Security Area Advisory Group

Stephen Farrell
Tim Polk
Sean Turner

March 31, 2011

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,
- any IETF working group or portion thereof,
- the IESG or any member thereof on behalf of the IESG,
- the IAB or any member thereof on behalf of the IAB,
- any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices,
- 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.

- WG Reports
- BOF Reports
- Invited Presentation
  - Intro to MIBs, YANG, and why security geeks should care (Dan Romascanu)
  - HTTP-Mutual Authentication (Yutaka Oiwa)
  - The FNV Non-Cryptographic Hash Algorithm (Donald Eastlake)
  - DNS Certification Authority Authorization (CAA) Resource Record (Phillip Hallam-Baker)
- Open Mike

dkim

(Domain Keys Identified Mail)

- Barry Leiba

http://www.ietf.org/mail-archive/web/saag/current/msg03135.html

pkix

(Public Key Infrastructure using X.509)

- Stephen Kent
- Stefan Santesson

abfab
(Application Bridging for Federated Access Beyond web)

- Leif Johansson
- Klaas Wierenga

hokey

(Handover Keying)

- Tina Tsou
- Glen Zorn

http://www.ietf.org/mail-archive/web/saag/current/msg03138.html

krb-wg

(Kerberos)

- Jeff Hutzelman
- Larry Zhu
- Sam Hartman

http://www.ietf.org/mail-archive/web/saag/current/msg03144.html

nea

(Network Endpoint Assessment)

- Stephen Hanna
- Susan Thomson

http://www.ietf.org/mail-archive/web/saag/current/msg03141.html

msec

(Multicast Security)

- Vincent Roca
- Brian Weis

http://www.ietf.org/mail-archive/web/saag/current/msg03143.html

dane

(DNS-based Authentication of Named Entities)

- Ondrej Sury
- Warren Kumari

emu

(EAP Method Update)

- Alan DeKok
- Joe Salowey

http://www.ietf.org/mail-archive/web/saag/current/msg03145.html

tls

(Transport Layer Security)

- Eric Rescorla
- Joe Salowey

kitten
(Common Authentication Technology Next Generation)

- Shawn Emery
- Tom Yu
- Alexey Melnikov
- (meeting Friday)

ipsecme
(IP Security Maintenance and Extensions)

- Paul Hoffman
- Yaron Sheffer
- (not meeting this week)

http://www.ietf.org/mail-archive/web/saag/current/msg03137.html

isms

(Integrated Security Model for SNMP)

- Jürgen Schönwälder
- Russ Mundy
- (not meeting this week)

ltans

(Long Term Archive and Notary Service)

- Tobias Gondrom
- Carl Wallace
- (not meeting this week)
  - Final WG draft approved yesterday

Other WGs and BOFs

- BOF
  - PLASMA
    - http://www.ietf.org/mail-archive/web/saag/current/msg03142.html
- Security Related WGs
  - KARP
  - SIDR
  - OAUTH
  - WEBSEC
- Side Meetings
  - Web Object Encryption and Signature (WOES)
  - HTTP Authentication
  - Do Not Track

Invited Presentations

- Intro to MIBs, YANG, and why security geeks should care (Dan Romascanu)
- HTTP-Mutual Authentication (Yutaka Oiwa)
- The FNV Non-Cryptographic Hash Algorithm (Donald Eastlake)
- DNS Certification Authority Authorization (CAA) Resource Record (Phillip Hallam-Baker)

Open Mike

- Concerns?
- Issues?
- Soap Box?