Inband key updates

Lakshminath Dondeti

ldondeti@qualcomm.com

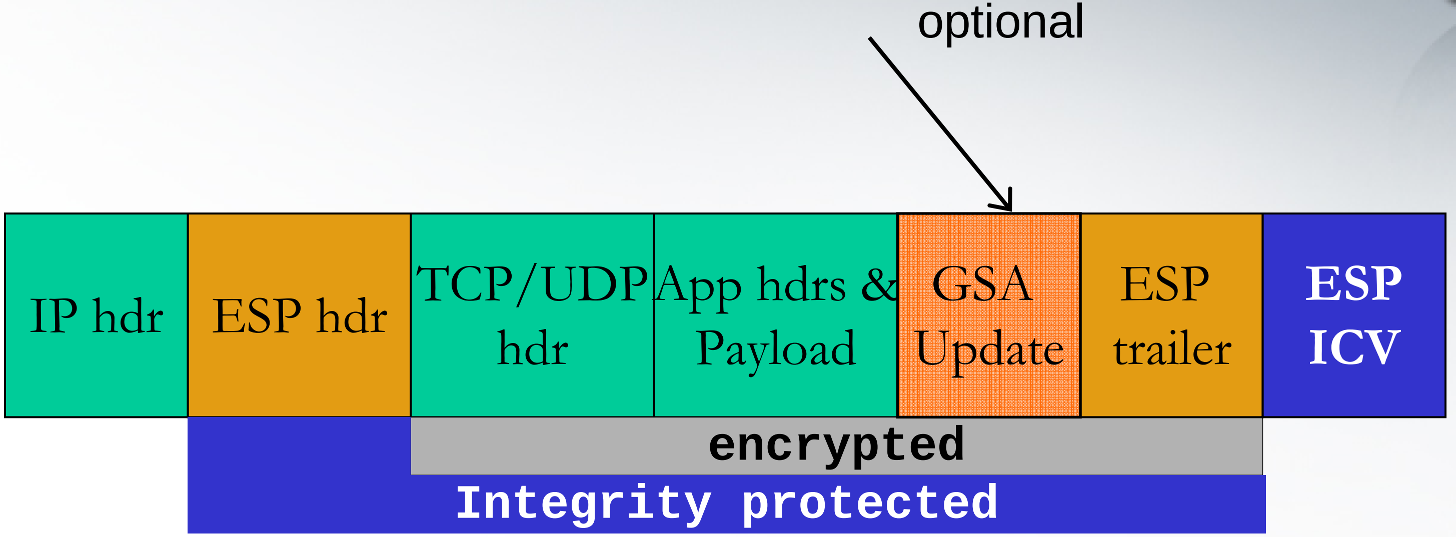
What?

- Proposal to send GSA updates via data encapsulation protocol
- Send a rekey message or some portion of it via IPsec or SRTP
- Credits
  - – I have heard similar proposals from others before
    - Ran?

Why?

- GSA updates may be lost in transmission
- Current approach is to send a few times and
  - pray …
  - The unfortunate receivers are required to re-register
- Others are doing it already
  - e.g., 3GPP2 BCMCS specification uses the MKI field
  - Recall that the MKI field is not integrity protected
    - It doesn’t need to be if used for the intended purpose
    - A variable length field so an attractive place to piggyback on

How?



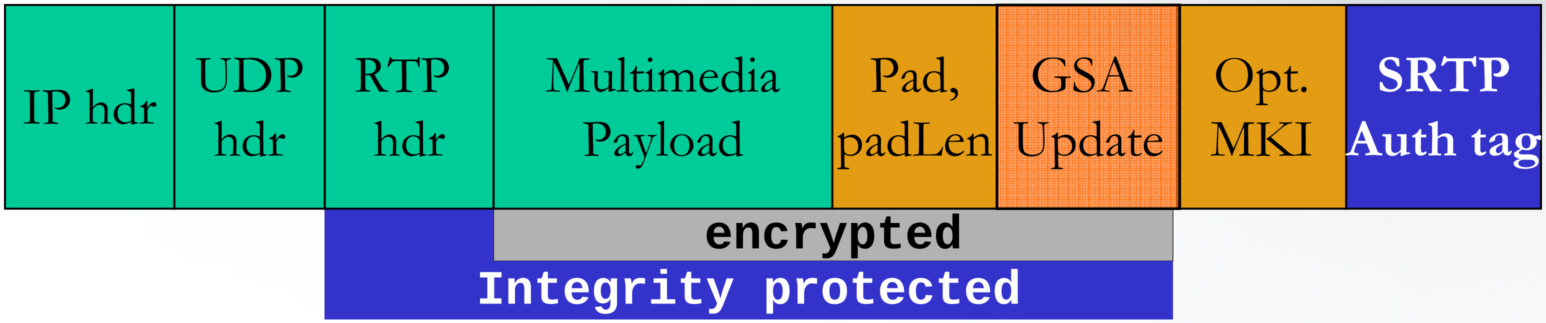
optional

IP hdr	ESP hdr	TCP/UDP hdr	App hdrs & Payload	GSA Update	ESP trailer	ESP ICV

encrypted

Integrity protected

How?



IP hdr

UDP hdr

RTP hdr

Multimedia Payload

Pad, padLen

GSA Update

Opt. MKI

SRTP Auth tag

encrypted

Integrity protected

Shall we?

- Strawman proposal for the WG’s consideration
- Need comments on why this is good, bad or ugly
- Please send your reviews to the list
  - If there is consensus (Ran will decide), we’ll make this a WG item