Enabling Coalition Operations with A New Standard for Group Security and Key Management

Presented by
Hugh Harney, and Rod Fleischer
SPARTA Inc.
7075 Samuel Morse Dr.
Columbia, MD, 21046
(410) 872-1515, Fax: (410) 872-8079
hugh.harney@sparta.com

Agenda

- **Coalitions and Group Security**
- **Evolution in Group Security**
  - Group Secure Association Key Management Protocol
  - Secure Group Sessions
  - Secure Group Objects
- **Conclusions**

Coalitions are Complex Group

- A coalition is defined as a temporary alliance among people, organizations and nations to achieve a shared common goal.

- Information needs to get to many end users.
  - **People**
  - **Organizations**
  - **Nations**
- Policy is dynamic and complex
  - **Multiple PKIs**
  - **Multiple accrediting authorities**
- Many Internet services are used to move data
  - **E-mail**
  - **Web Browsers**
  - **Peer to Peer Networks**
  - **IM**
  - **Chat**

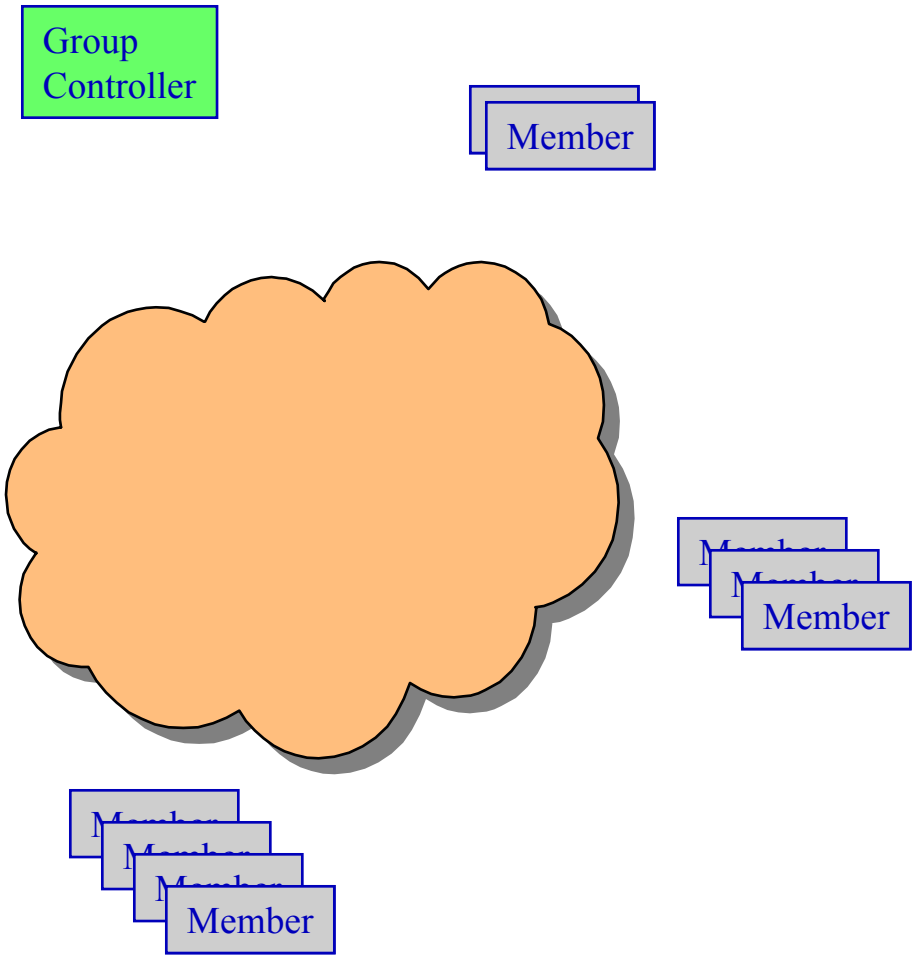
Evolution in Group Security Protocols

- **Good News - Security Protocols are Evolving to meet Coalition Needs**
  - Group Key Management Protocol
    - » Introduced concept of Group Secure Associations
  - Group Domain of Interpretation
    - » Group keying for simple broadcast
  - MIKEY
    - » Group keying and policy for simple music streaming servers
  - GSAKMP
    - » Group Keying
    - » Group Policy Management
    - » Scalable Infrastructures
  - IPSec multicast extensions
  - Secure Group Sessions, Secure Group Objects
    - » Fundamental security building blocks for Secure Group Applications

