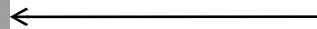


TCP-AO Test Vectors

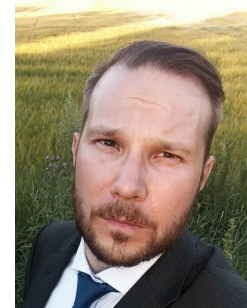
draft-touch-tcpm-ao-test-vectors-02

IETF 110 - 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
 - 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 presented in IETF 108*

New draft changes

- draft-touch-tcpm-ao-test-vectors-01
 - While testing an issue was found in the KDF setup
 - Updated draft -01 accordingly with additional guidance
 - Interoperability with two vendors achieved
 - Full interop with a routing vendor
 - Later HMAC-SHA1 interoperability with a fuzzing vendor
 - draft was an input for them to reach interoperability
 - (they do not yet support AES128-CMAC)
- draft-touch-tcpm-ao-test-vectors-02
 - Included IPv6 test vectors
 - Minimal implementation changes compared to IPv4
 - Only pseudo-header handling is different
 - Not expecting issues - feedback is welcome

Ways forward

- Intended as informational
- Authors consider it ready for WG adoption
 - Interoperability confirmed, IPv4 and IPv6 test vectors available
- We would like to request WG adoption