
- Vincent Roca
- Watson Ladd
- Yaron Sheffer
- Yoav Nir

Thank you to Tero Kivinen for managing the reviews!

Open Mic