Group Security Association Definition for Multicast

draft-irtf-smug-gsadef-00.txt

Indermohan Monga

Thomas Hardjono

Nortel Networks

Goals

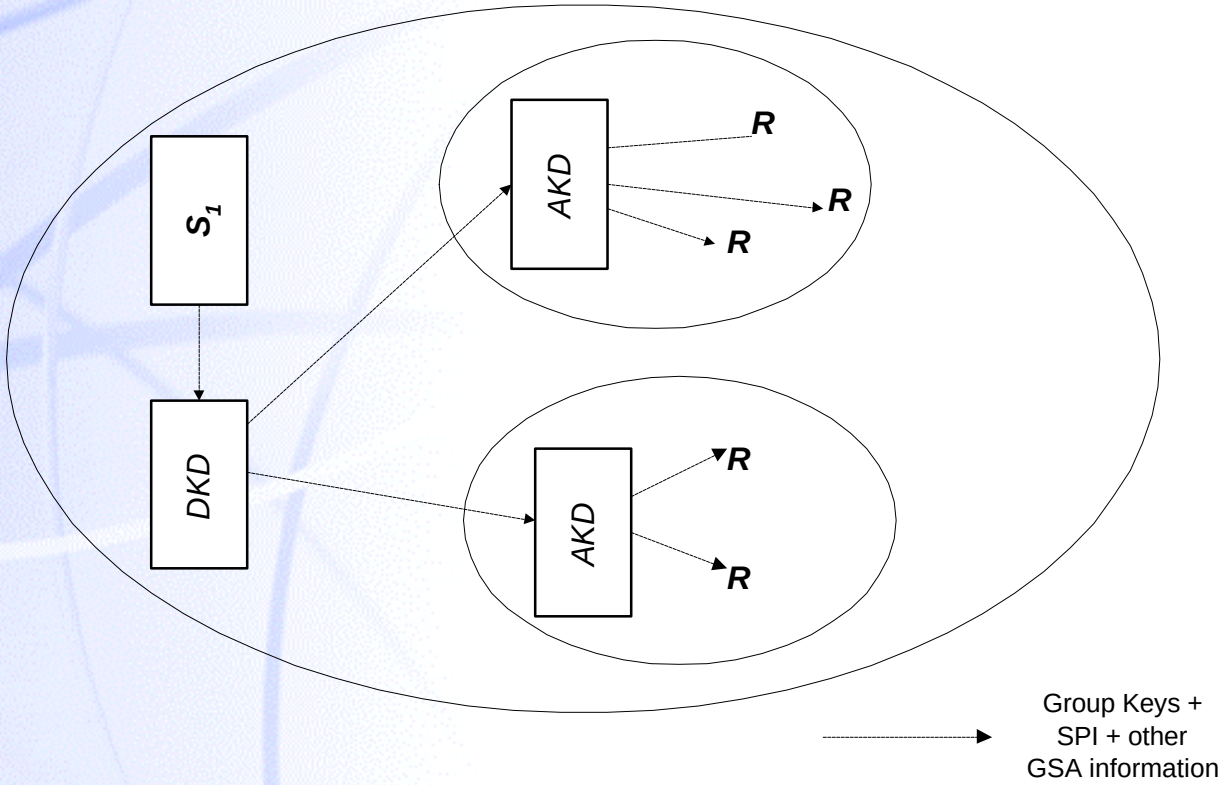
- Leverage IPsec Architecture concepts
- Re-use IPsec encryption and authentication protocols
- Maintain security services provided by IPsec protocols
- Simple to understand and implement

Benefits

- IPsec Security Association Database maintains GSAs. SAD design and lookup remains same.
- Replay prevention possible.
- Easier selective reception.
- Source authentication needed only once.
- M - M retains these advantages.

Brief Description

- GSA uniquely identified by (source IP address, SPI, IPsec protocol)
- Sender chooses GSA parameters with/without help from Key Distributor
- GSA distributed by GKM protocol along with group keys.


S1
DKD
AKD
R
R
R
AKD
R
R
Group Keys +
SPI + other
GSA information

Comparison

Group SA

- Transport only
- Anti- replay enabled
- Algorithm sender chosen
- SPI sender chosen
- Simplex, one per sender
- Lifetime chosen, maintained by sender

IPsec SA

- Tunnel / Transport
- Anti- replay enabled
- Algorithms negotiated
- SPI receiver chosen
- Simplex, one per sender
- Lifetime negotiated