Group key management architecture -04-

Mark Baugher
Ran Canetti
Lakshminath Dondeti
Fredrik Lindholm

IETF-56 MSEC WG meeting
March 17 2003, San Francisco

GKM Architecture updates

- **Updates to address comments on the list**
  - Thanks Andrea and Hugh!
- **Updated group/multicast security requirements**
  - Protection against collusion
  - Compromise recovery
  - Other editorial
- **GSAKMP-classic (?) related edits**
- **Editorial**

GSAKMP-related changes

- **Edited references to the way GSAKMP-classic did things**
  - “GSAKMP is no longer using a secure-channel protocol”
  - More on this during the GSAKMP presentation

Open items: TPK

- **Andrea requested that TEK be changed to TPK (traffic protection key)**
  - To represent integrity protection and encryption
- **I understand the logic, but dislike "TPK/DPK"**
- **Ran likes it just fine**
- **Mark noted that TEK has been in the literature for a long time**
  - So keep it!
- **Comments and suggestions, please!**

IPsec references

- **There was a request to remove IPsec related references (e.g., SPD and SAD)**
- **Some of us like that terminology**
  - We can generalize with IPsec terminology as examples
  - But IPsec terminology is widely used and understood
  - Would like to keep it as is!

Examples

- **We used IP telephony and other examples in the I-D**
  - There was a request to remove the references to applications
  - I like references to applications
  - We would like to add more ☺, not delete
    - Is that better?

Comparison of MSEC protocols

- **Will be adding a comparison chart/section on GDOI, GSAKMP, and MIKEY**
  - Hope we can explain why we need three!
- **The next rev appears to be substantial**
  - Note: Only clarification, no new requirements really
- **Proposed last call March 2003 according to the new Charter** ☺
  - Informational/Standards RFC?