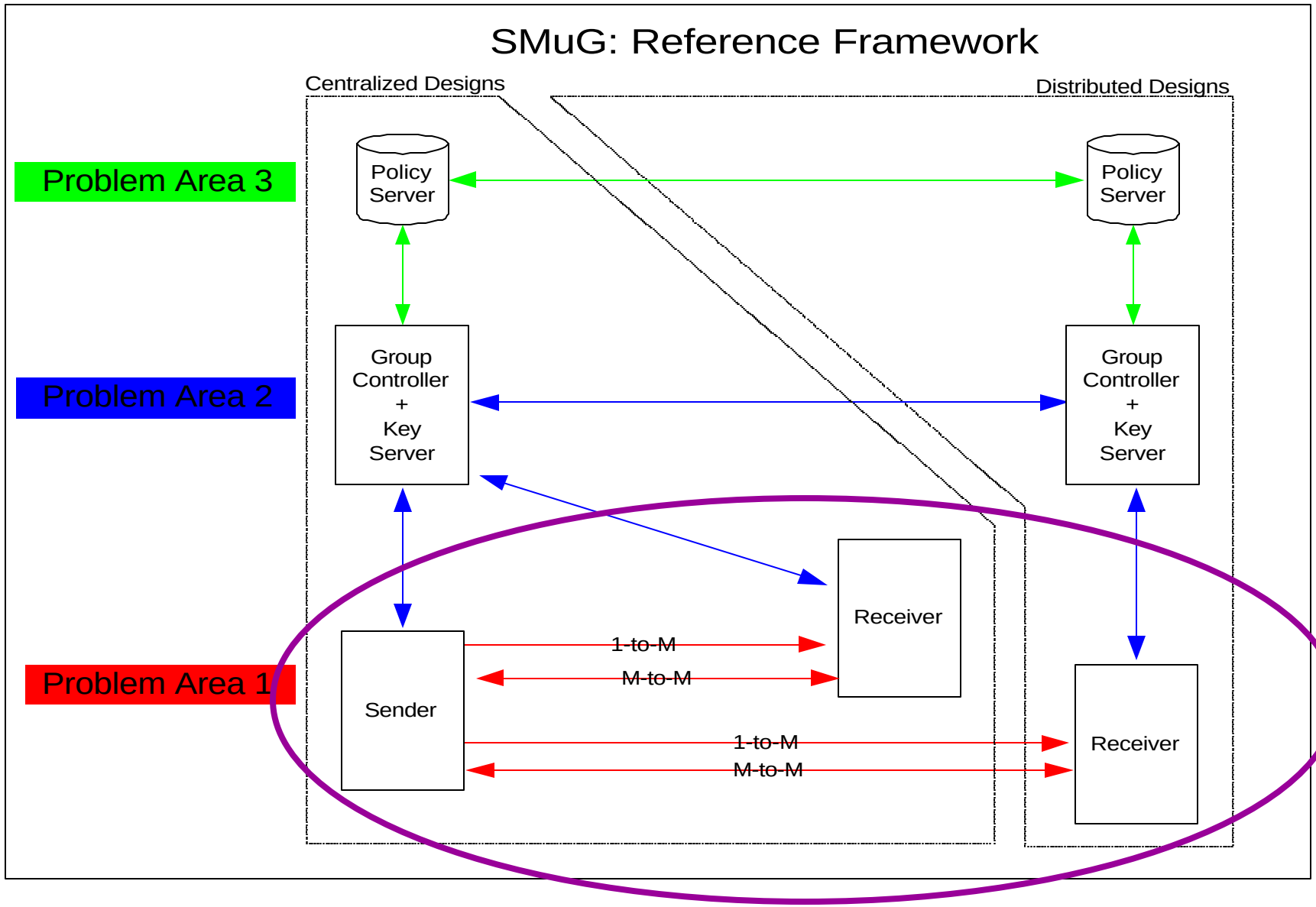
Multicast Data Security Transformations

draft-irtf-smug-data-transforms-01.txt

Ran Canetti, Pankaj Rohatgi Pau-Chen Cheng
IBM Watson

A reference framework: The building blocks at a glance



The desired functionalities

- Group confidentiality (GS):
  - Guarantee that only group members have access to the communicated data.
- Group Authentication (GA):
  - Guarantee that received data was generated by *some* group member.
- Source Authentication (SA):
  - Guarantee that received data originates with claimed sender and was not modified en-route.

Deployment Issues (I):
Placement in communication layers

- Data Encryption and Group authentication:
  - Standard encryption methods exist (ESP, SSL/TLS)
  - Can be done on any-size frames, no need in state across frames.
- Source Authentication:
  - Many different algorithms, new ones keep coming up.
  - Some algorithms more suitable to transport/application, some more suitable to IP layer.
  - Typically state kept across frames/packets

Deployment Issues (II):
Order of application

- Conflicting requirements:
  - For authentication, MAC is better done on the ciphertext.
  - For non-repudiation, signature is better done on the cleartext.

