TCP-AO Test Vectors

draft-touch-tcpm-ao-test-vectors-00

IETF 108 - Online

Joe Touch, consultant

Juhamatti Kuusisaari, Infinera Corp.

Rationale

- Provide test vectors to validate implementation
  - All four derived traffic keys
  - Both current required algorithm sets (key derivation, MAC)
  - Both including and excluding TCP options
  - Currently includes IPv4
  - Covers TCP ports

- For all entries, indicates:
  - Derived traffic key
  - Test TCP header
  - MAC for verification

- Pending additions
  - IPv6
  - NAT-traversal variant

Other issues

- Discusses known implementation issues
  - Algorithm
  - Parameter
  - String handling
  - Header coverage

- Based on updated sequence number extension (SNE) computation
  - Details in a separate draft (to be submitted)
  - Intended for future consideration as WG BCP

Ways forward

- Intended as informational

- Requesting WG adoption