MPTCP – Multipath TCP

WG Meeting

Berlin, IETF-87, 30th July 2013

Philip Eardley

Yoshifumi Nishida

- Note taker
- Jabber [IMPORTANT]
- Please include “-mptcp-” in your draft names
- Please say your name at the mike

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- **the IETF plenary session,**
- **any IETF working group or portion thereof,**
- **the IESG, or any member thereof on behalf of the IESG,**
- **the IAB or any member thereof on behalf of the IAB,**
- **any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices,**
- **the RFC Editor or the Internet-Drafts function**

All IETF Contributions are subject to the rules of RFC 3978 (updated by RFC 4748) and RFC 3979 (updated by RFC 4879).Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 3978 (and RFC 4748) for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Milestones

- Dec 2012: Consensus on what high-level changes are needed to the current MPTCP Experimental document in order to progress it on the standards track
- Apr 2013: Implementation advice (Informational) to IESG
- Aug 2013: Use-cases and operational experiences (Informational) to IESG
- Dec 2013: MPTCP-enabled middleboxes (Informational) to IESG
- Dec 2013: MPTCP standards track protocol to IESG

- We're behind, but progressing (except for the middlebox one?)
- We (probably) have achieved the first one.

Agenda

1. Chairs update (Chairs, 15 mins)
2. Discussions for MPTCP Future Security (90 mins)
3. RFC6824bis (15 mins) Alan Ford

If time permits:

1. MPTCP path selection using Port Control Protocol (PCP) (15 mins) Dan Wing
2. Evolving the Internet with Connection Acrobatics (10 mins) Marcelo Bagnulo

November 6, Wednesday, Afternoon Session II 15:50-16:50 Room Name: Regency

1. Wrap-up for security and 6824bis discussion (30 mins)
2. MPTCP path selection using Port Control Protocol (PCP) (15 mins) Dan Wing
3. Evolving the Internet with Connection Acrobatics (10 mins) Marcelo Bagnulo
4. Apple Update Stuart Cheshire
5. FreeBSD implementation status update (to be confirmed)

News

- MPTCP is in iOS8 (used for Siri)
- Linux Kernel MPTCP stable release - v0.88
- Soon: new release of FreeBSD mptcp
- New version of draft-khalili-mptcp-congestion-control
- Tsvarea: TCPcrypt, part of 'Evolution of IETF Transport Protocols' discussion (+ tcpcrypt & mptcp lunch)
- Multipath Networks – commercial home router with mptcp to bond access links
- Interim meeting on security (audio)

Summary of interim

- Prong 1
  - small fixes to RFC6824 to get security exactly same as SCTP with dynamic addresses & very similar to TCP security. We believe should be sufficient to get on Standards track
  - fix the ADD-ADDR attack (with HMAC – same method as for JOIN);
  - define now how to signal upgraded security
- Prong 2
  - more secure
  - 2 choices are to secure signalling better (as RFC6824 has keys in the clear on the MP_CAPABLE exchange) – or to secure data as well
  - tentative conclusion is to go for second choice (just securing signalling doesn't help because need to be compatible with NATs – and NATs change the source address therefore attacker can do same thing)
  - tend to favour TCPcrypt (vs ssl) as secures more of the traffic

Consensus calls

- We proceed with defining better MPTCP security as per interim meeting
- Make draft-bagnulo-mptcp-attacks wg doc

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

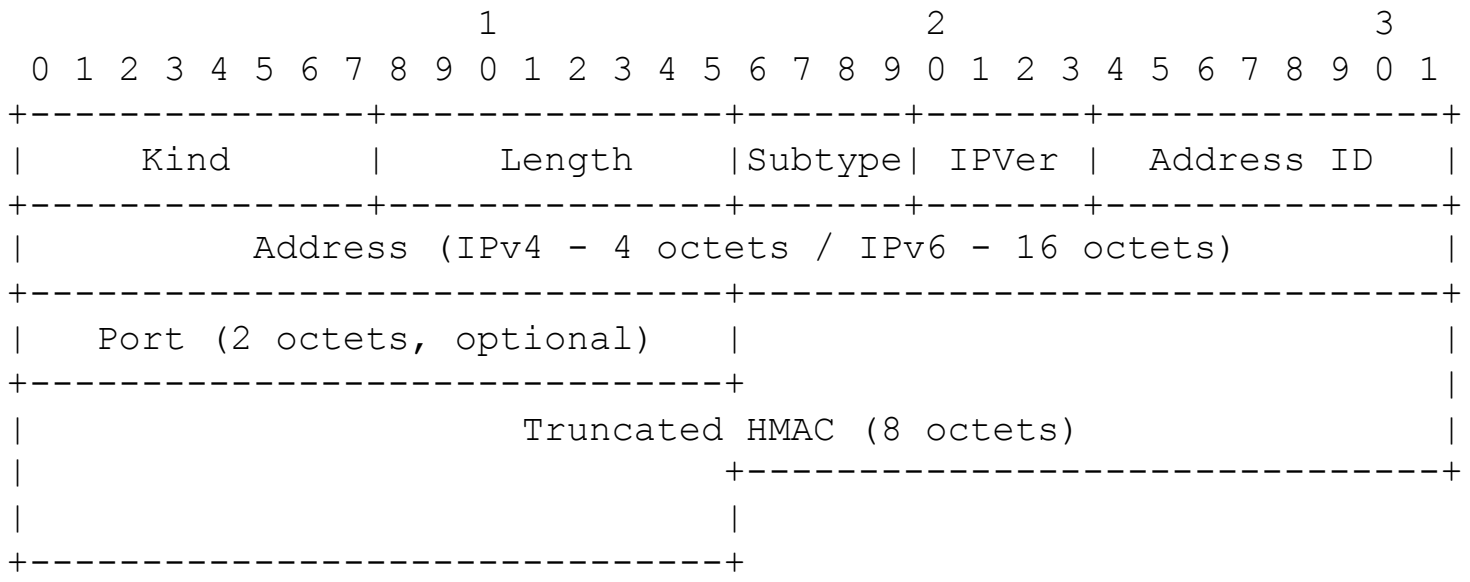

Figure 12: Add Address (ADD_ADDR2) Option

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…