Security Area Advisory Group

Stephen Farrell

Sean Turner

November 8, 2012

note well summary

- ## The brief summary:
  - This summary is only meant to point you in the right direction, and doesn't have all the nuances; see below for the details.
  - By participating with the IETF, you agree to follow IETF processes.
  - If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.

- ## You understand that meetings might be recorded and broadcast.

- ## The details:
  - For further information, talk to a chair, ask an Area Director, or review BCP 9 (on the Internet Standards Process), BCP 25 (on the Working Group processes), BCP 78 (on the IETF Trust) , and BCP 79 (on Intellectual Property Rights in the IETF).

agenda

- WG Reports, <10 mins
- Security Related BOFs, 10 mins
- Invited Presentation
  - SSH and Host Key Management Problems
    Tatu Ylonen, 30 mins
  - Review of CRIME/BEAST
    Yoav Nir, 20 mins
  - Heads-Up: Securely Initializing Devices in LLNs etc
    Carsten Bormann, 10 mins
  - Heads-Up: Security and SDNs
    Margaret Wasserman, 5 mins
- Other Security Related WGs/BOFs, <8 mins
- Open Mike

WGs

- Chairs
  - Leif Johansson
  - Klaas Wierenga

ipsecme

- Chairs
  - Paul Hoffman
  - Yaron Sheffer

krb-wg/kitten

- Chairs
  - Shawn Emery
  - Josh Howlett
  - Sam Hartman

- Chairs
  - Kathleen Moriarty
  - Brian Trammell

tls

- Chairs
  - Eric Rescorla
  - Joe Salowey

jose

- Chairs
  - Jim Schaad
  - Karen O'Donoghue

emu

- Chairs
  - Alan DeKok
  - Joe Salowey

oauth

- Chairs
  - Derick Atkins
  - Hannes Tschofenig

- Chairs
  - Stephen Kent
  - Stefan Santesson

dane

- Chairs:
  - Ondřej Surý
  - Warren Kumari

not meeting

nea

- Chairs
  - Stephen Hanna
  - Susan Thomson

not meeting

BOFs

wpkops

- Chairs
  - Steve Hanna
  - Tim Moses

- Chairs
  - Dan Romascanu
  - Kathleen Moriarty

certrans

- Chair
  - Paul Hoffman

- Chairs
  - Yoav Nir
  - Derek Atkins

other

- Security Related WGs
  - WEBSEC
  - HTTPBIS
  - Routing: KARP & SIDR
  - PRECISE
- Security Related RGs
  - CFRG

Invited Presentations

- SSH and Host Key Management Problems
  Tatu Ylonen, 30 mins

- Review of CRIME/BEAST
  Yoav Nir, 20 mins

- Heads-Up: Securely Initializing Devices in LLNs
  Carsten Bormann, 10 mins

- Heads-Up: Security and SDNs
  Margaret Wasserman, 5 mins

OPEN MIC