• Draft: Using approximate authentication with Secure Real-time Transport Protocol (SRTP)
• Author: Gabor Feher, Budapest University of Technologies and Economics
• Short abstract: Using approximate authentication in SRTP to provide integrity protection for RTP. Exact payload match is not necessary, but a certain amount of deviation is acceptable.
Motivation

• Error resilient video decoders – bit errors can be tolerated
  – Lots of theoretical publications. Few software releases
• Capturing corrupt frames easily
  – Works for Linux easily, can work for others

• SRTP is strict, does not work on bit errors
  → Weak payload authentication: use approximate authentication for the payload
  – Let the decoder decide what to drop

• Few errors: no attack, tolerable: KEEP
• Many errors: possible attack or quality downgrade: DROP
Corrupt WiFi frames #1
Corrupt WiFi frames #2

- 1000 byte long frames, frame burst, 36 Mbps
Proposed algorithm

- \( E_{k1}(H_{k2}(\text{SRTP header} \oplus \text{ROC}) + AA_{k3}(\text{SRTP payload})) \) using keys \( k1, k2 \) and \( k3 \)

![Diagram showing the proposed algorithm flow]

- Protects against header/sequence number modification
- Protects against bit modification of AA code + reversible
Approximate authentication

• Output should not be secure, the attacker can not modify it (due to the block encryption)
• Even sophisticated modifications on the input should result unpredictable change
• Distance of two inputs -> approximation

• Example algorithm:

010001000... packet

Increasing counter values based on bit value
Counter selection with non-uniform distribution

Difference of two inputs is the sum of counter differences
Plans

• Provide an approximate authentication algorithm as draft (to IETF 80)
  – There is a candidate one, but needs more testing and verification

• Go for RFC

The research leading to these results has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement n° INFSO-ICT-214625.