GSAKMP Properties

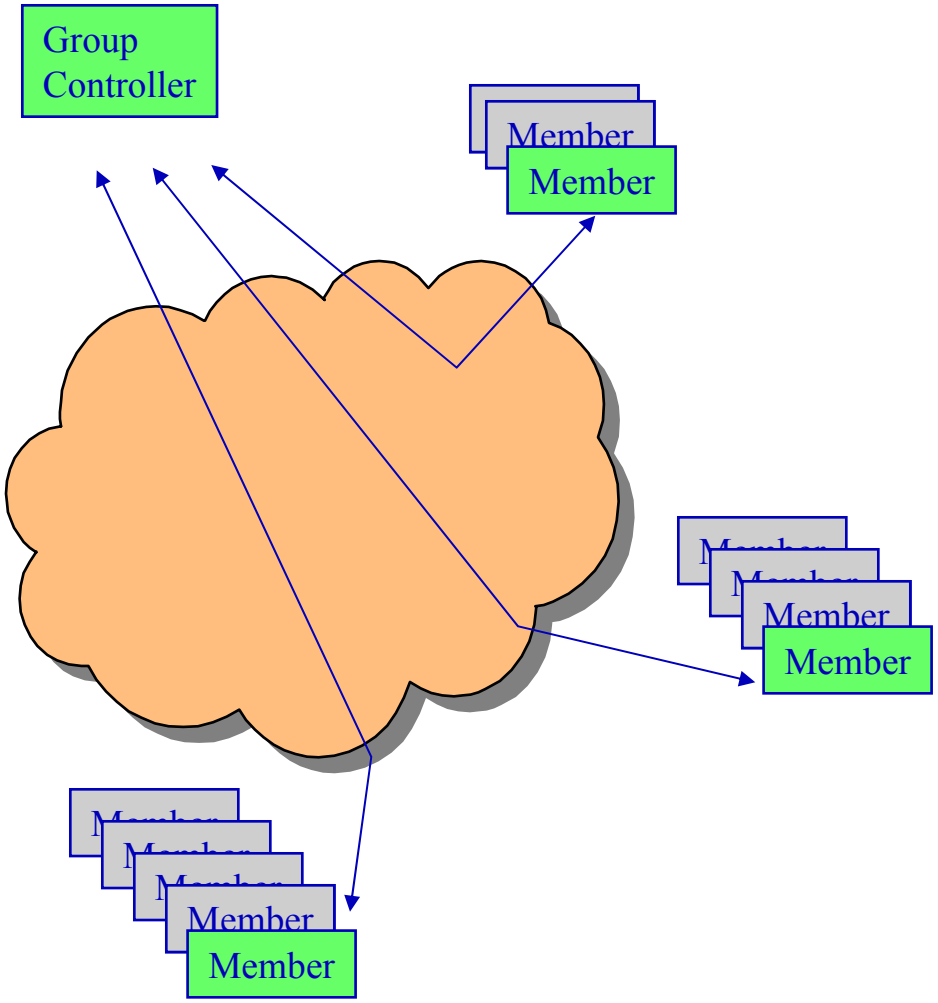
- **GSAKMP: Group Secure Association Key Management Protocol**
  - Create groups of cryptographic keys that can be trusted
    - » Mutual suspicion
    - » Complete security policy definition and enforcement
    - » Balanced security mechanisms
  - Scale to Internet sizes
    - » Delegate and distribute KM processes
  - Peer to Peer software paradigm
    - » Roles can be assigned
  - IETF Standards Track RFC to be issued.

