



TCP Authentication Option

Joe Touch, USC/ISI

Allison Mankin, NSF

Ron Bonica, Juniper Networks



Auth Design Team

← Input

- ← Multiple candidate TCP MD5 update IDs
- ← Bellovin's requirements document

← Output

- ← Current TCPM ID
- ← Update to Bellovin's requirements doc
 - ← Became a focus of DT discussions
 - ← Summary inside current TCPM ID

Key DT Decisions - I

← Header requirements:

- ← New TCP option type
- ← No alg ID in the clear
- ← KeyID field for hitless intra-connection rollover

← Support use through NATs

- ← RFC-3947 style tunnels
- ← Optional coverage of TCP options

← Specify size of per-conn TSAD entries

- ← 2..256 keys/parameters

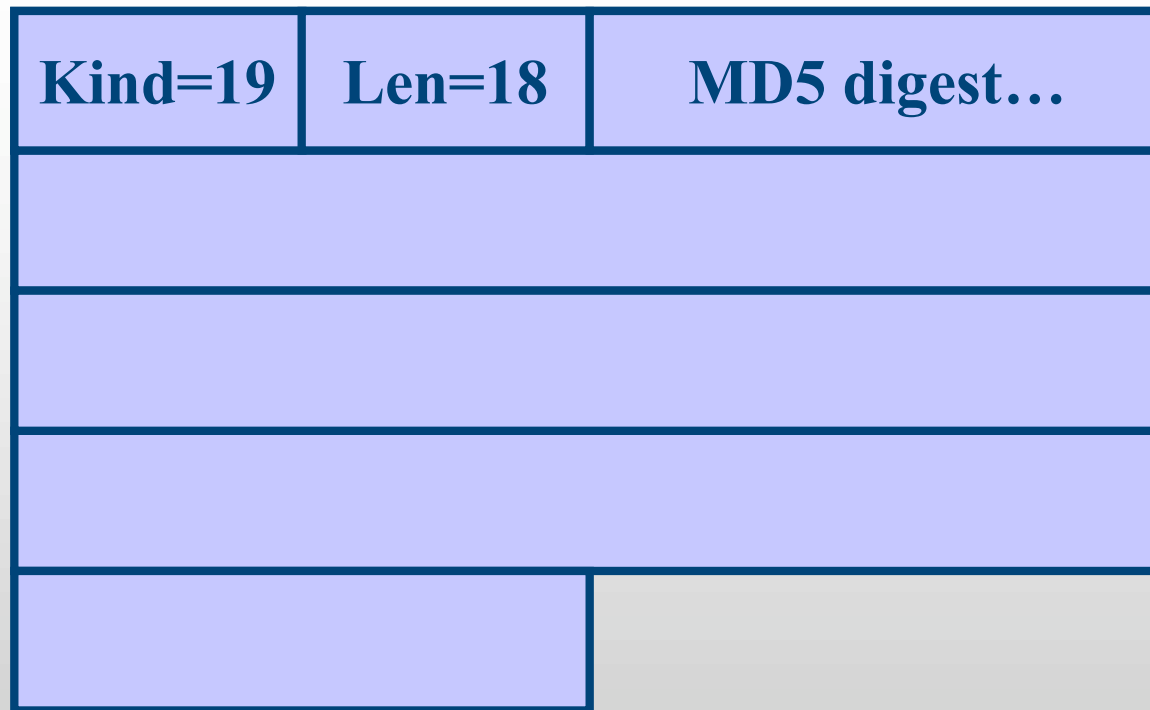
Key DT Decisions - II

- ← Allow the WG/SecArea to specify alg
 - ← Replace fixed algs with placeholders
- ← Process pre-TCP
 - ← Explored pre-authentication validation, but TCP often requires action for invalid segments
- ← Allow *any* external key mgt sol'n, incl. manual
 - ← Define a keying interface
- ← No upgrade support TCP MD5->TCP-AO
 - ← No support for TCP MD5 key rollover either
 - ← TSAD should support use for TCP MD5 info. (complementing RFC4808)

Overall Decision

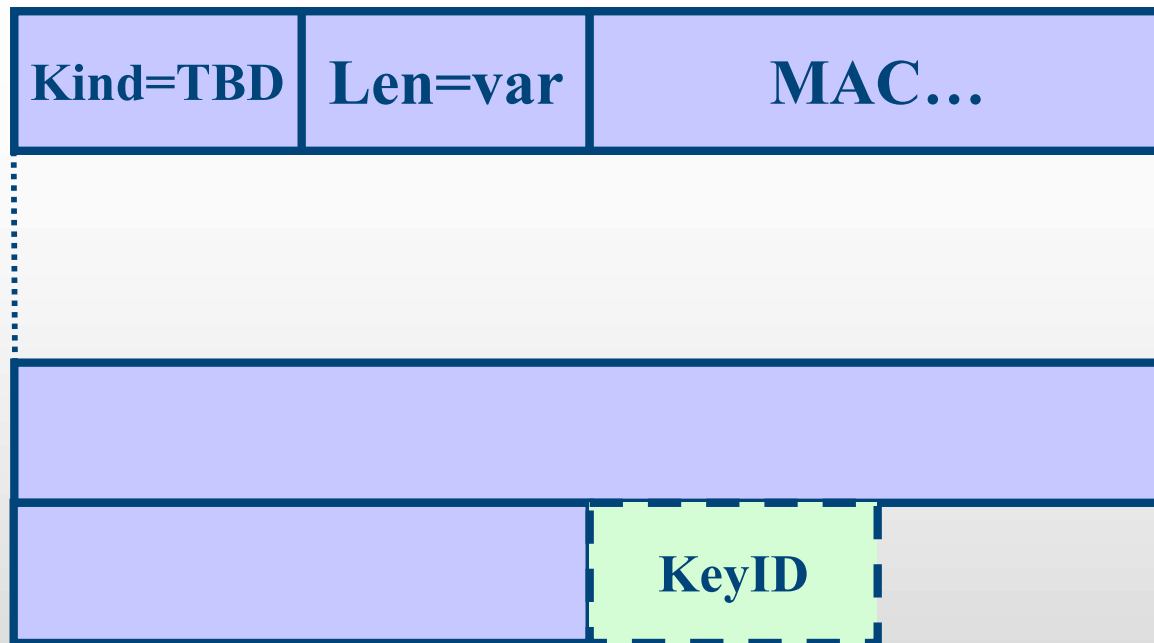
- ← Extend draft-touch-tcp-simple-auth
 - ← Update with key DT decisions
 - ← Expand to address Bellovin++ issues
 - ← Expand TSAD API
- ← Recognize contributions
 - ← Add Bonica as coauthor
- ← Issued as *draft-ietf-tcpm-tcp-auth-opt*

TCP MD5



← 128-bit MD5 digest; 18 byte total length

TCP-AO



- ← New Kind value (TBD)
- ← Supports optional KeyID
 - ← Use is determined by Len LSB (O/E)

Things the DT left out

- ← In-band key negotiation
 - ← Limited TCP 3WHS space prohibits sol'n
- ← Replay protection
 - ← Intra-session, TCP seqno avoids
 - ← Inter-session, key non-reuse avoids
- ← Key synchronization, key efficiency
 - ← Use KeyID

Way forward

- ← Work on draft-ietf-tcpm-tcp-auth-opt-00
 - ← Feedback on current version
 - ← Input on open questions (sec 1.3)
 - ← Ignore for now...
 - ← TOC mismatch
 - ← Numerous typos
- ← Join discussion in SAAG on TCP-AO-KM
 - ← Key management protocol issues