The MSEC Extensions to IP Security

Brian Weis, Cisco Systems

George Gross, IdentAware™ Security

Dragan Ignjatic, Polycom

IETF-63, Paris, France, August 2nd 2005

RFC2401-bis IP Security Profile

- RFC2401-bis: ASM and SSM multicast SA, ESP, tunnel mode, IKE-v2 crypto-suite
- Concurrent co-existence with IKE-v2, requires SPD/SAD policy coordination
- SPD/SAD configurable by GO to three dominant multicast service models
- Require multiple speakers with anti-replay

Examples of IPsec Policy Objects

- Policy filters, a match triggers an action(s)
  - 5-tuple traffic selector filter
  - compound filter: prioritized filters sequence
- Policy actions
  - discard/log packet or allow packet to proceed
  - apply IPsec Group SA processing
  - multicast packet distributor
  - compound action: actions sequenced in a list

Security Associations Modes

- Transport
- Tunnel – must be supported by a GW, optional for a host implementation

Routing

- Address preservation
  - Destination address should have SPD-S PFP flag set
  - Some SSM implementations may need source address SPD-S PFP flag set as well
  - A new flag is introduced to copy remote address to the tunnel header remote address

SPD

- Directionality attribute
  - Common (as in 2401bis)
  - Send only
  - Receive only
- Both send / receive only should support multicast destination addresses
- Discard & bypass policies applied to the send only should only create entries in SPD-O
- Likewise, applied to receive only should only create entries in SPD-I

Traffic Processing

- Inbound traffic – SA’s point to their parent SPD entries
- Outbound traffic – any multicast destined traffic should be matched against SPD send only entries

SAD

- Replay protection is needed for multi sender SA’s - TBD

PAD

- Needs to be extended for peers with specific roles:
  - GCKS
  - Group Speaker
  - Group Member
  - Root Certs used by the group

NAT’s

- SSM adversely impacted by it
  - GCKS can not be preconfigured with NAT mappings
  - SSM routing depends on the source address that NAT changes
  - ESP cloaks its payloads from NAT gw
  - UDP checksum depends on source address
  - AH can not be used