GSAKMP - Group Controller



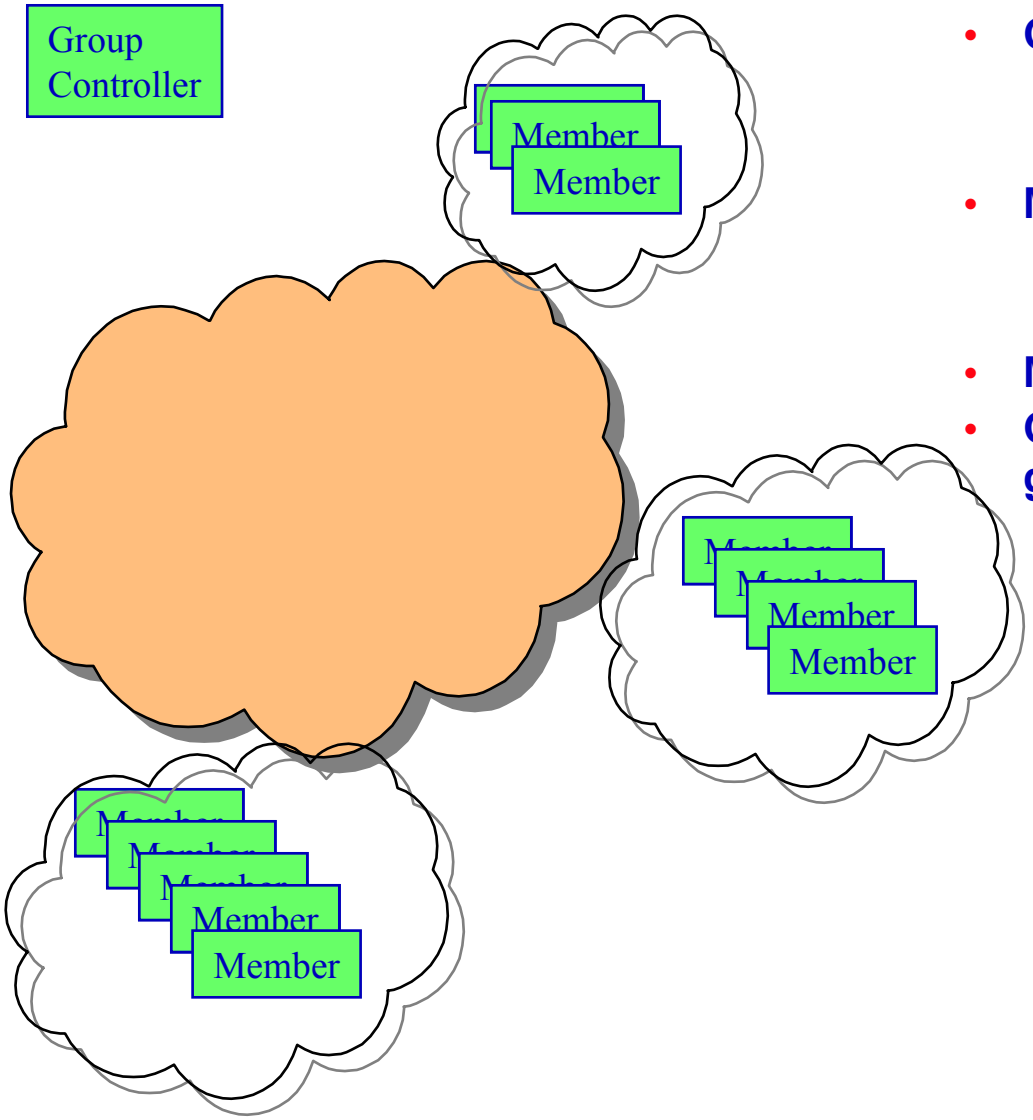
- **Group Controller**
  - Defines group policy
  - Creates initial keys

