TCP AO

Joe Touch, USC/ISI
Allison Mankin, JHU
Ron Bonica, Juniper
& TCP Auth. Design Team

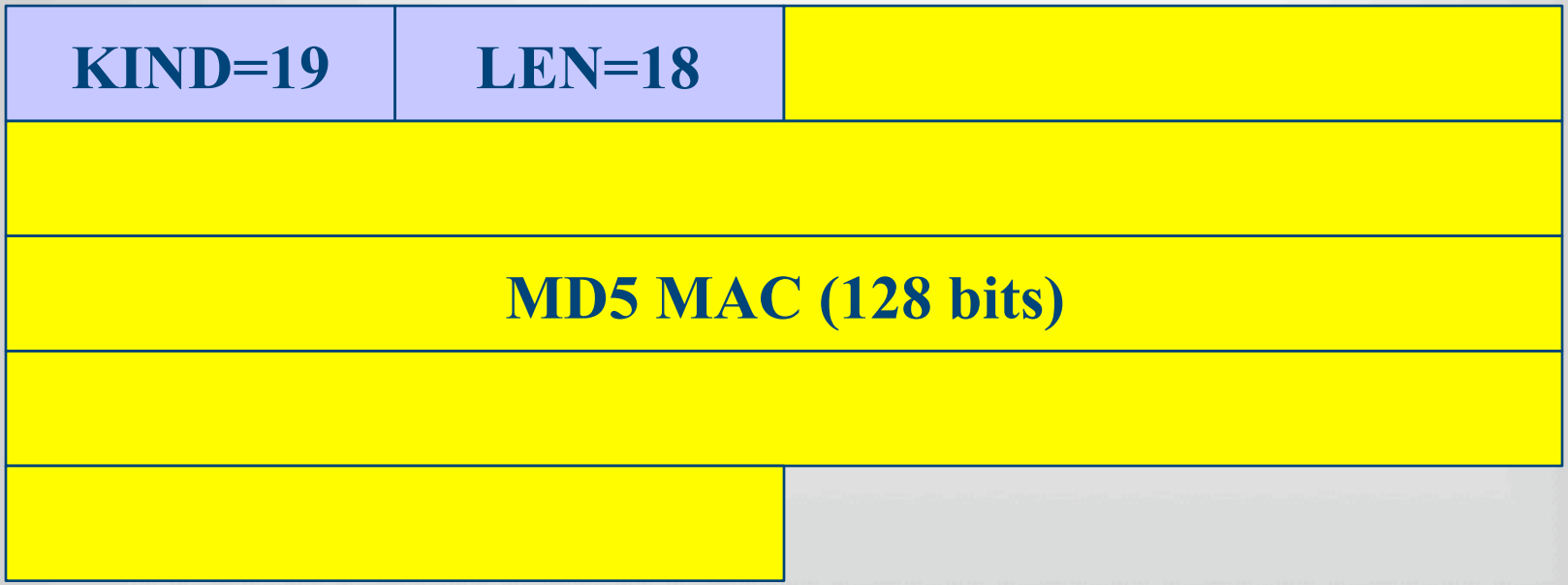
USC Viterbi
School of Engineering

Outline

- Issues with TCP MD5
- Replacement Goals
- TCP-AO
- Status

TCP MD5 (RFC2385)

- Header just stores MAC:



