Multicast ESP <draft-ietf-msec-mesp-01.txt>

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

Overview

- Changes from previous draft
- The problem we are trying to solve
- What is MSEC MESP?
- Open issues
- Signaling
- Summary

Changes from Previous Draft

- MESP started as a multi-layer security protocol in SMuG
- MESP resumed as a multicast variant of IPsec ESP in MSEC
- MESP re-defined as a multicast transform-framework for ESP today

ESPbis has incorporated needed multicast features and so MESP need not be a separate protocol.

Multicast Data Security

- The MESP framework is for multicast IPsec data-origin authententication
  - 3 MESP framework services
    - Source message authentication (SrA)
    - Group authentication
    - Group Secrecy

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

1. Authenticating the Source of Multicast Messages

- When group size > 2, symmetric MACs don't provide data-origin authentication
- 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 one of the first.

2. Group Authentication

- MAC authentication authenticates a source as a group member only (Group Authentication)
- MACs protect digital signatures against DoS attacks
- MACs protect timed MACs (TESLA) against DoS attacks

AES-XCBC-MAC-96 and combined mode MACs may not fulfill the DoS protection functions

3. Group Secrecy

- IPsec ESP confidentiality in a group security setting
- Generally, IPsec encryption transforms are suitable for multicast operation
- Each should be evaluated, however briefly, as suitable for multicast

Multicast Data Security Services

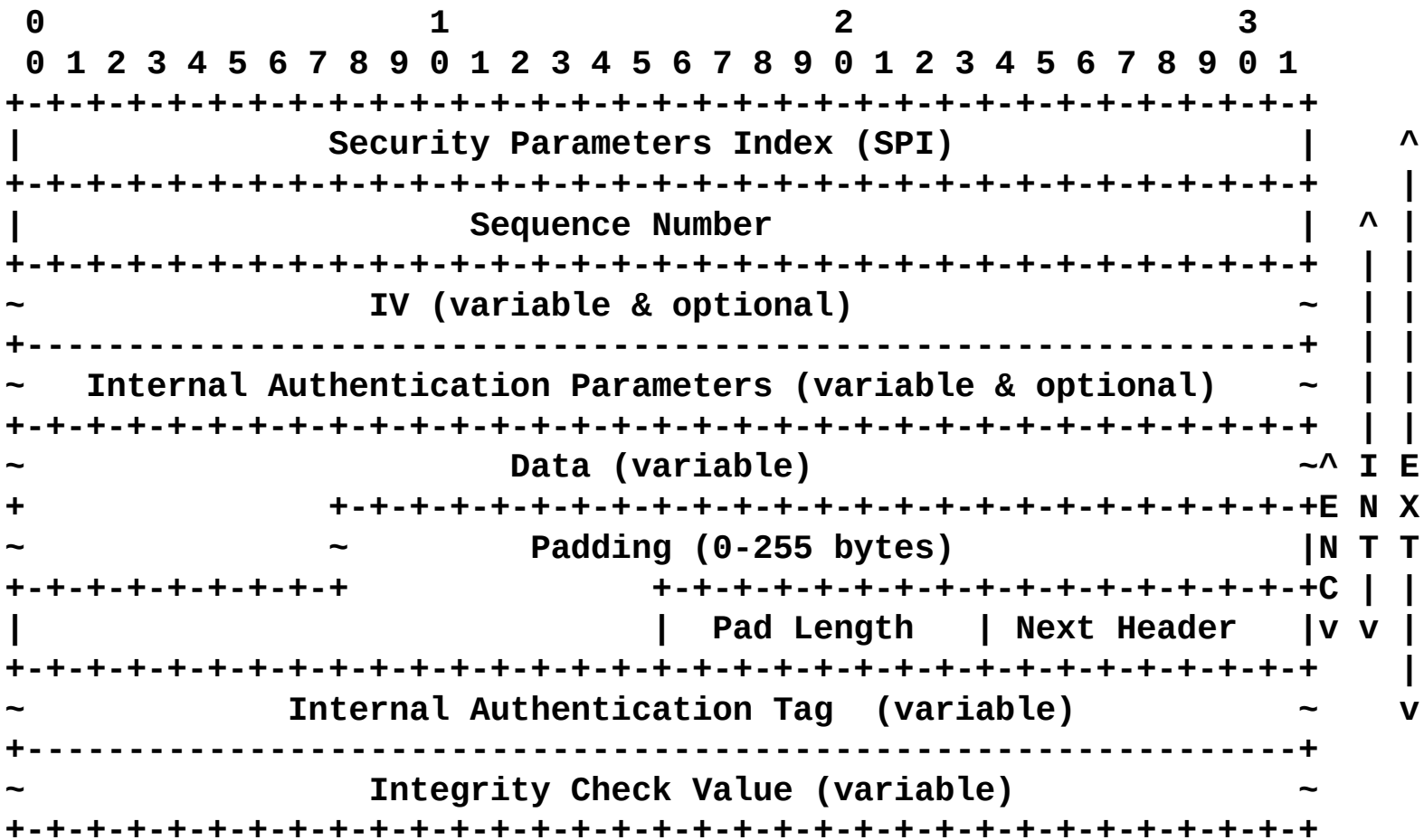
- Point-to-point Security Services
  - Confidentiality
  - Message integrity
  - Message Source-Authentication
- Multicast Security Services
  - Group Secrecy
  - Group Authentication
  - Source Authentication

