GSAKMP - Light

Presented by

Hugh Harney
hh@sparta.com

Agenda

- Motivation
- Announcement
  - Security Suite 1
- GSAKMP-Light Message Structures
- Summary

Motivation

- Simplify
  - Eliminate the need for underlying unicast SA
  - Reduce the number of messages
  - Reduce number of payloads
- Provide full GSAKMP functionality
  - Distribution of policy
  - Secure distribution of key
  - Group management
- Target GSAKMP for common applications
  - Group announcements

Announcement

- Announcement supported
  - Well known
  - Posted
  - Expanding Ring Announcements (ERA)
- Includes security suite definition for category 1 exchanges
  - Category one exchanges allow members to join a group

Suite 1 definition

- The GSAKMP Light Suite 1 definition is:
  - Key download encryption algorithm definition:
    - Algorithm: 3DES
    - Mode: CBC64
    - Key Length: 192 bits
  - Policy Token encryption algorithm definition:
    - Algorithm: 3DES
    - Mode: CBC64
    - Key Length: 192 bits
  - The Key Creation definition is:
    - Algorithm type is Diffe Hellman
    - MODP group definition
  - The digital signature algorithm is:
    - DSS_ANS1_DER
    - Hash algorithm is:
    - SHA-1

GSAKMP Light Message Structures

- **Category 1 Messages – Group Establishment**
  - ***Light Request to Join***

    {GrpID, key creation, Nonce_I} SigM, [CertM]
  - ***Light Key Download***

    {GrpID, Member ID, Nonce_R, Nonce_C, key creation, *(P.T.), *(download)} SigM, [CertM]
  - ***Light Acknowledgement***

    {GrpID, Nonce_C, Ack} SigM,]

- **Category 2 Messages – Group Management**
  - ***Group Delete***

    {HDR, GrpID, [Policy Token], Delete Notification}SigC, [CertC]
  - ***Policy Update***

    {HDR, GrpID, Policy Token}SigC, [CertC]
  - ***Rekey***

    {HDR, GrpID, [Policy Token], Rekey Array}SigC, [CertC]

Summary

- **GSAKMP Light Functionality**
  - **Policy Distribution and enforcement**
    - Key Management EQUALS Policy Enforcement
  - **Key Management**
    - Group Establishment
    - Group Management
- **GSAKMP Light vs GSAKMP**
  - **Fewer messages**
  - **No unicast SA necessary**
  - **Fewer optional payloads**