GSAKMP - Initial Joins



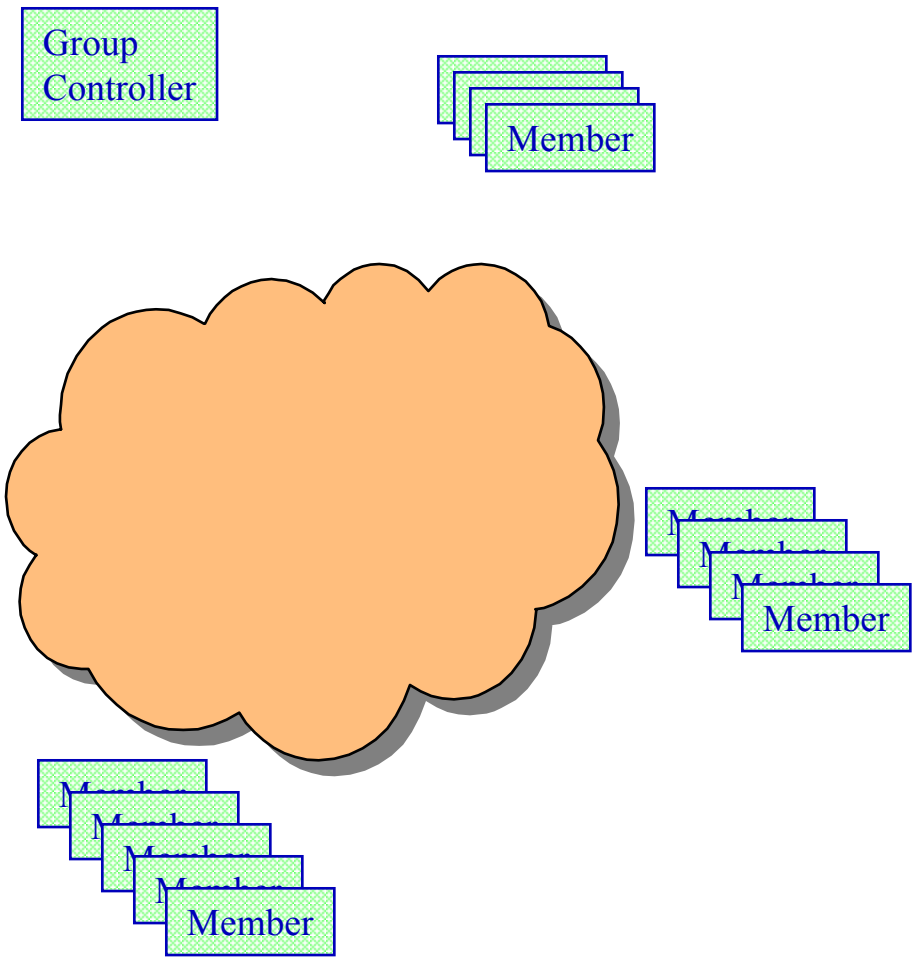
- **Group Controller**
  - Defines group policy
  - Creates initial keys
- **Members join the group**
  - Can become subordinate GCs
  - Can be key consumers

