Security Area Advisory Group

Benjamin Kaduk
Eric Rescorla
IETF-101
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. WG/BoF Reports and administrivia (10 mins)

2. Invited/offered talks
   1. Verifying Real-World Protocols (30 min)
      Karthik Bhargavan
   2. The Sphinx Packet Format for Mix-nets and Bitcoin
      Harry Halpin
   3. Capsule: A Protocol for Secure Collaborative Document Editing (5 min)
      Nadim Kobeissi
   4. draft-nslag-mpls-deprecate-md5 (10 min)
      Stewart Bryant

3. open-mic (10 mins)
WG\text{~}s
ace

• Chairs
  – Ben Kaduk
  – Jim Schaad
ACME

• Chairs
  – Rich Salz
  – Yoav Nir
CURDLE

1. Chairs
   1. Daniel Migault
   2. Rich Salz
DOTS

• Chairs
  – Roman Danyliw
  – Tobias Gondrom
EMU

- Chairs
  - Joe Salowey
I2NSF

• Chairs
  – Linda Dunbar
  – Yoav Nir
ipsecme

• Chairs
  – Tero Kivinen
  – David Waltermire
kitten

• Chairs
  – Matt Miller
  – Benjamin Kaduk

• Not meeting
LAMPS

- Russ Housley
MILE

• Chairs
  – Nancy Cam-Winget
  – Takeshi Takahashi
oauth

• Chairs
  – Hannes Tschofenig
  – Rifaat Shekh-Yusef
sacm

• Chairs
  – Chris Inacio
  – Adam Montville
  – Karen O’ Donoghue
SecDispatch

- Chairs
  - Richard Barnes
  - Roman Danyliw
SecEvent

• Chairs
  – Dick Hardt
  – Yaron Sheffer
SUIT

• Chairs
  – Russ Housley
  – Dave Thaler
  – David Waltermire
TEEP

• Chairs
  – Nancy Cam-Winget
  – Dave Thaler
tls

• Chairs
  – Joe Salowey
  – Sean Turner
tokbind

• Chairs
  – John Bradley
  – Leif Johansson
trans

• Chairs
  – Melinda Shore
  – Paul Wouters
Related WG}s
• Security Related WGs/Topics
  – ANIMA
  – DBOUND
  – DIME
  – DISPATCH
  – DMARC
  – DPRIVE
  – HTTPBIS
  – QUIC
  – NETCONF
  – NTP
  – PERC
  – RADext
  – SIDR
  – TCPINC
  – UTA

• Security Related IRTF
  – CFRG
  – IRTFOpen

• IAB Programs
  – PrivSec

• External related
  – W3C
BoFs
MLS

- Chairs
  - Sean Turner
  - Nick Sullivan
Presentations
Presentations

Verifying Real-World Protocols: finding attacks and proving security theorems (30 min)
Karthik Bhargavan

The Sphinx Packet Format for Mix-nets and Bitcoin (10 min)
Harry Halpin

Capsule: A Protocol for Secure Collaborative Document Editing (5 min)
Nadim Kobeissi

draft-nslag-mpls-deprecate-md5 (10 min)
Stewart Bryant
OPEN MIC

10 Minutes