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

Multicast ESP (MESP) Design

- A transform framework for ESP
  - Defines GS, SrA and GA functionalities
    - Predetermined sender order: GS, SrA, GA
  - GA protects SrA
- Uses internal & external authenticators
  - SrA called “internal authentication”
  - GA called “external authentication”
  - GA protects SrA

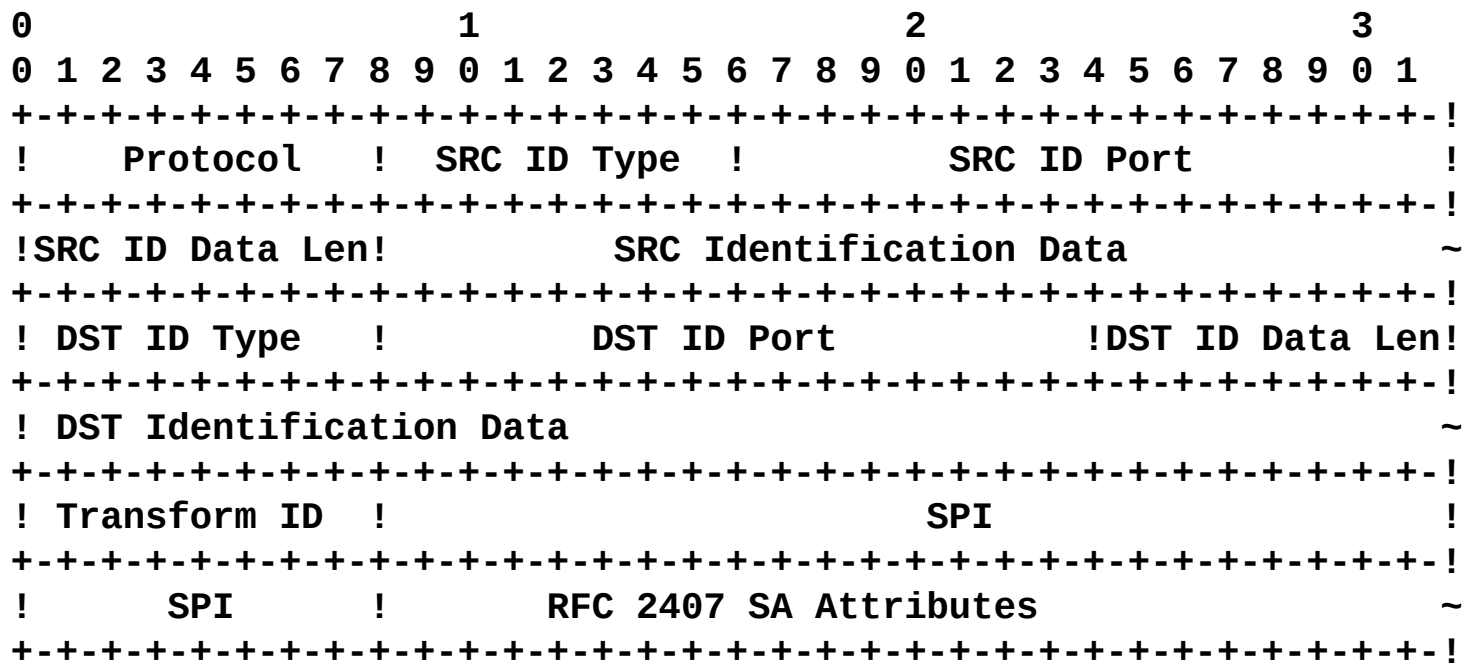
MESP Packet Format



Some Open MESP Issues

- EXT (GA) as a MUST or SHOULD?
- INT (SrA) as a MUST or SHOULD?
- AES-MAC and combined-mode xforms don’t serve the GA function well
- AHbis could serve the GA function

GDOI Signaling: SA TEK



MESP is a new IPsec Transform ID. The ENC, INT and EXT transforms are new SA attributes

GDOI Signaling: SA Attributes

class	value	type
ENC-Transform	11	B
INT-Transform	12	B
EXT-Transform	13	B

