Security Area Advisory Group

Benjamin Kaduk
Roman Danyliw
IETF 108

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. DOTS Overview (10 mins)
4. PKI vs. Pinning Applicability (10 mins)
5. BCP 72 updates (15 mins)
6. Open mic (remaining)

Working Group Summaries

ACE

Chairs

- Daniel Migault
- Jim Schaad

Report

https://mailarchive.ietf.org/arch/msg/saag/SX6mVLael0eN8HDDh-SoR_YK8jc/

ACME

Chairs

- Rich Salz
- Yoav Nir

Report

Meets next session

https://mailarchive.ietf.org/arch/msg/saag/cDyYqIcjThsYO2nim200EOEnpEM/

COSE

Chairs

- Matthew Miller
- Ivaylo Petrov

Report

https://mailarchive.ietf.org/arch/msg/saag/h2ufzztYTkmGIDe1oj2KMKf3Xy8/

CURDLE

Chairs

- Daniel Migault
- Rich Salz

Report

Did not meet

https://mailarchive.ietf.org/arch/msg/saag/MV5_VvFU30uV7AC9g3TJt2LlPCI/

DOTS

Chairs

- Valery Smyslov
- Liang Xia (Frank)

Report

Did not meet

https://mailarchive.ietf.org/arch/msg/saag/lD9sDys_6IoALSlfDanKd6GNjvU/

EMU

Chairs

- Joe Salowey
- Mohit Sethi

Report

https://mailarchive.ietf.org/arch/msg/saag/f2pTF09c_BKSPCxwCLGixl8O9_s/

GNAP

Chairs

- Leif Johansson
- Yaron Sheffer

Report

https://mailarchive.ietf.org/arch/msg/saag/iBK8ddKPUcNJsveOvpW7r2W5aZM/

I2NSF

Chairs

- Linda Dunbar
- Yoav Nir

Report

Did not meet

IPSECME

Chairs

- Tero Kivinen
- Yoav Nir

Report

https://mailarchive.ietf.org/arch/msg/saag/BbmzIKJyB02SYQK7jClhOZrkGxY/

KITTEN

Chairs

- Robbie Harwood

Report

Not meeting

LAKE

Chairs

- Stephen Farrell
- Mališa Vučinić

Report

https://mailarchive.ietf.org/arch/msg/saag/Ljb-rnPG6d-nXIpqRr6RC6ipbMI/

LAMPS

Chairs

- Russ Housley
- Tim Hollebeek

Report

https://mailarchive.ietf.org/arch/msg/saag/6a5jyyj2pABXZk4HfhP-3kyTPzE/

MILE

Chairs

- Nancy Cam-Winget
- Takeshi Takahashi

Report

Did not meet

MLS

Chairs

- Nick Sullivan
- Sean Turner

Report

https://mailarchive.ietf.org/arch/msg/saag/EpAtzHZourjPE8z-opGpHoX27_c/

OAUTH

Chairs

- Hannes Tschofenig
- Rifaat Shekh-Yusef

Report

Did not meet

PrivacyPass

Chairs

- Benjamin Schwartz
- Joseph Salowey

Report

https://mailarchive.ietf.org/arch/msg/saag/wmzX-GkDjVruSmtqK0ARrZZkbGM/

RATS

Chairs

- Nancy Cam-Winget
- Ned Smith
- Kathleen Moriarty

Report

https://mailarchive.ietf.org/arch/msg/saag/ib9dfxWZlMIkoNDzkd-gs8Ck4_8/

https://mailarchive.ietf.org/arch/msg/saag/JA6yZKIOm9HJ6SXlP1MqWkpaHDQ/

SACM

Chairs

- Chris Inacio
- Karen O’Donoghue

Report

https://mailarchive.ietf.org/arch/msg/saag/4Son5mw_vZClUmOf45wT_tszlOs/

SecDispatch

Chairs

- Richard Barnes
- Francesca Palombini
- Kathleen Moriarty

Report

[met last session]

SecEvent

Chairs

- Dick Hardt
- Yaron Sheffer

Report

Did not meet

SUIT

Chairs

- Russ Housley
- Dave Thaler
- David Waltermire

Report

https://mailarchive.ietf.org/arch/msg/saag/VUtcskAbo1wmlD-e-rnYQCYvo50/

TEEP

Chairs

- Nancy Cam-Winget
- Tirumaleswar Reddy

Report

https://mailarchive.ietf.org/arch/msg/saag/ld0fVTvbDh4UZ9tUtCRy0ZglvHk/

TLS

Chairs

- Joe Salowey
- Sean Turner
- Chris Wood

Report

https://mailarchive.ietf.org/arch/msg/saag/-ZnJBTXj3TOhkBM3zu2N2G71LgM/

TOKBIND

Chairs

- John Bradley
- Leif Johansson

Report

Did not meet

TRANS

Chairs

- Melinda Shore
- Paul Wouters

Report

Did not meet

Related Non-SEC Area Activities

Security Topics in Related WGs

- ANIMA
- DIME
- DISPATCH
- DMARC
- DOH
- DPRIVE
- HIP
- HTTPBIS
- QUIC
- NETCONF
- NTP
- OPSEC
- PERC
- RADext
- SIDROPS
- STIR
- TCPINC
- UTA
- TAPS

