The Secure Real Time Protocol

David McGrew and David Oran, Cisco Systems
{mcgrew,oran}@cisco.com

SRTP Overview

- uses fast, parallelizable stream ciphers (default: AES Counter Mode using Segmented Integer Counter Mode (SICM)),
- uses fast message authentication (default: UMAC draft-krovetz-umac-01.txt),
- uses sequence number based synchronization,
- fits into the RTP framework as a profile.

Security Goals

- enable SRTP applications to avoid security considerations,
- privacy of payload, header extensions, and CSRC list,
- authentication of the header, payload, and header extensions,
- replay protection,
- resistance to DoS attacks.

Other Goals

- low computational cost, footprint, and memory size,
- limited packet expansion,
- preservation of RTP header compression efficacy.

Encryption

Additive stream ciphers (e.g., AES SICM):

- minimize packet expansion,
- fast, (often) paralellizable,
- do not propogate bit errors.

SRTP does not preclude other ciphers

Authentication

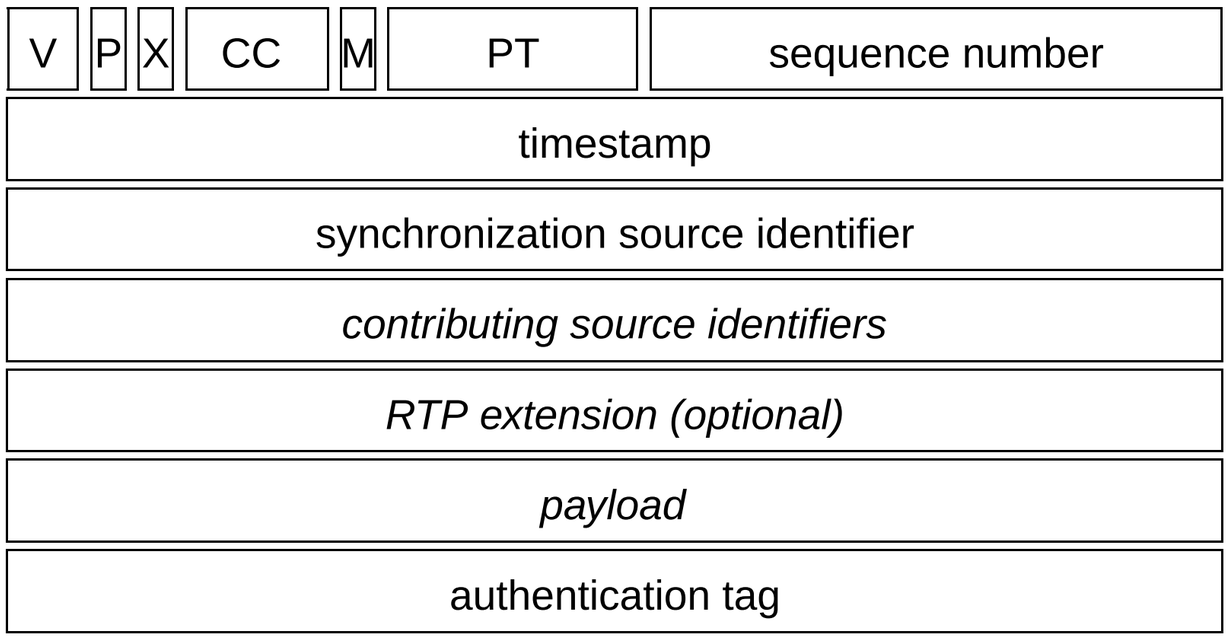
- enables replay protection,
- synchronization allows use of fast, secure universal-hash based MACs (e.g., UMAC, MMH, XORMAC, ...),
- other hash types not precluded.

Default: UMAC with a four-byte tag.

SRTP Cryptographic Context

- encryption key,
- message authentication key,
- 32-bit rollover counter
- sequence number s_l (last received and authenticated sequence number for the receiver, last sequence number sent for the sender), and
- replay list (maintained by the receiver only).

