SRTP Draft v2→ v3 Changes
53rd IETF

David A. McGrew

Cisco Systems, Inc.

mcgrew@cisco.com

Added Optional MKI

- Master Key Identifier – indicates master key used to protect packet
- Useful when frequently re-keying
- Expands packet, but is optional

TMMH Key Size Reduced

- TMMHv2 defined, following earlier work
  - Retains performance and provable security
- 85% of performance with 5% of key size
- Not backwards compatible with TMMHv1

Added Salt to Key Derivation

- Master Salt goes with Master Key
- Provides secure key derivation independent of crypto transforms used
- Protocol complexity and bandwidth are unaffected

AES Counter Mode Tweaked

- Avoids 128 bit modular arithmetic
  - Aligns CM definition with other specs
- Takes advantage of SSRC uniqueness
  - Applications may want to use key management or signaling to ensure SSRC distinctness

Added ‘Scenarios’ Section

- Guidelines how to use SRTP in various unicast and multicast scenarios

Feedback

- Possibly allow both orderings of SRTP/FEC
- Separate document on SRTP key management might be nice
- Exposition improvements