MSEC Agenda and WG Status
IETF-63, Paris

Ran Canetti
Lakshminath Dondeti

August 2, 2005

Preliminaries

- Minute takers
- Goal of the meeting
  - Keep presentations succinct and use the time for discussions

Agenda

- **MSEC status report** **(Ran/Lakshminath)**
  - Revised milestones & Document status
  - Notes on cross-area work and reviews
- **draft-ietf-msec-bootstrapping-tesla** **(Steffen)**
- **draft-ietf-msec-ipsec-extensions** **(Dragan)**
- **draft-ietf-msec-mikey-ecc** **(Andy)**
- **draft-ietf-msec-mikey-rsa-r** **(Dragan)**
- **draft-dondeti-msec-inband-key-updates** **(Lakshminath)**
- **draft-faurite-rmt-tesla-for-alc-norm** **(RMT proposal for review)**
  - Where does this work belong? RMT or MSEC?
- **draft-cruickshank-ipdvb-sec-00.txt** **(IPDVB proposal for review)**
  - What next on this?
- **Discussion**
  - **MIKEY, TESLA, IPsec Extensions etc.**

Agenda bashing …

- Any changes to the agenda?

New/Recent MSEC RFCs

- RFC 4046 Multicast Security (MSEC) Group Key Management Architecture (Apr 2005)
  - Informational
- RFC 4082 TESLA (Jun 2005)
  - Informational

MSEC drafts, post-WGLC

- IESG Processing:
  - draft-ietf-msec-bootstrapping-tesla -01 2005-05-24
    - AD Evaluation::Revised ID Needed
  - draft-ietf-msec-newtype-keyid -01 2005-02-14
    - Waiting for AD Go-Ahead
    - Waiting for 3GPP SA3 coordination
  - draft-ietf-msec-srtp-tesla -03 2005-02-14
    - Waiting for AD Go-Ahead::Revised ID Needed
- RFC-Editor's Queue:
  - draft-ietf-msec-gsakmp-sec -10 2005-05-17
  - draft-ietf-msec-ipsec-signatures -06 2005-06-22
  - draft-ietf-msec-mikey-dhhmac -11 2005-04-04

MSEC drafts, work in progress

- draft-ietf-msec-ipsec-extensions -00 2005-07-25
- draft-ietf-msec-mikey-ecc -00 2005-07-07
- draft-ietf-msec-mikey-rsa-r -00 2005-07-08
- draft-ietf-msec-policy-token-sec -03 2005-07-08
  - Finishing up the WGLC process and forwarding to AD soon
- Expired, but active work:
  - draft-ietf-msec-gdoiv2 -01 2004-10-26
  - draft-ietf-msec-tesla-spec -00 2002-10-30
- Did we miss any?

Proposed completed milestones

- Dec 03 WG Last Call on MSEC Security Requirements draft
  - ** Done (Sep 2003; Published as RFC 3740, in Mar 2004)
- Dec 03 WG Last Call on MSEC Policy Token
  - ** Done (WGLC July 2005; will forward to AD after the Paris meeting)
- Dec 03 WG Last Call on GSAKMP
  - ** Done (July 2004)
- Dec 03 Last Call on GSAKMP-Token
  - (Dead; became MSEC Policy Token)
- Dec 03 WG Last Call on IP Multicast issues with IPsec
  - (Dead, revived, TBD)
- Mar 04 WG Last call on TESLA-Intro draft
  - ** Done (Finished in Feb 2004; Published as RFC 4082)
- Mar 04 WG Last Call on MESP Framework (Data Security Architecture) draft
  - (dead; absorbed into IPsec ESP)
- Mar 04 WG Last call on TESLA-Spec draft
  - Delete (For Updated name & timeline: see below)
- Jul 04 WG re-charter for other work items (or disband)
  - (Rechartered; new milestones will run into early 2006)

“New” MSEC milestones

- Aug 04 WG Last call on "Use of RSA/SHA-1 Signatures within ESP and AH"
  - Done (in RFC Ed queue)
- Mar 05 WG Last Call on "Key ID Information Type for the General Extension Payload in MIKEY"
  - Done (in IESG review)
- Mar 05 WG Last Call on "The Use of TESLA in SRTP"
  - Done (in IESG review)
- Mar 05 WG Last Call on "Bootstrapping TESLA"
  - Done (in AD review)
- Nov 05 WG Last Call on "MIKEY-RSA-R"
- Dec 05 WG Last Call on "MIKEY-ECC"
- Mar 06 WG Last Call on "TESLA-ESP-Spec"
- Apr 06 WG Last Call on "Multicast Extensions to IPsec"
- Jun 06 WG Last Call on GKDP

MSEC liaison activities

- 802.16e review request
  - Several folks volunteered and most returned reviews
  - Thanks to
    - Ran Canetti, Dragan Ignjatic, Men Long, QinKe, Brian Weis
    - Comments pending from a few
  - Outstanding requests for the draft spec from a few
  - What next?
    - I am yet to hear from Jeff Mandin, the IEEE 802.16e liaison about what next
    - The plan was to compile all the comments and submit to 802.16 as a contribution