Security Area Advisory Group

CodiMD for notes: https://codimd.ietf.org/notes-ietf-111-saag

Meetecho link:
https://meetings.conf.meetecho.com/ietf111/?group=saag&short=&item=1

Benjamin Kaduk
Roman Danyliw

IETF 111

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)

Agenda

1. Welcome, Administrivia, and Agenda Bashing (5 mins)
2. WG Reports (10 mins)
3. AD Report (5 mins)
4. draft-richardson-saag-onpath-attacker (10 min, Michael Richardson)
5. How should the IETF approach Post-Quantum security? (30 min, Roman Danyliw and Ben Kaduk)
6. Open Mic

Working Group Summaries

GNAP

Chairs

- Leif Johansson
- Yaron Sheffer

Report

https://mailarchive.ietf.org/arch/msg/saag/H1aQjECDH6PLqCSmK_W8doTnUKk/

IPSECME

Chairs

- Tero Kivinen
- Yoav Nir

Report

https://mailarchive.ietf.org/arch/msg/saag/n54wb6EaBygFmGAXUwEfxgNp3u0/

LAMPS

Chairs

- Russ Housley
- Tim Hollebeek

Report

https://mailarchive.ietf.org/arch/msg/saag/-u7QujFO4B9VYDTrA9nupaAjAIw/

RATS

Chairs

- Nancy Cam-Winget
- Ned Smith
- Kathleen Moriarty

Report

https://mailarchive.ietf.org/arch/msg/saag/0VKfgspSO88jpX0Xm2VmHMDTLnI/

SACM

Chairs

- Chris Inacio
- Karen O’Donoghue

Report

https://mailarchive.ietf.org/arch/msg/saag/NhtLfQIxh6g0ngL1ImhP4AsyIss/

SecDispatch

Chairs

- Richard Barnes
- Kathleen Moriarty
- Mohit Sethi

Report

https://mailarchive.ietf.org/arch/msg/saag/iosyMsudHlmMkB6JuEhT_qhP5eM/

WGs meeting later in the week (1)

- ACE (https://mailarchive.ietf.org/arch/msg/saag/XC5CLEGyYvdf9sKwreYq3muc5PQ/)
- ACME (https://mailarchive.ietf.org/arch/msg/saag/tMEYUrd1Xbu7Nc2hL-M3VHomEL4/)
- COSE
- DOTS (https://mailarchive.ietf.org/arch/msg/saag/I6hv86VfBHbQyokpU1kOGbtSPXs/)
- EMU (https://mailarchive.ietf.org/arch/msg/saag/9VbsLxAvlTluyD0NGYR3wV8rng0/)
- LAKE
- PRIVACYPASS
- SUIT

WGs meeting later in the week (2)

- TEEP (https://mailarchive.ietf.org/arch/msg/saag/FRMLSaHNkiCcJ7hTi1deN5x1B9Y/)
- TLS

WGs not meeting at IETF 111

- CURDLE (https://mailarchive.ietf.org/arch/msg/saag/OX6KiJPqUXFTgDtRUcE12imF8bE/)
- I2NSF
- KITTEN (https://mailarchive.ietf.org/arch/msg/saag/yilM-Yf_9CLQRi6X_PaKkHYhipo/)
- MLS
- OAUTH
- OPENPGP (https://mailarchive.ietf.org/arch/msg/saag/UHftvUIz3eS4kjmVYJ5T6hgrWpU/)
- SECEVENT
- TRANS

Related Non-SEC Area Activities

Security Topics in Related WGs

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

BoFs

- DANISH
- SINS

Security Related IRTF

- CFRG
- PEARG

IAB Programs

- model-t

External related

- W3C
- IEEE
- ITU
- NIST Lightweight Crypto

AD Sponsored Drafts

Draft	Sponsor	Status
draft-foudil-securitytxt	Ben	RFC Editor
draft-gont-numeric-ids-sec-considerations	Ben	IESG::Waiting for Writeup
draft-housley-ers-asn1-modules	Roman	IETF LC till 2021-08-13
draft-eastlake-rfc6931bis-xmlsec-uris	Roman	With Author/Coordination with W3C

SEC Area Highlights

Common SEC AD DISCUSS items

- https://trac.ietf.org/trac/sec/wiki/TypicalSECAreaIssues

Where is my document that is with AD/IESG?

- https://datatracker.ietf.org/doc/ad/roman.danyliw
- https://datatracker.ietf.org/doc/ad/benjamin.kaduk

Thanks to the SECDIR Reviewers since IETF 110

- Adam Montville
- Alexey Melnikov
- Barry Leiba
- Carl Wallace
- Charlie Kaufman
- Chris Lonvick
- Christian Huitema
- Christopher Wood
- Dan Harkins
- Daniel Franke
- Daniel Migault
- David Mandelberg
- Derek Atkins
- Donald Eastlake
- Hilarie Orman
- Joseph Salowey
- Kyle Rose
- Linda Dunbar
- Loganaden Velvindron
- Magnus Nystrom
- Mališa Vučinić
- Melinda Shore
- Phillip Hallam-Baker
- Rich Salz
- Rifaat Shekh-Yusef
- Robert Sparks
- Russ Housley
- Scott Kelly
- Shawn Emery
- Stefan Santesson
- Tero Kivinen
- Tirumaleswar Reddy
- Valery Smyslov
- Vincent Roca
- Watson Ladd
- Yaron Sheffer

Attack Taxonomies

Post-Quantum Security for the IETF

Open Mic