

# Security Area Advisory Group

Stephen Farrell

Kathleen Moriarty

IETF-97

# 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 (20 mins)
2. Overview of Information Security relevant work in Korea, Dr. Heung Youl YOUM, 30 mins
3. Crypto-conditions, Adrian Hope-Bailie, 20 mins  
draft-thomas-crypto-conditions
4. Update on "Effect of Ubiquitous Encryption," Al Morton, 10 mins  
draft-mm-wg-effect-encrypt
5. DHCP/802.1X, Alan DeKok 15 mins  
draft-dekok-saag-dhcp-keys
6. Numeric IDs Update, Fernando Gont, 15 mins  
Draft-gont-predictable-numeric-ids
7. open-mic

**WGs**

ace

- Chairs

- Kepeng Li

- Hannes Tschofenig

# acme

- Chairs
  - Ted Hardie
  - Rich Salz

# COSE

- Chairs
  - Kepeng Li
  - Justin Richer
- Not meeting this time

# curdle

- Chairs
  - Daniel Migault
  - Rich Salz



# dane

- Chairs
  - Warren Kumari
  - Olafur Gudmundsson
- Not meeting this time

# dots

- Chairs
  - Roman Danyliw
  - Tobias Gondrom

# httpauth

- Chairs
  - Yoav Nir
  - Rifaat Shekh-Yusef
- Not meeting this time

# i2nsf

- Chairs
  - Adrian Farrel
  - Linda Dunbar

# ipsecme

- Chairs
  - Paul Hoffman
  - David Waltermire

# kitten

- Chairs
  - Matt Miller
  - Benjamin Kaduk
- Not meeting this time

# lamps

- Chair
  - Russ Housley

# mile

- Chairs
  - Nancy Cam-Winget
  - Takeshi Takahashi



# oauth

- Chairs
  - Derick Atkins
  - Hannes Tschofenig

# openpgp

- Chairs
  - Daniel Kahn Gillmor
  - Barry Lieba
- Not meeting this time

# sacm

- Chairs
  - Adam Montville
  - Karen O'Donoghue

# secevent

- Chairs
  - Yoav Nir (Temporary thanks!
  - <your name here> :-)

# tls

- Chairs
  - Joe Salowey
  - Sean Turner

# tokbind

- Chairs
  - John Bradley
  - Leif Johansson

# trans

- Chairs
  - Melinda Shore
  - Paul Wouters

**Related WGs**



# wg/rg

- ANIMA
- DIME
- DISPATCH
- DMARC
- DPRIVE
- HTTPBIS
- QUIC
- NETCONF
- PERC
- RADext
- TCPINC
- UTA
- IRTF
  - CFRG
  - IRTFOpen
- IAB Programs
  - Privsec
- External
  - W3C
  - IEEE

# BoFs

None this time

# Presentations

# agenda

1. WG/BoF Reports and administrivia (20 mins)
2. Overview of Information Security relevant work in Korea, Dr. Heung Youl YOUM, 30 mins
3. Crypto-conditions, Adrian Hope-Bailie, 20 mins  
draft-thomas-crypto-conditions
4. Update on "Effect of Ubiquitous Encryption," Al Morton, 10 mins  
draft-mm-wg-effect-encrypt
5. DHCP/802.1X, Alan DeKok 15 mins  
draft-dekok-saag-dhcp-keys
6. Numeric IDs Update, Fernando Gont, 15 mins  
Draft-gont-predictable-numeric-ids
7. open-mic

**OPEN MIC**