Security Area Advisory Group

Pasi Eronen
Tim Polk
Sean Turner

March 25, 2010

- WG Reports
- BOF Reports
- Invited Presentation
  - Fundamental ECC Algorithms (David McGrew)
  - MashSSL (Ravi Ganesan)
- Open Mike

ipsecme
(IP Security Maintenance and Extensions)

- Paul Hoffman
- Yaron Sheffer
- http://www.ietf.org/mail-archive/web/saag/current/msg02728.html

nea

(Network Endpoint Assessment)

- Stephen Hanna
- Susan Thomson
- http://www.ietf.org/mail-archive/web/saag/current/msg02732.html

pkix

(Public Key Infrastructure using X.509)

- Stephen Kent
- Stefan Santesson
- http://www.ietf.org/mail-archive/web/saag/current/msg02735.html

msec

(Multicast Security)

- Vincent Roca
- Brian Weis

emu

(EAP Method Update)

- Alan DeKok
- Joe Salowey
- http://www.ietf.org/mail-archive/web/saag/current/msg02729.html

hokey

(Handover Keying)

- Tina Tsou
- Glen Zorn

kitten

(GSS-API Next Generation)

- Shawn Emery
- Tom Yu
- http://www.ietf.org/mail-archive/web/saag/current/msg02726.html

krb-wg

(Kerberos)

- Jeff Hutzelman
- Larry Zhu
- http://www.ietf.org/mail-archive/web/saag/current/msg02736.html

tls

(Transport Layer Security)

- Eric Rescorla
- Joe Salowey
- (meeting later today)

dkim

(Domain Keys Identified Mail)

- Stephen Farrell
- Barry Leiba

isms

(Integrated Security Model for SNMP)

- Jürgen Schönwälder
- Russ Mundy
- http://www.ietf.org/mail-archive/web/saag/current/msg02727.html

keyprov

(Provisioning of Symmetric Keys)

- Phillip Hallam-Baker
- Hannes Tschofenig

Itans

(Long Term Archive and Notary Service)

- Tobias Gondrom
- Carl Wallace

sasl

(Simple Authentication and Layer Services)

- Tom Yu
- Kurt Zeilenga

smime

(S/MIME Mail Security)

- Paul Hoffman
- Blake Ramsdell

syslog

(Security Issues in Network Event Logging)

- David Harrington
- Chris Lonvick
- http://www.ietf.org/mail-archive/web/saag/current/msg02730.html

Other WGs and Bar BOFs

- WGs
  - APPAREA
  - KARP
  - OAUTH
  - SIDR
- Bar BOFs
  - High Assurance Cryptographic API
  - Federated Authentication for Non-Web Applications

Representation and Verification of Application Server Identity

- draft-saintandre-tls-server-id-check
  - Peter Saint-Andre and Jeff Hodges
  - http://www.ietf.org/proceedings/10mar/slides/pkix-4.pdf

Invited Presentations

- Fundamental ECC Algorithms (David McGrew)
- MashSSL (Ravi Ganesan)

Open Mike

- Concerns?
- Issues?
- Soap Box?