RFC6824bis
draft-ietf-mptcp-rfc6824bis-00

Alan Ford

alan.ford@gmail.com

Rationale

- Consensus to move to Standards Track
  - Security
  - Feedback from implementation experience

Security Issues

- Thanks to Marcelo for the study
- Off-path ADD_ADDR hijack attack
  - Medium risk, needs to be addressed
- DoS attacks
  - Can be mitigated outside of protocol
- Eavesdropper of initial handshake
  - Accepted out of scope

ADD_ADDR hijack

- Solution: ADD_ADDR2!
- We now add a HMAC of the new (addr, port) keyed against the sender's connection key
  - As secure as MP_JOIN
- Impact:
  - Addresses cannot be changed en route
  - Note that now no middleboxes can add addresses unless they have seen the initial handshake

ADD_ADDR2

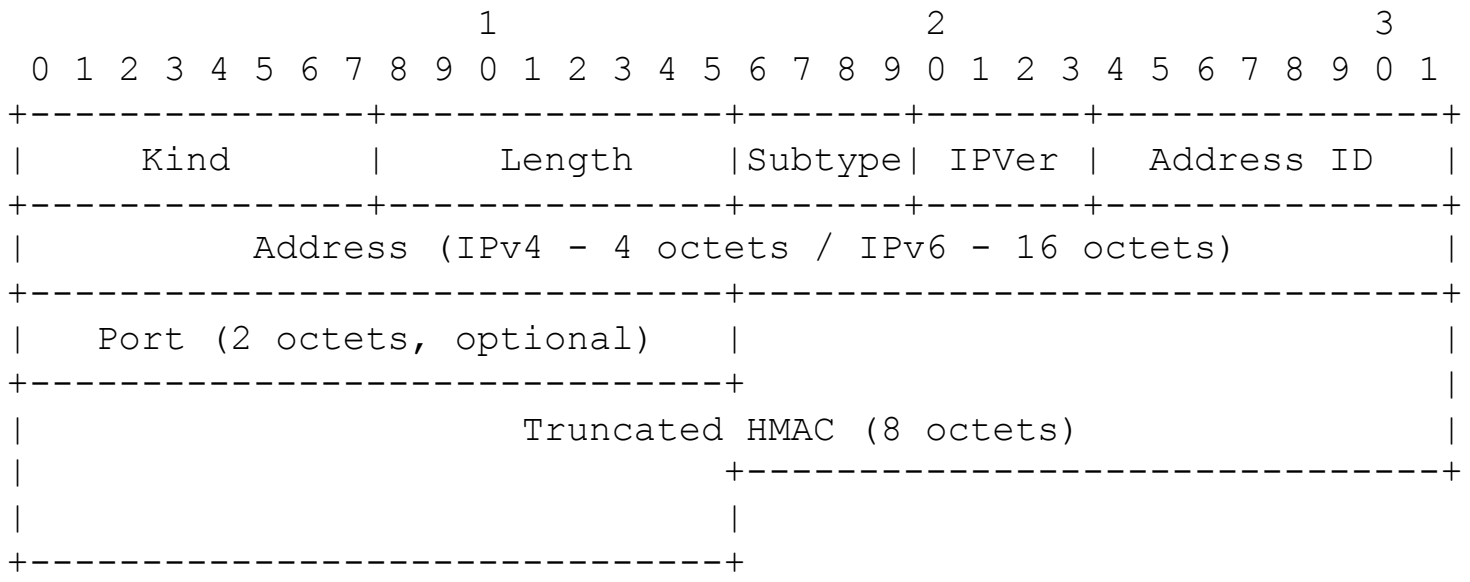

Figure 12: Add Address (ADD_ADDR2) Option

Other updates

- A number of textual clarifications
  - E.g. purpose of IDSN generation
- Notably fallback
  - Note: fallback can be unidirectional but unlikely to be implemented as such
- Plus the errata

Next Steps…