Security Area Advisory Group

Stephen Farrell
Kathleen Moriarty

IETF-92

note well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

The IETF plenary session

The IESG, or any member thereof on behalf of the IESG

Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices

Any IETF working group or portion thereof

Any Birds of a Feather (BOF) session

The IAB or any member thereof on behalf of the IAB

The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

agenda

1. WG/BoF Reports and administrivia (10 mins)
2. Status on PM
3. Invited/offered talks
    1. Joe Bonneau (30 mins)
    2. AGL/QUIC (15 mins)
    3. NSEC5, DNSSEC Authenticated Denial of Existence (10 mins)
    4. Darkmail (20 mins)
4. open-mic (40 mins)

WGs

ace

- Chairs
  - Kepeng Li
  - Hannes Tschofenig

abfab

- Chairs
  - Leif Johansson
  - Klaas Wierenga

dane

- Chairs
  - Warren Kumari
  - Olafur Gudmundsson

dice

- Chairs
  - Dorothy Gellert
  - Zach Shelby

HTTPAuth

- Chairs
  - Yoav Nir
  - Matt Lepinski

ipsecme

- Chairs
  - Paul Hoffman
  - Yaron Sheffer

jose

- Chairs
  - Jim Schaad
  - Karen O’Donoghue

kitten

- Chairs
  - Shawn Emery
  - Matt Miller
  - Benjamin Kaduk

MILE

- Chairs
  - Alexey Melnikov
  - Takeshi Takahashi

oauth

- Chairs
  - Derick Atkins
  - Hannes Tschofenig

sacm

- Chairs
  - Adam Montville
  - Dan Romascanu

tls

- Chairs
  - Joe Salowey
  - Sean Turner

tokbind

- Chairs
  - John Bradley
  - Leif Johansson

trans

- Chairs
  - Melinda Shore
  - Paul Wouters

Related WGs

wg/rg

- Security Related Wgs/Topics
  - ANIMA
  - TCPINC
  - HTTPBIS
  - DPRIVE/DNSOP
  - UTA
  - CIDR
- Security Related IRTF
  - CFRG

BoFs

DOTS

- Chairs
  - Russ Housley
  - Roman Danyliw

ACME

- Chairs
  - Ted Hardie
  - Rich Salz

Side Meetings

- I2NSF
  - Dan Romascanu
  - Joe Salowey
- PGP
- Captive Portals

Update on PM Drafts

- Lots of work is happening across many WGs related to PM, thank you all for your work!
  - IPsecMe, UTA, TLS,
- Drafts/RFCs specific to PM:
  - RFC7258 Pervassive Monitoring is an Attack, May 2014
  - Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement, draft-iab-privsec-confidentiality-threat
  - Effects of Ubiquitous Encryption, draft-mm-wg-effect-encrypt
    - Call for contributions/comments/text
- What to do next?

Effects of Ubiquitous Encryption draft

- Increased use of encryption will impact operations for security and network management causing a shift in how these functions are performed. In some cases, new methods to both monitor and protect data will evolve.
- In more drastic circumstances, the ability to monitor may be eliminated.
- This draft includes a collection of current security and network management functions that may be impacted by the shift to increased use of encryption.
- This draft does not attempt to solve these problems, but rather document the current state to assist in the development of alternate options to achieve the intended purpose of the documented practices.

Presentations

Presentations

1. Joe Bonneau (30 mins)
2. AGL/QUIC (15 mins)
3. NSEC5, DNSSEC Authenticated Denial of Existence (10 mins)
4. Darkmail (20 mins)

OPEN MIC