Changes from -00

• Scope was refined
  – Composite Groups was removed, and will be re-introduced as a separate document

• Lots of cleanup
  – Terminology
  – References
  – Consistent wording, tone, etc.
Overview of -01

• Further defines the security services for IP multicast packets with RFC 4301
  – Allow IP multicast packets to be processed by IPsec and remain as IP multicast packets
  – Describe additional semantics to the SPD, SAD, and PAD to support this goal.
  – Identifies new SA attributes by which a group key management protocol can signal the new semantics to IPsec.
Overview of -01 (cont.)

• Describes the MSEC Group SA (GSA) for IPsec
• Describes IP Traffic Processing for IP multicast traffic matching an IPsec SA
• Describes the issues of NAT with IPsec multicast packets.
IPsec-protected multicast packets

• Host Implementation
  – “MAY use both transport mode and tunnel mode to encapsulate an IP multicast packet.”

• Gateway implementation
  – “MUST use a tunnel mode SA”
  – SAs with a single source address and single destination address use normal tunnel mode processing.
  – This draft defines “Tunnel Mode with Address Preservation” for SAs with richer traffic selectors.
    • The source address and/or destination address is carried forward to the encapsulating IP header.
SPD support for Tunnel Mode with Address Preservation

• A gateway needs to retain the destination address of an IP multicast packet if the packet is to be routed properly.
  – Accomplished by setting the Remote Address PFP flag in the SPD-S entry for the traffic selectors

• A gateway needs to retain the source address of an IP multicast packet if the packet is to be forwarded down the correct multicast distribution tree.
  – Accomplished by setting the Source Address PFP flag in the SPD-S entry for the traffic selectors
SPD Directionality

• An SPD entry can be installed *directionally*.  
  – “Sender only”. The IPsec system may only send IPsec packets matching this entry.  
    • SHOULD support multicast IP address as destination  
    • Bypass/Discard: entry SHOULD be put only in SPD-O  
  – “Receiver only”. The IPsec system may only receive IPsec packets matching this entry.  
    • SHOULD support multicast IP address as destination  
    • Bypass/Discard: entry SHOULD be put only in SPD-I  
  – “Symmetric”. The IPsec system may send and receive IPsec packets matching this entry.  
    • SHOULD be the default directionality
SAD

• Outbound SA:
  – Source Address is that of sender
  – Destination Address is the multicast group address.

• Inbound SA:
  – Configured with the source addresses of each peer authorized to transmit to the multicast SA
PAD

• Roles needed, each of which may have different authorization rules
  – GCKS
  – Group Speaker
  – Group Receiver

• Group “trusted root certificates” are included in the PAD.
PAD

• Management Interface required
  – “MUST allow an administrator to enforce that the scope of a GKMP group's policy specified SPD/SAD modifications are restricted to only those traffic data flows that belong to that group”
  – “MUST provide a mechanism(s) to enforce that IKEv2 security associations do not negotiate traffic selectors that conflict or override GKMP group policies.
  – “SHOULD offer PAD configuration capabilities that authorize the GKMP policy configuration mechanism to set security policy for other aspects of an endpoint's SPD/SAD configuration, not confined to its group security associations.”
New SA Attributes

• A Group Key Mgmt Protocol (GKMP) MUST support the following attributes
  – Address Preservation: source only, destination only, or both source and destination addresses
  – Direction: Sender only, Receiver only, or Symmetric (default)
• Details of the attributes are left to each GKMP
GSA for IPsec

- GSA includes all IPsec SAs and one or more GKMP SAs for the group.
  - IPsec SA lifetimes can be concurrent
    - If each group speaker has a unique SA
    - SAs with the same traffic selectors overlap in time for continuity during a rekey event
- The process of replacing an SA is specified in the draft (Section 4.1.4.1)
Outbound Traffic Processing with Address Preservation

- If the source address is marked for an IPsec SA
  - During header construction “src address” header field MUST be “copied from inner header” rather than “constructed”

- If the destination address is marked for an IPsec SA
  - During header construction the “dest address” header field MUST be “copied from inner hdr” rather than “constructed”
Inbound Traffic Processing with Address Preservation

- If the source address is marked for an IPsec SA
  - Outer source IP address MUST match the inner source IP address
- If the destination address is marked for an IPsec SA
  - Outer dest address MUST match the inner dest IP address
- If either check fails the packet MUST be discarded, and it MUST be an auditable event.
NAT issues

• Many issues! See Section 6.1
  – Unreliable Transit IP addresses in the SPD
  – Changes of NAT mappings affect the SPD
  – ESP cloaks its payloads from a NAT GW
  – Etc.
Next Steps

Is it ready for IPsec mailing list review?