Security Area Advisory Group

Stephen Farrell
Kathleen Moriarty
IETF-96
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.  Invited/offered talks
   1.  TRON workshop & prize-winner, Karen O’Donoghue/ Tibor Jager (15 min)
   2.  Port Scanning and Websockets, Tom Gallagher (15 min)
   3.  ITU-T SG/17, Vasily Dolmatov (10 min)
   4.  GCM nonce reuse bugs as an example of easy to misuse crypto constructions, Hanno Bock/Aaron Zauner (30 min)
3.  Process Stuff
   1.  Update on Censorship draft, Joseph Lorenzo Hall (10 min)
   2.  RFC3552bis, Yoav Nir/Magnus Westerlund (10 min)
4.  open-mic (20 min)
WGs
abfab

• Chairs
  – Leif Johansson
  – Klaas Wierenga

• Not meeting
ace

• Chairs
  – Kepeng Li
  – Hannes Tschofenig
ACME

• Chairs
  – Ted Hardie
  – Rich Salz
cose

• Chairs
  – Kepeng Li
  – Justin Richer
CURDLE

• Chairs
  – Daniel Migault
  – Rich Salz
dane

• Chairs
  – Warren Kumari
  – Olafur Gudmundsson

• Not meeting
DOTS

• Chairs
  – Roman Danyliw
  – Tobias Gondrom
HTTPAuth

• Chairs
  – Yoav Nir
  – Rifaat Shekh-Yusef

• Not meeting
I2NSF

• Chairs
  – Adrian Farrel
  – Linda Dunbar
ipsecme

• Chairs
  – Tero Kivinen
  – David Waltermire
jose

• Chairs
  – Jim Schaad
  – Karen O’Donoghue

• Not meeting
kitten

• Chairs
  – Matt Miller
  – Benjamin Kaduk

• Not meeting
LAMPS

• Russ Housley
MILE

• Chairs
  – Nancy Cam-Winget
  – Takeshi Takahashi
oauth

• Chairs
  – Derick Atkins
  – Hannes Tschofenig
openPGP

• Chairs
  – Daniel Kahn Gillmor
  – Barry Leiba
sacm

• Chairs
  – Adam Montville
  – Karen O’ Donoghue
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
  - DBOUND
  - DIME
  - DISPATCH
  - DMARC
  - DPRIVE
  - HTTPBIS
  - NETCONF
  - NTP
  - PERC
  - RADext
  - SIDR
  - TCPINC
  - UTA
  - WebPUSH

- Security Related IRTF
  - CFRG
  - IRTFOpen

- IAB Programs
  - PrivSec

- External related
  - W3C
BoFs
LURK

• Limited Use of Remote Keys
  – Eric Burger
  – Yaron Sheffer
Presentations
Presentations

1. Invited/offered talks
   1. TRON workshop & prize-winner, Karen O’Donoghue/ Tibor Jager (15 min)
   2. Port Scanning and Websockets, Tom Gallagher (15 min)
   3. ITU-T SG/17, Vasily Dolmatov (10 min)
   4. GCM nonce reuse bugs as an example of easy to misuse crypto constructions, Hanno Bock/Aaron Zauner (30 min)

2. Process Stuff
   1. Update on Censorship draft, Joseph Lorenzo Hall (10 min)
   2. RFC3552bis, Yoav Nir/Magnus Westerlund (10 min)
OPEN MIC