- Not much else specified

Issues with TCP MD5

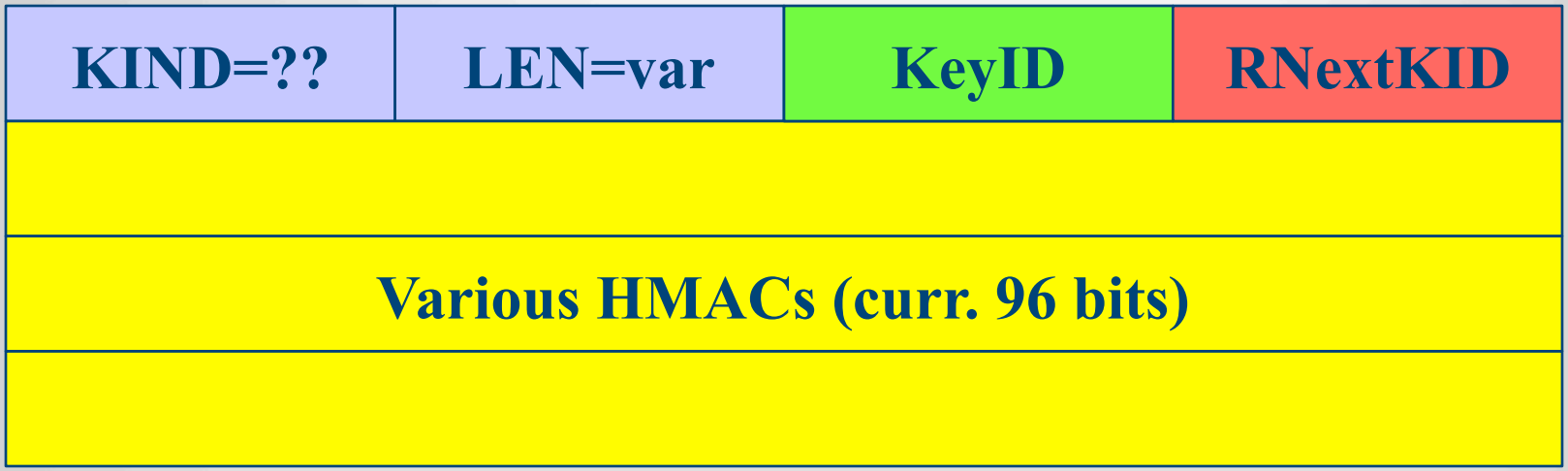
- MD5 weakness as a MAC
- Algorithm rigidity
- Does not specify intra-conn. rekeying
  - Doesn't prohibit, but loses packets/window
- No replay protection
- Does not require per-conn. keys
- Underspecified w.r.t TCP

Replacement Goals

- Algorithm agile
- Allows rekeying
  - Without loss or window impact
  - Without requiring multiple tries (DOS issue)
- Replay protection
- Per-connection keys
- Supports manual and auto. keying
  - KMI agnostic
- ***OBSOLETES TCP MD5***

TCP-AO

- Header includes KeyIDs:



- KeyID = current key for this HMAC
- RNextKeyID = "ready" to receive key ID

TCP-AO Features

- Loss-free rekeying – KeyID
- Loss-free sync. use of new key – RNextKID
- Per-connection keys
  - Master key + ISNs -> conn. Key
- Replay protection
  - Via sequence number extensions
- Master key tuple (MKT) includes parameters
  - Conn. key alg., HMAC alg., TCP option incl. flag
- Fully specified w.r.t. TCP states/events

TCP-AO Summary

Algorithm agile	MKT indicates alg. Algs. specified separately.
Allows rekeying, esp. efficiently	KeyID for current segment MKT. RNextID for return path sync.
Replay protection	Ext. sequence numbers maintained, used in HMAC.
Per-connection keys	Derived keys using KDF.
Man/auto KMI agnostic	MKT treated as external. Parameter changes require MKT changes.

TCP-AO Future Plans

- NAT support
  - Currently a separate I-D
- Key management protocol
  - No current plans

Current Status

- In TCPM last call:
  - draft-ietf-tcpm-tcp-auth-opt – *Touch/Mankin/Bonica*
    - Explains probs. with TCP MD5, IPsec
    - Describes AO
  - draft-ietf-tcpm-tcp-ao-crypto – *Lebovitz/Rescorla*
    - Describes HMAC and KDF algs.
- In TCPM for discussion:
  - draft-touch-tcp-ao-nat – *Touch*
    - Describes NAT-compatible configuration
    - Requires MKT add a flag that modifies HMAC calc.