TLS/DTLS AES-CTR

`draft-ietf-tls-ctr-01`

Nagendra Modadugu

Eric Rescorla

AES-CTR Overview

- Works like a stream cipher, e.g. RC4
  - XOR keystream with plain text:

    `CT[i] := PT[i] ⊕ AES(CTR(i))`

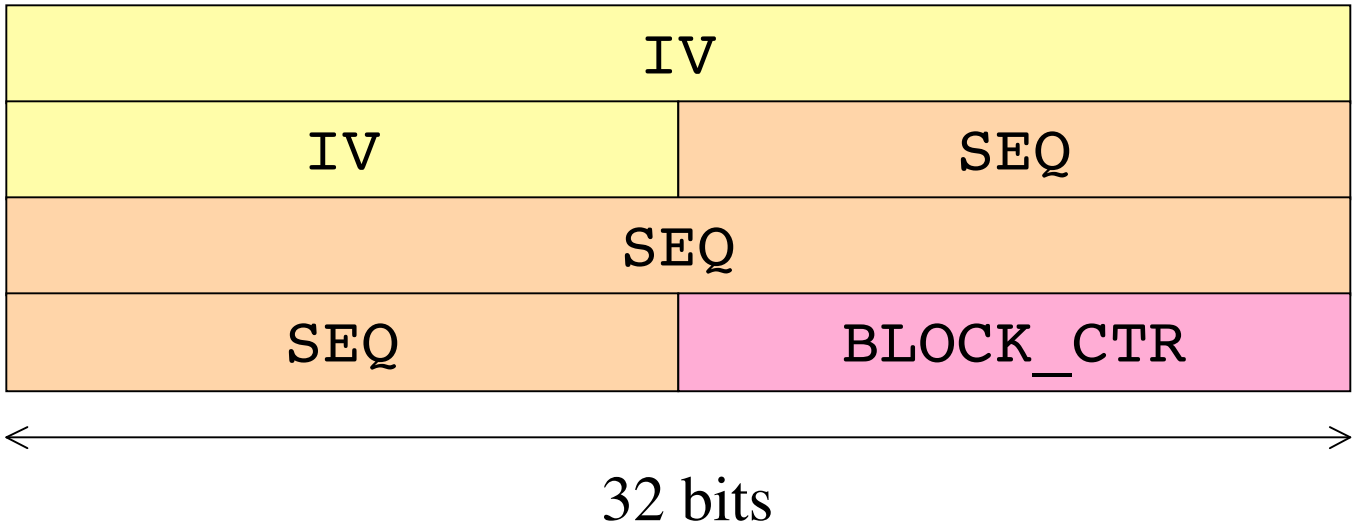
  - Increment `Counter`

- `Counter` encrypted to generate keystream
  - `Counter` MUST never be re-used (with same key)
- No harm if `Counter` is public
  - But MUST be initially unpredictable

Motivation

- Low bandwidth
  - Save between 17-32 bytes compared to CBC
- Random access (for DTLS)
- Parallelizable/pipelining
- Implement both block/stream ciphers with AES

Counter Design



- `IV := {client_write_IV, server_write_IV}`
- `SEQ := {seq_num}` (64-bits)
- `BLOCK_CTR := 1` (16-bits)

Changes since -00

- Incorporate comments
  - Clarify endien ordering of Block Counter
  - Expand description on max. record size
  - Clean up overview description

Questions?