GSAKMP - Distributed Joins



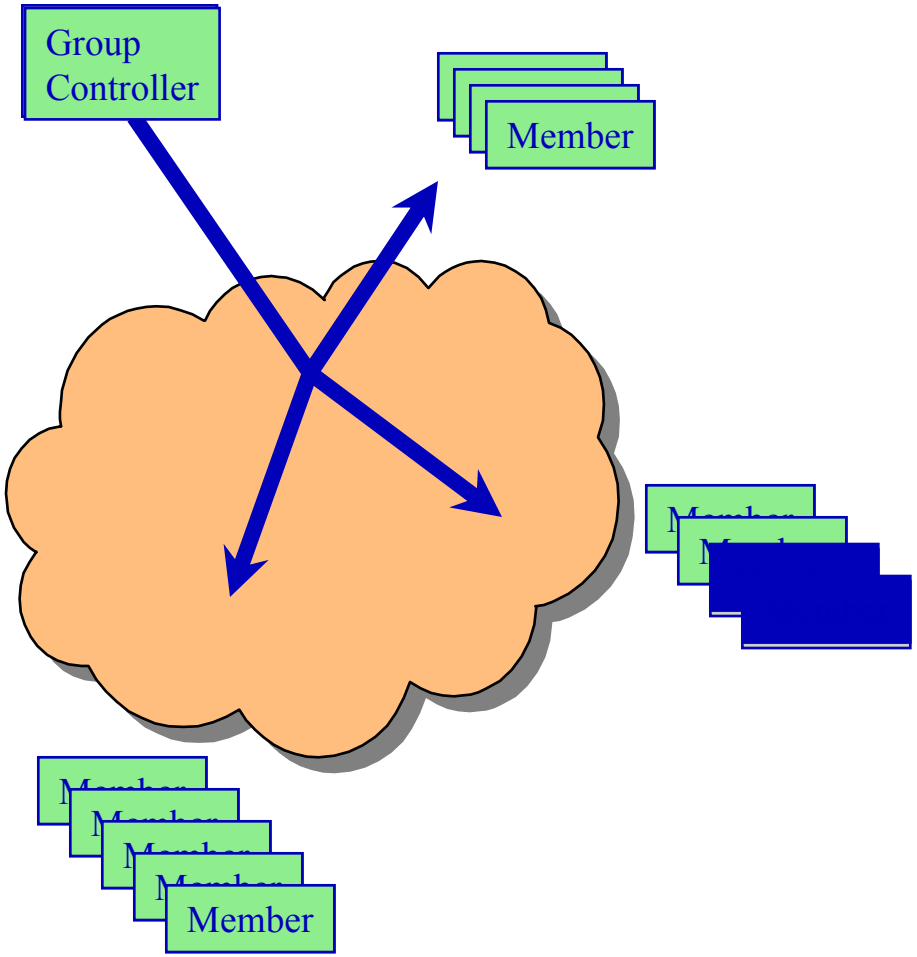
- **Group Controller**
  - Defines group policy
  - Creates initial keys
- **Members join the group**
  - Can become subordinate GCs
  - Can be key consumers
- **Member can get keys from GC or S-GC**
- **Group membership is managed using group cryptography**
  - One message can reconfigure membership of receivers

Membership management



- **Groups must endure**
  - Member expulsions
  - Changes in group Policy
    - » More restrictive
  - Merging with other groups
  - Splitting into sub-groups