ENC-Transform has the values:

name	value
Reserved	0
3DES	1
AES-CBC	2
AES-CTR	3

INT-Transform has the values:

name	value
Reserved	0
RSA-SHA	1
TESLA	2

The EXT-Transform has the values:

name	value
Reserved	0
HMAC-SHA1	1

Summary

- We want to promote MESP as a transform framework for multicast IPsec ESP applications
- We have several issues
- Need definitions for MIKEY and GSAKMP
- Need to work on implementation concurrent to TESLA development

TESLA Overview

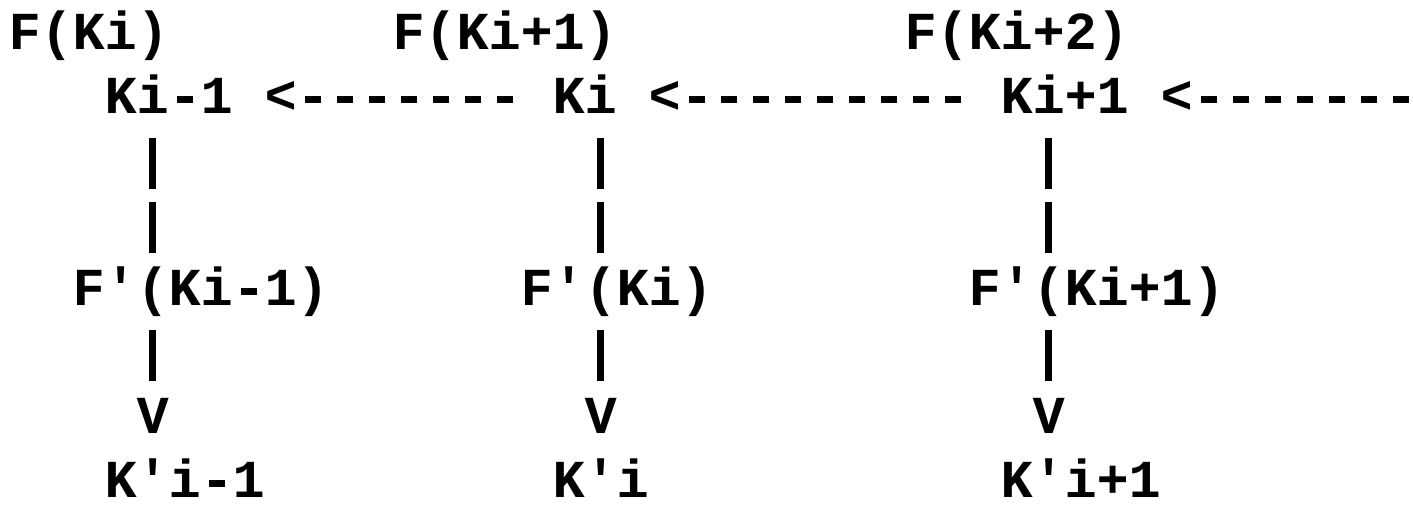
Overview

- TESLA developed by Perrig, Canetti, et. al. as an efficient source authentication transform
- Seems to have advantages over other MAC-bases source authentication schemes
- It is destined to be used by MESP
- There are some complexity issues with TESLA
- Need to consider if this is something that belongs in the kernel

