# Multicast ESP

Mark Baugher (Cisco Systems), Ran Canetti, P. Chen, P. Rohatgi (IBM)

# Overview

- The problem we are trying to solve
- What's wrong with IPsec ESP?
- What is MSEC MESP?
- Discussion
- TESLA

# Multicast Data Security

- There are three issues
  - Source message-authentication (SrA)
  - Relating SrA to group authentication (GA) & group secrecy (GS)
  - Support for IGMPv3 SSM operation

The following three slides address each of the three issues listed above.

# 1. Authenticating the Source of Multicast Messages

- When group size > 2, one group member might impersonate another sending member
- Asymmetric techniques work for some (small number) of applications
- Newer more-efficient solutions exist that might be suitable at the IP layer

MESP is a framework for group source message authentication algorithms; TESLA is the first.

# 2. Multicast Has New Message-Authentication Distinctions

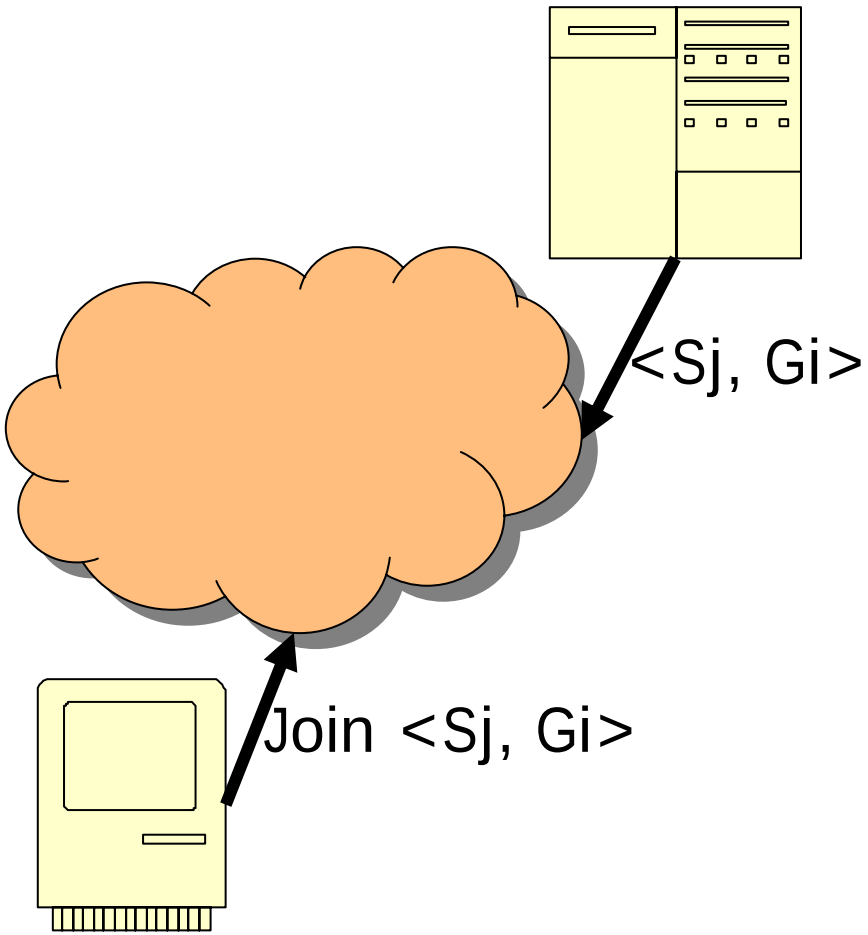
- Secrecy is group based (Group Secrecy)
- MAC authentication authenticates a source as a group member only (Group Authentication)
- Digital signatures and some MAC-based schemes can uniquely identify a source (Source Authentication)
- MACs can protect digital signatures

# Multicast Data Security Services

- Point-to-point Security Services
  - Confidentiality
  - Message integrity
  - Message Source-Authentication
- Multicast Security Services
  - Group Secrecy
  - Group Authentication
  - Source Authentication

Group secrecy is group analog to confidentiality; group authentication gives message integrity and validates the message originated from a member; source authentication validates that it originated from a specific group member