Membership management

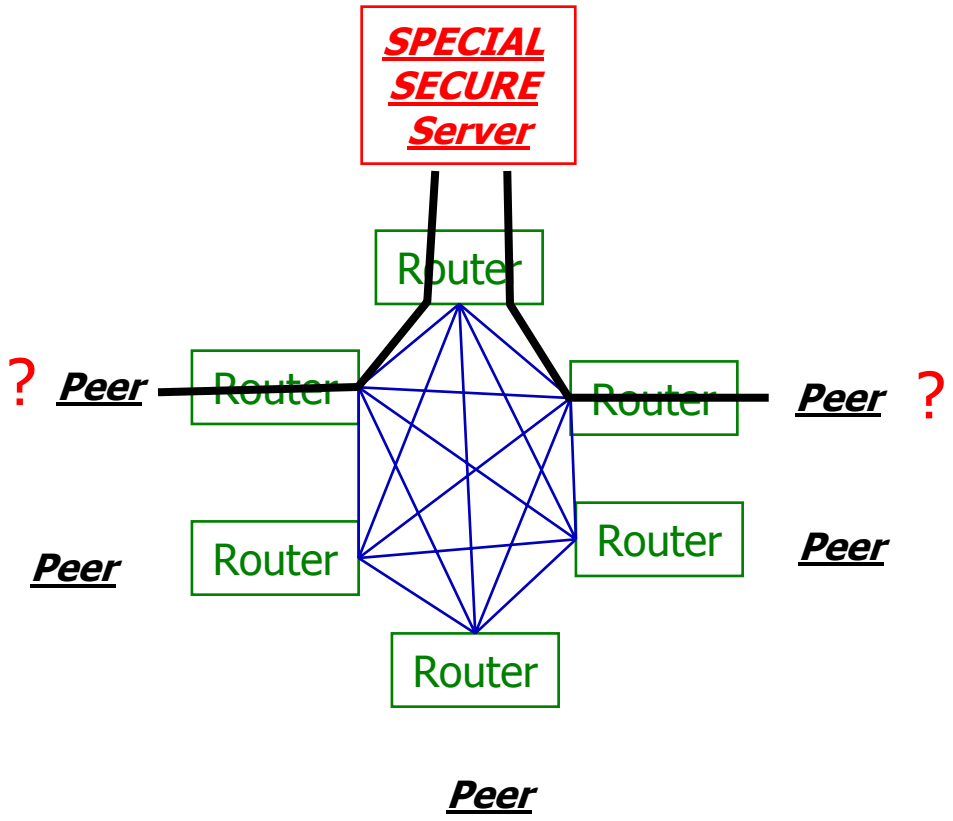


- **Crypto trees**
  - Allow efficient rekey of groups to reflect membership and policy changes.
  - One message can distribute new keys to all desired group members

Group Applications using GSAKMP

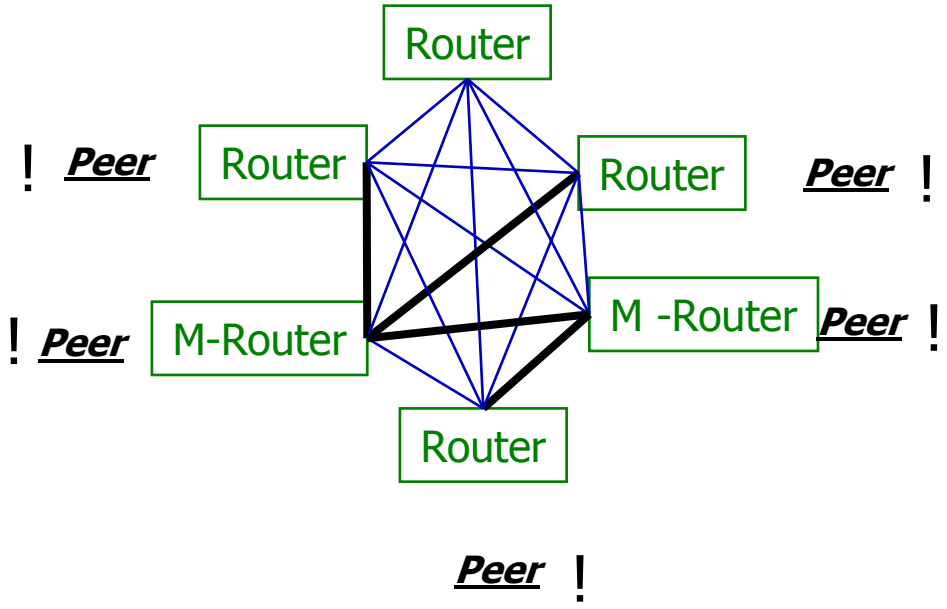
- **Secure Group Sessions**
  - VoIP Conferencing
  - Video Audio Teleconferencing
  - Data delivery to synchronized processing resources
  - Large data set applications
- **Secure Group Objects**
  - Web servers
  - Gnutella
  - Mail
  - IM
  - Chat
  - Push

Why not IPSec or SSL?



