Securing feedback messages

Lakshminath R. Dondeti
Thomas Hardjono

IETF-56 MSEC WG meeting
March 16-21 2003, San Francisco

Introduction

- **Feedback messages**
  - NACKs
  - GSA synchronization
  - De-registration ☺
  - Others?
- **Protecting feedback messages**
  - Offer similar protection as rekey messages
  1. Keep Registration SAs around
     - Inefficient for large groups
  2. Use rekey SA

Need for feedback messages

- **GSA synchronization**
  - Rekey messages may be lost in transit
  - Members may go offline
- **Inefficient to have out-of-sync members run Registration protocol again**
- **Reliable transport**
  - Proposed schemes require NACK transmission
- **De-registration**
  - The much maligned De-registration feature!

Making Rekey SA versatile

- **Rekey SA can do more!**
- **Can be used to protect member(s)→GCKS messages**
- **Most GKM algorithms use a unique key per-member (UKM or MUK? ☺)**
  - Ran C. noted that subset-diff is an exception
  - See next slide!
- **Use UKM or derived keys for securing feedback messages**

Subset revocation and UKMs

- **Subtree based revocation (STR) scheme**
  - A Subset corresponding to each complete subtree
  - Every leaf is a subtree
  - Thus there is a UKM in STR
- **Subset difference based revocation (SDR)**
  - All subsets of STR are subsets in SDR as well
  - Representation is different, however
    - SDR subset: parent's subtree – sibling's subtree
  - There is a UKM in SDR scheme as well

UKM to protect feedback msgs

- **Generate an encryption key and integrity key from UKM**
  - This is new, i.e., not part of GDOI or GSAKMP
- **Encrypt and integrity protect feedback messages**
  - Use the same MAC and ENC algms as specified in Rekey SA policy
- **SA lookup: use the SPI in the received rekey message**
  - Brian W. noted that this might not work!

Proposed feedback message

- **Member → GCKS: HDR*, SEQ, REQ, AUTH**
  - * protected by UKM
  - Everything between the HDR and the AUTH payload is encrypted

Next payload	Reserved	Payload length
Request type	Reserved2	
Request data; e.g., NACKs (Variable)		

AUTH payload

Next payload	Reserved	Payload length
UKM ID (e.g., LKH ID)		Reserved2
Auth data (variable)		

- **AUTH payload contains an HMAC computed using the unique integrity key**
- **AUTH payload provides integrity protection**
- **Assists in SA lookup**
  - Contains UKM ID
    - (e.g., LKH ID as defined in GDOI and GSAKMP specs)

Replay protection

- **Tougher problem due to the many-to-one nature of communication**
  - Efficient multi-sender replay protection is an open problem
- **An idea that may work for this special case**
  - Members use the most recent sequence # received from GCKS
- **GCKS maintains a windows of acceptable SEQ# (per group)**

SEQ number window at GCKS

- **GCKS accepts feedback msgs with a SEQ# within a pre-defined window of curr SEQ#**
  - Might work for NACKs and De-registration
  - Might now work for re-sync'ing after a long time offline
- **Resync requests typically result in a member-specific message**
  - Turning off replay protection might result in DoS attacks at GCKS and that member

Summary

- **Protected Feedback messages needed for**
  - NACK messages
  - Resync requests, and
  - Deregistration
- **May use Rekey SA for protection**
  - Use keys derived from UKM for privacy & integrity
  - Members may use most recent SEQ# for replay protection
  - SA lookup using UMK ID and Rekey SA cookies

Where do we go with this?

- **Questions and Comments**
  - Here at the meeting or
  - on the Mailing list
- **draft-dondeti-ietf-msec-secure-feedback-00.txt**
  - Should this be a WG I-D?
- **Thanks to**
  - Brian Weis for comments on suggestions
  - David McGrew for work on GKTP (w/ Lakshminath)