# 3. Source-Specific Multicast (SSM)




- IGMPv3 redefines a multicast group to be source-specific
- <*, G> is an Any-Source Multicast group (ASM)
- <S, G> is a Source-specific Multicast group (SSM)

# IPsec ESP Multicast Issues

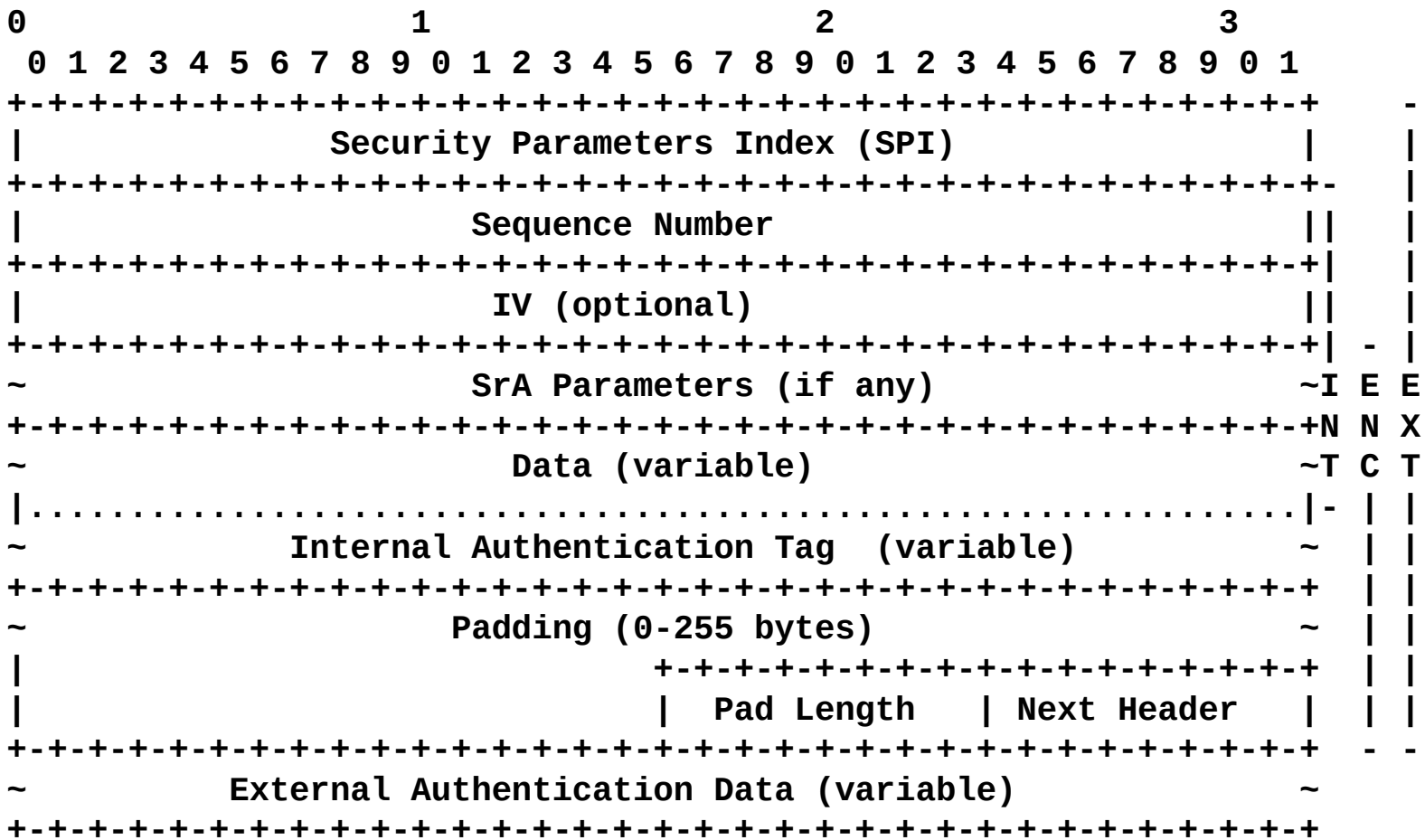
- IPsec SA lookup does not use source address
- IPsec message authentication is not source message authentication (aka “data origin authentication”) for groups
- IPsec ESP format doesn’t accommodate multiple authentication types
- IPsec ESP does not protect digital signatures

Thus, we choose to develop MESP as a new IP security protocol that closely resembles IPsec ESP.