Deployment Issues (III):

- Interaction with RM protocols:
  - SA is easier if RM is provided.
  - FEC-based RM needs SA on individual packets/frames (I.e., “below” the RM transform)
  - Retransmission-based RM needs the encryption to be done “above” the RM transform (unless repair-nodes have access to group key)
- Should transforms include only a single functionality or should there be aggregation?

A proposed design

- Two “identical” transforms:
  - One in IP layer, one in transport/application layer.
  - Each transform can provide all three security functionalities: SA, GA, GS.
  - Group policy will specify where is each functionality carried out.

The IP-layer transform: MESP

- An extension of ESP, where the encryption algorithm is extended to potentially include an "internal authentication" mechanism:

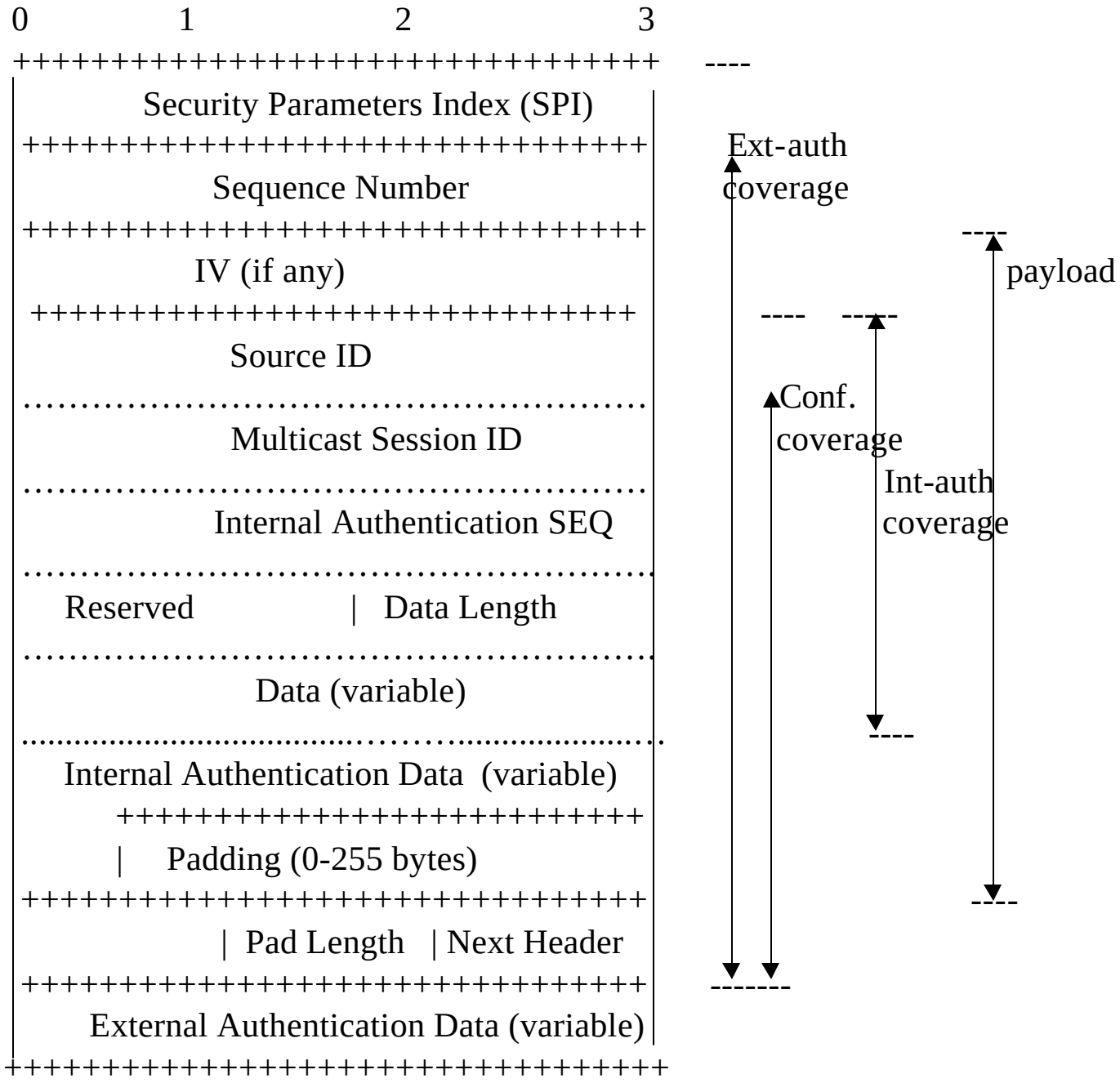
  Ext-auth[Enc[Int-auth[Data]]]

- When no Int-auth is provided, it is identical to ESP. In particular, can keep the IANA prorocol number of ESP (protocol 50).