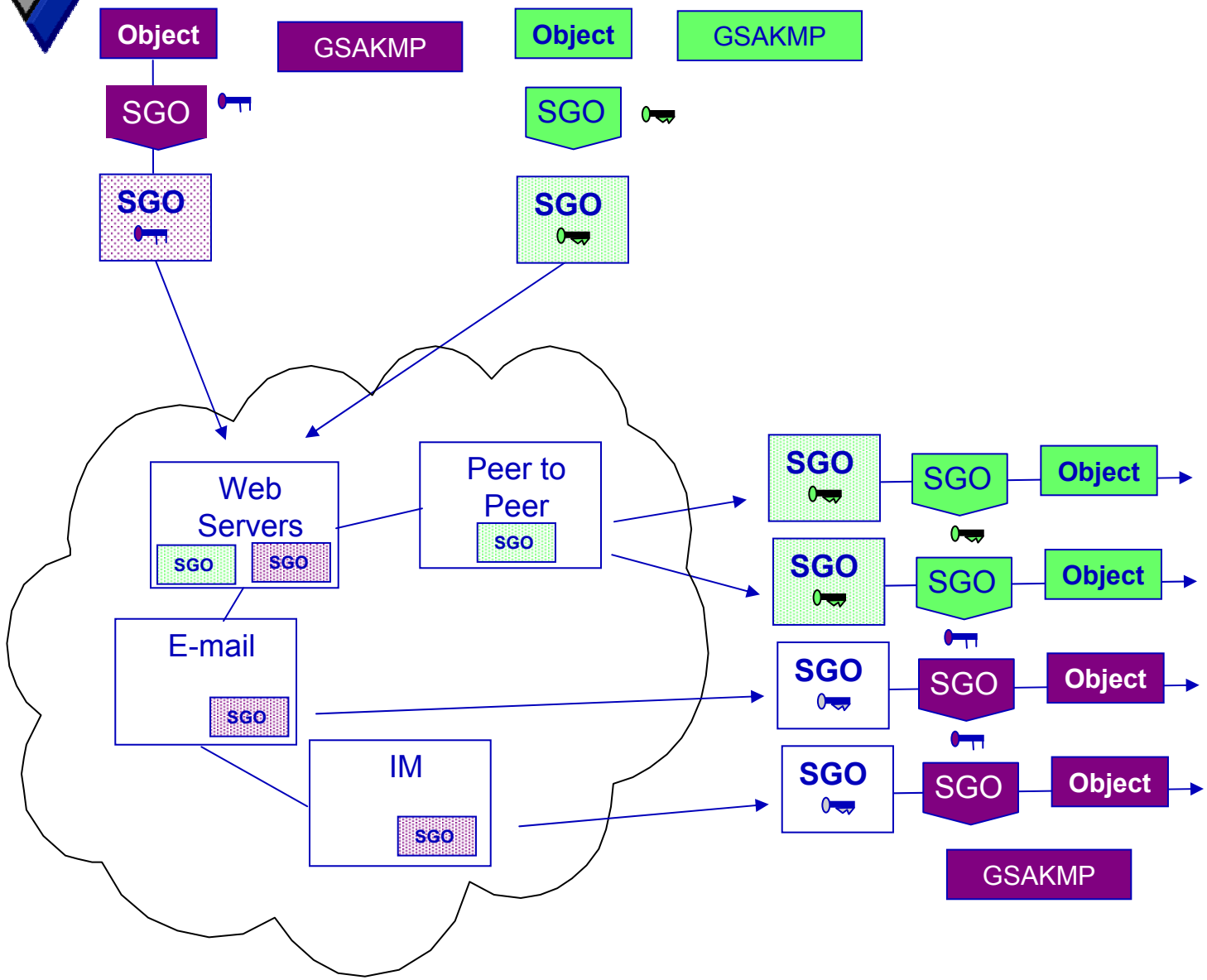
- **IPSec / SSL**
  - Point to Point Network/Transport layer connection
  - "Special" Server is in the middle
    - » Server in the middle attacks
    - » Server is security relevant
    - » Costs to create, architect, manage secure servers

Why Secure Group Sessions?



- **Secure Group Sessions**
  - If security is separated, then perhaps we can use multicast to communicate
  - Use the network
  - Less congestion
  - Less points of failure
  - Simple is good

SGO - Multi-application, Multi-path



Conclusions

- **Coalitions need Group Secure Associations**
  - Dynamic policy
  - Multiple infrastructures
  - Group key and policy management
- **Separating security from the communications allows**
  - Freedom in choosing communications applications
  - Focus on the real security boundary
  - Moving cryptographic solutions closer to the real endpoints makes the architects job easier
- **GSAKMP is the basis for dynamic GSAs**
  - Standards Track IETF RFC
- **Group Secure (sessions and objects)**
  - Provide a common security basis for many group applications
  - Improve the existing coalition group security paradigm