SRTP STORE-AND-FORWARD USE CASES AND REQUIREMENTS

JOHN MATTSSON, ERICSSON
AVTEXT, IETF 80, PRAGUE, MARCH 2011
ANY APPLICATION WHERE AN UNTRUSTED MIDDLEBOX NEEDS TO STORE AND LATER FORWARD ENCRYPTED MEDIA.

1) Server streaming pre-encrypted media.

2) Client recording streamed encrypted media.

3) Network node caching/recording streamed encrypted media.
WHY AN EXTENSION IS NEEDED

› Can existing protocols be used for encrypted?

› Transport protection in SRTP is dependent on the header.
  – Needed: Header independent payload protection.

› Context identification in SRTP is dependent on transport parameters.
  – Needed: Context identification independent of transport parameters.

› Other protocols (i.e. ISMACryp) are not published by a recognized standards development organization (SDO). As ISMA has ceased to exist, active maintenance is questionable.
  – Needed: Lightweight solution published by a recognized SDO.
REQUIRED AND DESIRED FEATURES

› Required features
  – Header independent payload protection providing confidentiality, integrity and replay protection.
  – Context identification independent of transport parameters.

› Desired features
  – Reuse SRTP security functions and transforms.
    › Enables fast and easy implementation
    › Enables reuse of key management protocols
  – Lightweight solution
  – Independent of whether RTP/SRTP is used for transport.
RELEVANT INTERNET-DRAFTS

› SRTP Store-and-Forward Use Cases and Requirements
  – draft-mattsson-srtp-store-and-forward-04

› The Use of the Secure Real-time Transport Protocol (SRTP) in Store-and-Forward Applications
  – draft-naslund-srtp-saf-04

› Co-authors welcome!