The IP-layer transform: MESP

- Ext. authentication can provide either GA or SA. (Currently ESP provides GA. Using, say, TESLA, can provide also SA.)
- Int. authentication will typically provide signature-based SA.

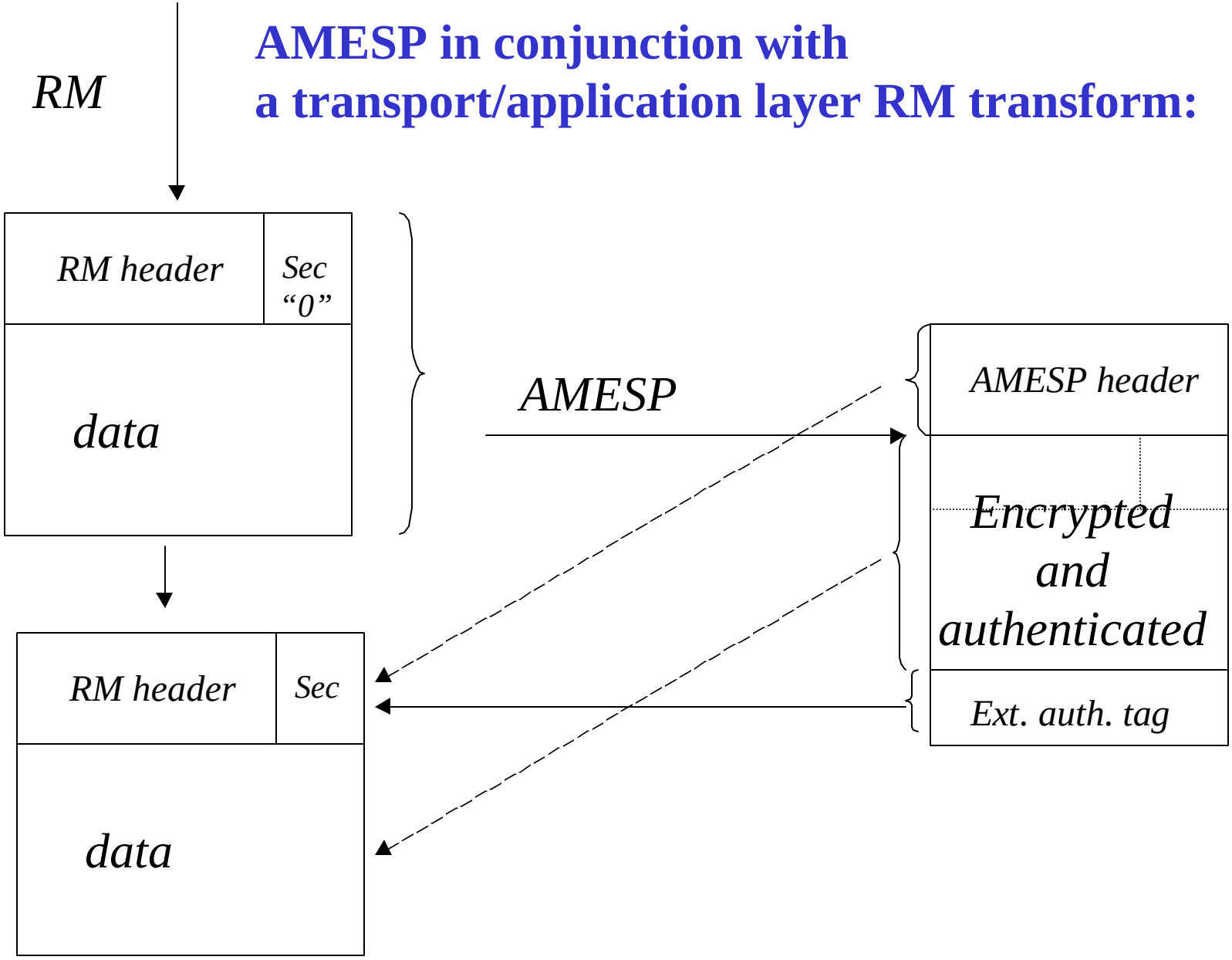
MESP packet format



The transport/application layer transform: AMESP

- Identical to MESP, with the exception that the IP header and next-protocol are not necessary.
- Can be used either as a stand-alone transform or in conjunction with an RM transform.

AMESP in conjunction with a transport/application layer RM transform:



Possible usage patterns

- Everything in application layer:
  - AMESP with GA[ENC[SA[data]]
  - AMESP with SA[ENC[data]]
  - Null MESP
- Everything in IP layer:
  - Null AMESP
  - MESP like AMESP in above case
- Mixed: SA in App, GS+GA in IP, etc.