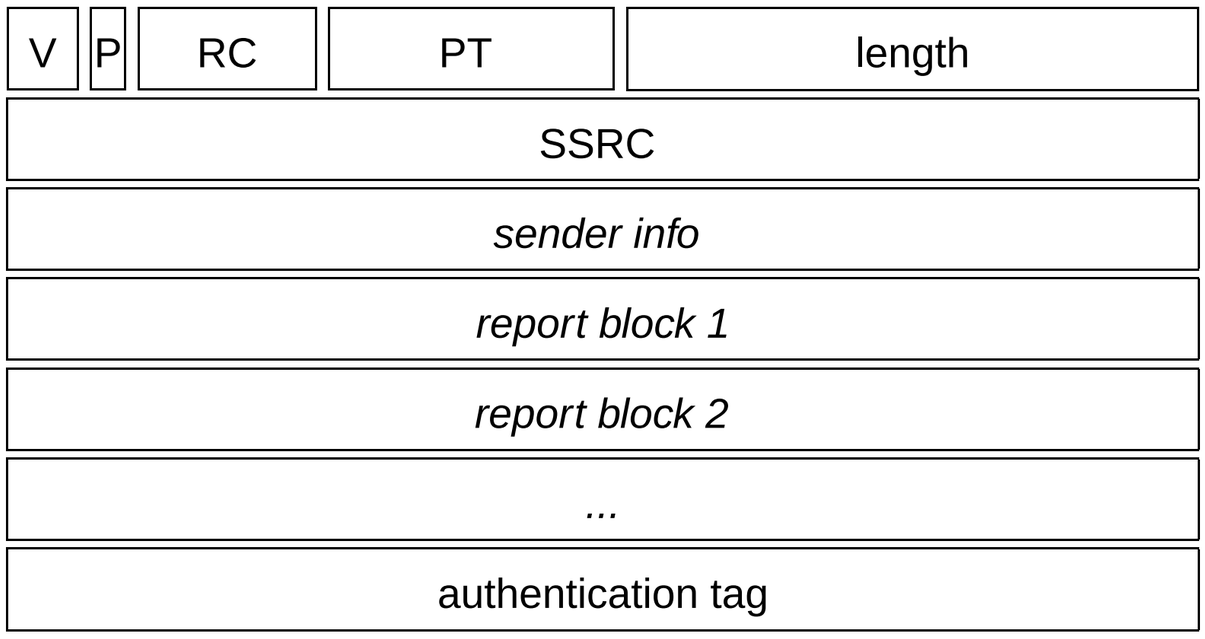
SRTP Packet Format



SRTP Packet Processing

1. Determine which cryptographic context to use by checking the SSRC field.
2. Determine the index of the SRTP packet from the rollover counter and the sequence number.
3. Check the Replay List to ensure that no packet with that index has been received and authenticated before.
4. Compute the authentication tag for the Authenticated Portion of the packet.
5. If the authentication tag that is computed matches that in the SRTP packet, then the packet is accepted and the index is added to the Replay List.
6. Decrypt the Encrypted Portion of the packet.

SRTCP Packet Format



Comparison with RTP Encryption for 3G Networks (`draft-blom-rtp-encrypt-00`)

SRTP has more ambitious security goals, is less wireless-friendly.

- Synchronization via sequence number and rollover counter,
- Cipher: Counter Mode rather than F8,
- Encrypts starting after SSRC, rather than at payload beginning,
- Authentication: UMAC rather than ‘implicit’,
- Replay protection: sequence number rather than ‘implicit’,
- Secure RTCP.

Merging with RTP Encryption for 3G Networks (`draft-blom-rtp-encrypt-00`)

- rollover counter or other explicit synchronization,
- make authentication optional,
- selectable cryptographic algorithms.

Open Questions

- encryption start point (before header extension?).
- keying (SSRC one-to-one with keys?)

F8 (3GPP Cipher)

- half the speed of Counter Mode on small payloads,
- appears secure, but lacks proof,
- should use random IV for full security.

Security improvements in the use of F8:

- replace `IV = port_number || SSRC || SEQ` with `IV = port_number || SEQ || TS`,
- better, use a random IV (`www.mindspring.com/ dmcgrew/dam.htm`).