# Multicast ESP (MESP) Design

- Extends ESP but is a separate protocol
  - MESP to have its own protocol number
  - Has 2 forms of authentication, GA & SrA
  - Scales down to ESP when SrA not offered
- Uses internal & external authenticators
  - GA HMAC is external
  - Can protect an internal auth digital sig
  - Accommodates MAC-based source auth

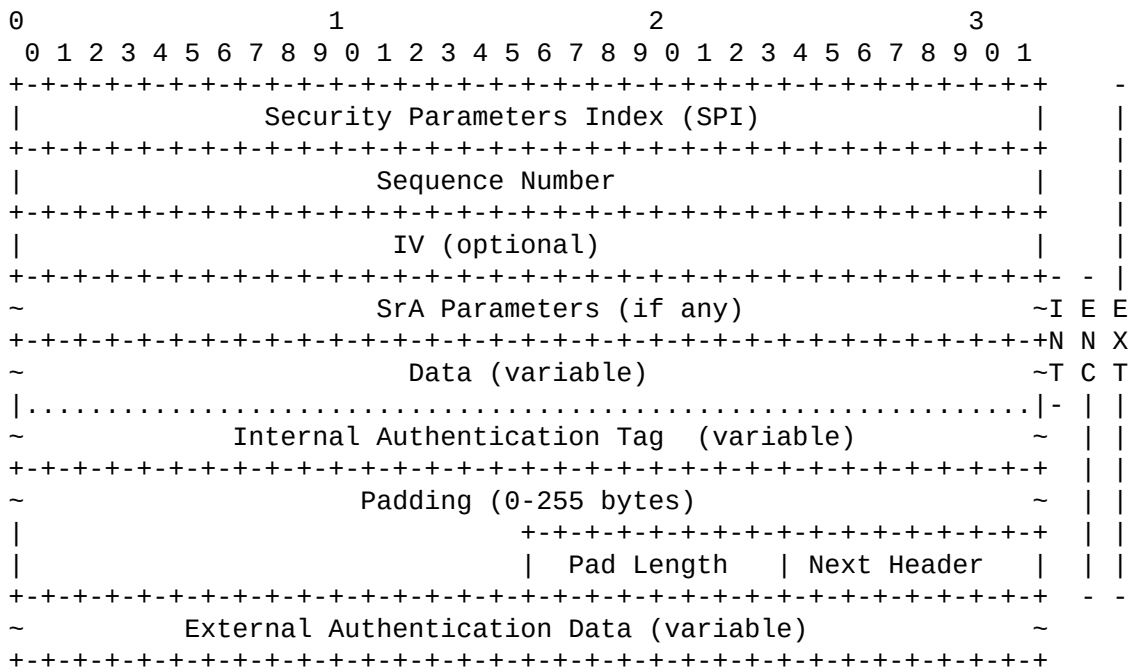
# MESP Packet Format



# MESP Transforms

| Transform Class | Transform Identifier | Dependencies |
|---|---|---|
| INT | RSA-SHA1 | HMAC-SHA1 EXT |
| | NULL | None |
| ENC | Any ESP encryption transform [RFC2407] | None |
| EXT | HMAC-SHA1 | None |
| | TESLA | No INT |

# Default & Mandatory Transforms




- INT default is RSA-SHA1
- ENC default is 3DES-CBC
- EXT default is HMAC-SHA1

# GDOI Signaling

| class | value | type |
|---|---|---|
| INT Transform | 1 | B |
| EXT Transform | 2 | B |
| Encapsulation Mode | 3 | B |
| SA Life Type | 4 | B |
| SA Life Duration | 5 | V |
| - GDOI SA TEK Attributes - | | |

Adds PROTO_MSEC_MESP to GDOI and reuses ESP's GDOI payload (SA TEK payload). Sig PubKey is sent in KD payload.

# Summary

- We want to promote MESP over IPsec ESP for multicast and group applications
- We have an issue INT, EXT and SrA, GA authentication: Should INT = SrA?
- Need definitions for MIKEY and GSAKMP