TESLA Properties

- High guarantee of source authenticity for multicast groups
- Does not provide non-repudiation
- Robust against loss and re-ordering
- Low overhead of 12-20 bytes/packet
- Delayed disclosure & receiver buffering
- No sender buffering

Deriving Authentication Keys

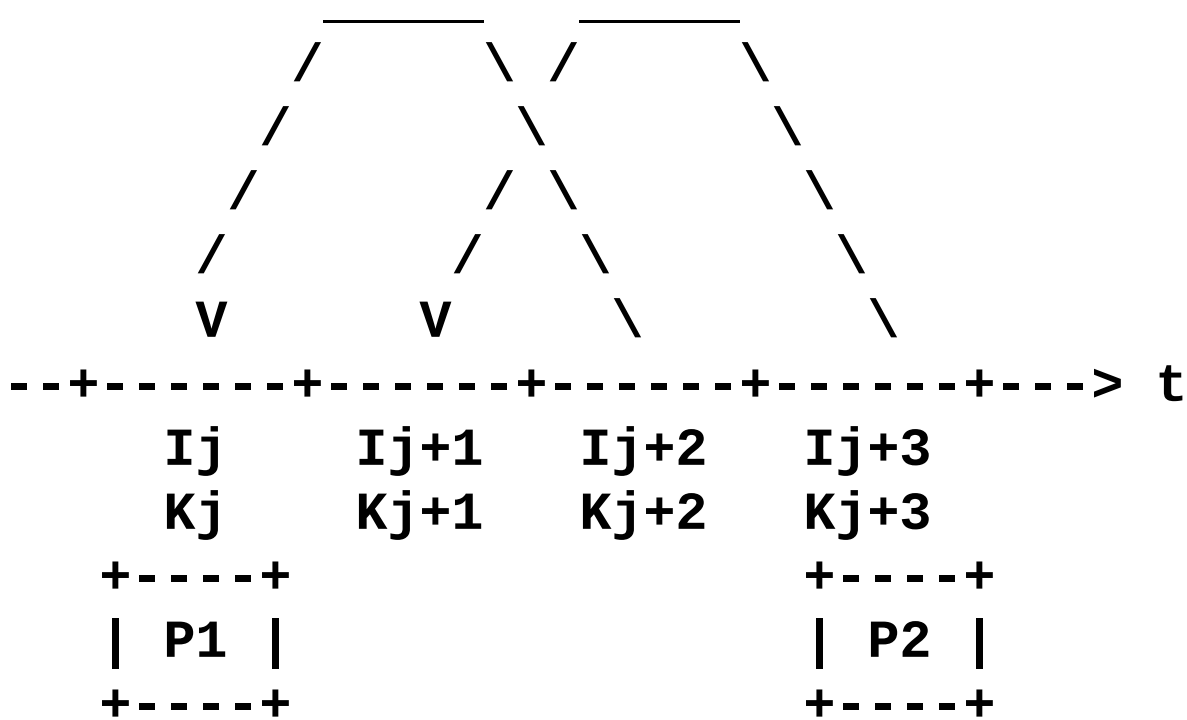


Based on an old scheme: Lamport's One-Way Hash Chain (1981) and S/KEY (RFC 1760). HMAC-SHA1 is just one type of one-way function that can be used.

