Minutes of MSEC WG meeting at IETF51
August 8, 2001, London, 3pm
==========

Thomas Hardjono and Ran Canetti, chairs

Copies of all of the presentations are on
www.securemulticast.org

GKM Architecture presentation by Mark Baugher:

Presented where GKM arch fits into big picture of docs
and architecture

Comments:

Hugh Harney:
   external policy interface necessary for static
   policy issues.
   Policy that insures that the key being passed
   around is secure should be included within the
   GKM. This can be dynamic (within a group) and
   is required to make/keep group secure.

Re-key protocol presented by Lakshminath Dondeti

(No I-D posted yet)

Comments:

Thomas Hardjono:
   - rekey protocol needs to deal with policy
     changes during rekey, e.g. changing from DES
     to 3DES when key changes.
   - Keep Cat 1 SA's up in place of backchannel

Pete Dinsmore
   - need backchannel for "I need to be resynched"
   - don't use backchannel for group management,
     i.e., de-registration
   - don't include support for subgroup
     communication/keying; too complicated

Hugh Harney:
   - don't confuse KEK's with TEK's. i.e., don't
     use tree keys for subgroup communication

Ken Calvert:
   - what is motivation for subgroup
     communication? It seems too complicated for
     now.

???:
- will backchannel have implosion problem?

Ran Canetti
- separate de-registration from key mgmt backchannel (for resynch)
- subgroup is too complicated for now
- Suggest piggybacking key messages on data
- Will the rekey protocol be stateless? What happens if a message is missed?

GSAKMP Lite presentation by Hugh Harney:

(no I-D posted yet)

Purpose of work is to simplify GSAKMP and provide easier implementation, easier analysis, and faster setup

Cut out optional payloads, initial infrastructure search, first unicast SA.
Kept full GSAKMP functionality for distribution of policy, key mgmt,

Defined security suite for initial setup of group

Comments:

Thomas Hardjono:
- is cat 1 over secure channel? Hugh: Intent is to be secure without unicast SA Haven't specified yet which parameters are kept after exchange (state created by exchange)
- Where does member ID come from? Hugh – it's a 32 bit number.

Lakshminath Dondeti:
- will key node number updates be part of key update?

Key Mgmt for Multimedia Sessions (and SRTP)
presentation by Fredrik Lindholm

(drafts published as individual I-D)

This work originates from securing SRTP in AVT WG

Mark Baugher:
- is there a home for this work here?
- It does not seem this is doing authenticated

key exchanges (can it be done in less than 3 messages?)

Hugh Harney:
- What is the class of applications? Who owns the data shared on the group? The issue is that "how do group members trust that group is secure enough to share my data?

Thomas Hardjono:
- Does this work belong in MSEC? It is common with our work because it is group security.

Brian Weis:
- Isn't SRTP going forward as a unicast protocol? Therefore, this work might not belong in MSEC. However, if it wouldn't slow down the progress of SRTP, I'd welcome their ideas to the working group.

??
- Mmusic will be discussing the unicast/multicast aspects of SRTP. The group security aspects are covered better in MSEC

Mark Baugher:
- feels GKM arch is modular and should be able to handle this.

Ran Canetti:
- agrees this would be good for MSEC.

Mark Baugher:
- MSEC should define key messages, regardless of how they are transmitted (specified probably in Mmusic)

Straw poll taken by Ran was that this work should be included in MSEC (about 30 said yes, 0 said no)

Group Domain of Interpretation by Brian Weis

Brian first explained that GDOI uses IKE phase 1 unchanged, and does not use IKE phase 2 at all. It replaces IKE phase 2 with GDOI, under its own Domain number, and most likely running on its own port. He then presented updates on GDOI since the last IETF.

Questions/Comments

Andrew Krywaniuk

- Does it make sense to just redo the IKE phase 1 exchange to refresh the DH material, instead of having the KE payloads optional in phase 2?

Steve Kent

- Feasible just to use public key certs with narrow scopes of use in place of attribute certs.
- Warning: defering this (Alternative C) may end up requiring an arbitrary number of exchanges, as opposed to the current 2. Protocol will need to be more generic to account for this if the doc follows this alternative.

END==========