Multicast Security (MSEC) WG

IETF-56, San Francisco

Mon, March 17, 2003

1930-2200 Evening Sessions

MSEC Agenda

- Agenda Bashing (5min)
- Review of WG Status (T. Hardjono/R. Canetti) (10min)
- TESLA Update (A. Perrig) (15min)
- AH/ESP multicast issues (B. Weis) (15min)
- MESP draft (R.Canetti/M.Baugher) (15min)
- Feedback channel protection (L. Dondeti) (15min)
- GKM Algorithms (L. Dondeti/B. Weis) (15min)
- GSAKMP Update (H. Harney) (15min)
- GSAKMP Policy Token (H. Harney) (15min)
- DHHMAC for MIKEY Update (M. Euchner) (10min)
- SDP Descriptions (M. Baugher) (15min)
- Discussion
  - MIKEY and MMUSIC

Continue on Tuesday at GSEC
1415-1515 Afternoon Sessions II
1545-1645 Afternoon Sessions III

Current MSEC drafts

MSEC Architecture	draft-ietf-msec-arch-01.txt
Key manag. architecture	draft-ietf-msec-gkmarch-04.txt
GSAKMP Light	draft-ietf-msec-gsakmp-light-sec-01.txt
GSAKMP	draft-ietf-msec-gsakmp-sec-01.txt
GSAKMP Token	draft-ietf-msec-tokenspec-sec-00.txt
MESP	draft-ietf-msec-mesp-00.txt
TESLA specs:	draft-ietf-msec-tesla-spec-00.txt (Standards)
TESLA intro:	draft-ietf-msec-tesla-intro-01.txt (Informational)
DHMAC for MIKEY	draft-ietf-msec-mikey-dhhmac-01.txt
Issues w. IPsec for multicast	draft-ietf-msec-ipsec-multicast-issues-01.txt

Last Call docs

GDOI	draft-ietf-msec-gdoi-07.txt
MIKEY	draft-ietf-msec-mikey-06.txt

- MIKEY:
  - Some perceived “down-grade” attacks
  - Awaiting resolution with MMUSIC and ADs.

Recharter: Modification #1

- Re-charter:
  - Extend life-time of MSEC to 2004
  - Proposed modifications submitted to ADs on Dec 2, 2002

- Add new paragraph:

"In addition, as a secondary goal the MSEC WG will also focus on distributed architectures for group key management and group policy management, where for scalability purposes multiple trusted entities (such as Key Distributors) are deployed in a distributed fashion. For this purpose, the Reference Framework will not only describe one-to-many multicast, but also many-to-many multicast."

Recharter: Modification #2

- Goals and Milestones

Done	Working Group Last Call on GDOI Protocol.
Done	Working Group Last Call on MIKEY Protocol.
Mar 03	Last Call on Group Key Management Architecture draft
Jul 03	Last Call on Security Requirements draft and MSEC Architecture draft.
Nov 03	Last Call on Group Security Policy Architecture draft and Source Authentication draft.
Nov 03	Last Call on MESP (Multicast ESP) draft
Nov 03	Last call on MESP-TESLA draft.
Mar 04	Last Call on GSAKMP-Light protocol draft.
Jul 04	WG disband or re-charter for other work items

MSEC drafts tree