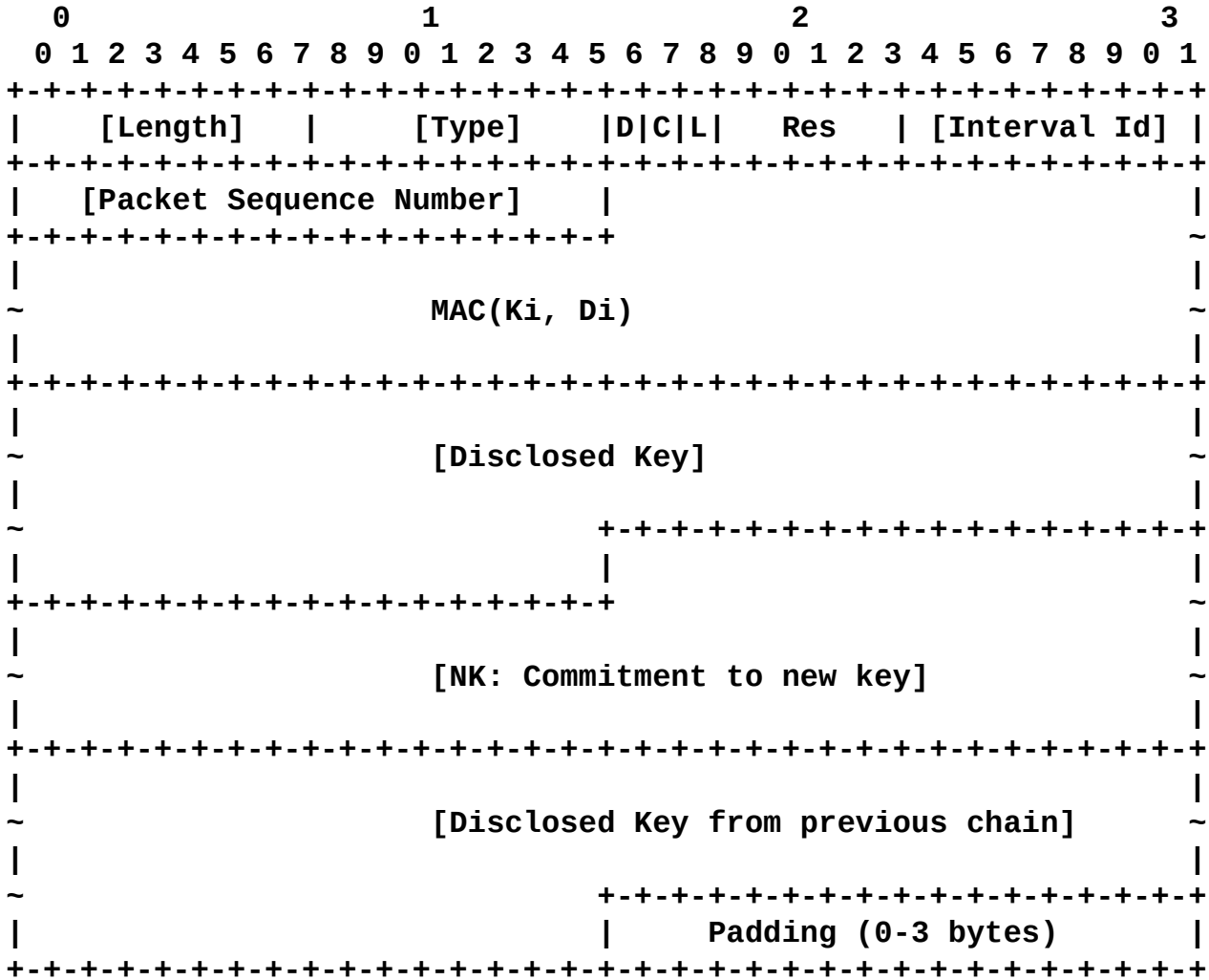
Based on Hashed Key Chain

- $K_i = HMAC(K_{i-1}, 1)$, $K_0 = K$
  - Sender selects chain length N
  - Precomputes chain from N-1 to zero
- K is digitally signed by sender
  - Disseminated e.g. by key management
  - One sig per arbitrarily long “key chain”
- $K_i' = HMAC(K_i, 0)$ is HMAC key for packet
- K_i' used for all packets in interval i

TESLA Packet Processing



TESLA Packet Format



TESLA Issues

- Time synch
  - Packets received after key disclosure
  - Receives with vastly different sender RTTs
- Receiver buffering
  - Problematic in the kernel
- Others?