TCP Auth Option Status

Joe Touch, USC/ISI

Allison Mankin, NSF

Ron Bonica, Juniper

SAAG Issues

- Applicability questions
  - Usage
  - Assumptions
  - Protections expected
- Determine
  - Algorithms
  - Key length

any?

- ←MAY for any
- ←SHOULD for connections whose semantics is adversely affected by transport attacks, e.g., BGP

AS: TCP assumptions

- ←No assumptions about connection properties other than TCP
- ←No TCP segment assumptions
  - ←No need for separate replay protection
  - ←TCP already protects against trusted replays
  - ←Networks can already replay TCP segments from legitimate users

AS: Overall perspective

- TCP-AO *authenticates* TCP segments
  - A given sender can still do whatever it does today
- TCP-AO does not *harden* TCP
  - TCP-AO tracks only whether a connection is open or not (association semantics), it does not further track TCP state (transport semantics)

SAAG IPsec-related Q's

- ←Why isn't IPsec the solution?
  - ←(review existing answer)
- ←Why not two dbases (SAD/SPD)?
  - ←TCP-AO sees only SAD; SPD is external
- ←Why not use IKE for key mgt?
  - ←SAAG can decide, but we hope to allow any key mgt solution, including one that is simpler than IKE

SAAG other Q's

- ←Auto key mgt is a MUST
  - ←Disagree; auto may be MUST for BGP, but not in general for TCP
- ←In-band key management is desirable
  - ←Disagree; this is off the table, as per the D-T

SAAG other Q's…

- Can connection keys be reused?
  - Per-connection only (no wildcards in TCP-AO)
  - MUST NOT be reused on a connection, or across connections within an IP address
    - What enforces this? TCP-AO, or the key manager?
- Any questions for SAAG on algs/lens?
  - E.g., for non-manditory algs

TCPM Q's (review)

- Should this obsolete MD5?
  - As per IKEv2, yes; that won't remove legacy code, though
  - MUST NOT use MD5 and AO on same connection
  - MAY use MD5 and AO on the same system to support legacy use
- One doc or two?
  - One doc unless there is a stall?

Eric R's Q's

- ←Is asymmetric auth useful?
- ←Key reuse (see SAAG Q's)
- ←TSAD concerns
  - ←IMO, needed detail for an API to key mgt
- ←Key-ID (see I-D Q's)
- ←Key mgt issues (to be discussed in SAAG)
- ←Handling unkeyed conns
  - ←Currently silent accept, equiv to no TCP-AO

Eric R's Q's...

- ←Number of bytes keyed?
  - ←Vs. number of segments?
- ←Requirements correctness
- ←Some issues the DT (and WG) discarded:
  - ←In-band keying
  - ←Partially authenticated streams (change from non-auth to auth based on data offset)

Current pending mods:

- Change “session” to “connection”
  - To be done.
- What if TCP-MD5 and TCP-AO in same segment?
  - TCP-AO authenticates before TCP processes, i.e., this is a misconfigured host, so RST
- Clarify default MAC selection?
  - Process for selecting alternate required MAC
- Need for a MAC registry?
  - Currently reuses IKEv2 Transform Type 3 ID