Other BoFs

- ASDF
- EMAILCORE
- LOOPS

Security Related IRTF

- CFRG
- PEARG

IAB Programs

- model-t

External related

- W3C
- IEEE
- ITU

Other SEC Area Highlights

AD Sponsored Drafts

- draft-foudil-securitytxt
- draft-gont-numeric-ids-sec-considerations

New Work

- Re-open OPENPGP

Common SEC AD DISCUSS items

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

Thanks to the SECDIR Reviewers since IETF 107

- Derek Atkins
- Nancy Cam-Winget
- Linda Dunbar
- Donald Eastlake
- Shawn Emery
- Stephen Farrell
- Daniel Franke
- Scott G. Kelly
- Steve Hanna
- Russ Housley
- Christian Huitema
- Charlie Kaufman
- Tero Kivinen
- Watson Ladd
- Chris Lonvick
- Aanchal Malhotra
- David Mandelberg
- Catherine Meadows
- Sandra Murphy
- Yoav Nir
- Hilarie Orman
- Francesca Palombini
- Radia Perlman
- Derrell Piper
- Tirumaleswar Reddy
- Kyle Rose
- Joseph Salowey
- Rich Salz
- Yaron Sheffer
- Rifaat Shekh-Yusef
- Valery Smyslov
- Robert Sparks
- Sean Turner
- Mališa Vučinić
- Carl Wallace
- Brian Weis
- Christopher Wood
- Paul Wouters
- Liang Xia

DOTS Overview

Tirumaleswar Reddy

PKI vs. Pinning vs. Manual Configuration Domains of Applicability

Why now?

NFSv4 is working on RPC-over-TLS.

https://mailarchive.ietf.org/arch/msg/nfsv4/SLTNqWbjE-H8JshLk0HwlwxArrI/ asserted “TLS Fingerprint Pinning Needed”. (Wants four options, manual-config/TOFU, pin EE/ignore CA, pin EE/verify CA, “normal” PKI/verify CA.)

Is that actually true? When might it be true?

Disclaimer

This is not limited to the Web (or the WebPKI).

Non-Web protocols are in scope (note that the prompting inquiry was in the context of NFSv4).

Taxonomy

(Thanks, Ekr!)

- Manual Configuration (of EE key), optionally with Trust On First Use (TOFU)
- “public” PKI (large set of CAs, e.g., WebPKI)
- local PKI (small set of local-only CAs)
- DNSSEC with TLSA or similar (not discussed further in these slides)

Why PKI?

- Handful of TAs allows scalable secure communication to many EEs
- Pick which CAs to trust … or let Mozilla do it for you
- Some classes of key rotation are easier
- Allows for enterprise CA
- But, leaves someone protecting high-value secrets

Why Manual Configuration/TOFU?

- No need to trust a third-party CA
- Cut out enterprise CA
- Avoid pull-based revocation
- Don’t need much infrastructure
- But, scaling not so great
- And you may not always get any revocation

Why Pinning?

- Pinning to a subset of CAs in a public PKI reduces risk from “less trusted” CAs misissuing or being subverted
- But, as a prerequisite, you already trust those “less trusted” CAs sometimes.
- Pinning to EE cert/key considered brittle and RFC 7469 no longer recommended

Questions

- Are some types of protocols naturally suited for manual config/TOFU vs. PKI?
- (Which ones?)
- If pinning, what to pin?
- [List discussion suggests “just CAs and not EEs”]

Questions

- Should we ~~require~~encourage all protocols to support both manual EE (fingerprint) config and PKI?
- Is it enough to just have the option for local PKI vs public PKI?
- Or is any of this an “implementation matter” that we should leave out of scope?

BCP 72 Updates

(BCP 72 is currently just RFC 3552, *Guidelines for Writing RFC Text on Security Considerations*, which notably includes an Internet Threat Model.)

Work currently underway that might update it:

- draft-gont-numeric-ids-sec-considerations is in AD Evaluation, as mentioned earlier
- IAB model-t program underway

Numeric Identifiers

AD Evaluation thread at https://mailarchive.ietf.org/arch/msg/saag/8CRgca7Ip9evFjNF0xVHzmghvi4/

- How much coverage of example attacks vs. just the overarching principles?
- Specifically require analysis (when applicable) vs. mentioning it as a relevant topic?

Model-T

Open Mic