Why SRTP isn't the Mandatory security solution for RTP

Colin Perkins / University of Glasgow
Magnus Westerlund / Ericsson

The Issue

- Common to get questions why SRTP is not the mandatory security solution for RTP.

- RTP is a framework and usable for a diverse set of applications and type of deployements:
    - Varying security requirements regarding need for:
        - Confidentiality
        - Integrity
        - Authentication
    - Unicast and Multicast/broadcast applications
    - Different trust in end-points or existing infrastructure
    - Different possible mechanism for transport of key-management

Why this document

- Have a guidance document regarding security with RTP with several purposes:
    - Explain the need for diversity in security solutions due to that RTP is a framework and known diversities
    - High level survey of security mechanisms used for RTP
    - Provide some guidance and recommendations to improve interoperability

Status and Open Issues

- This is the first version, still quite rough
  - Authors will work on improving this in coming versions
- The known open issues are:
  - Discuss how this document relates to BCP 61 (RFC 3365) " Strong Security Requirements for Internet Engineering Task Force Standard Protocols"
  - Expand survey of used key-management mechanism
- Is this something the AVT WG would like to take on as a WG item?