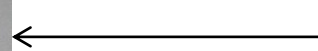


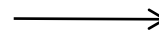
TCP-AO Test Vectors

draft-ietf-tcpm-ao-test-vectors-02
IETF 112 - Online



Joe Touch, consultant

Juhamatti Kuusisaari, Infinera



Rationale

- Provide test vectors to validate TCP AO implementation
 - All four derived traffic keys
 - Both current required algorithm sets (key derivation, message authentication code (MAC))
 - Both including and excluding TCP options
 - Includes IPv4 and IPv6
- For all entries, indicates:
 - Derived traffic key
 - Test TCP/IP header
 - MAC for verification
- Discusses known implementation issues
 - Algorithm
 - Parameter
 - String handling
 - Header coverage
- *Initial draft-touch-tcpm-ao-test-vectors-00 was introduced in IETF 108*

New draft changes since IETF 110

- draft-ietf-tcpm-ao-test-vectors-00
 - Improved introduction, the definitions of IP fields and options
- draft-ietf-tcpm-ao-test-vectors-01
 - Updated the expire date
- draft-ietf-tcpm-ao-test-vectors-02 (the latest)
 - Review comment changes:
 - Clarified introduction regarding interoperability to refer to implementations
 - Changed “NAT traversal” to “middlebox traversal”
 - Clarified parameters (whether decimal or hexadecimal)

Ways forward

- Thanks for the feedback so far!
 - More feedback is always welcome
- We think the draft is ready for WGLC