

MPTCP – Multipath TCP

WG Meeting

18th July & 21st 2017

Prague, Czech Republic

Philip Eardley

Yoshifumi Nishida

- Note taker
- Jabber
- Please say your name at the mike
- Please include “-mptcp-” in your draft names
- Blue Sheet!

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
 - The IESG, or any member thereof on behalf of the IESG
 - Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
 - Any IETF working group or portion thereof
 - Any Birds of a Feather (BOF) session
 - The IAB or any member thereof on behalf of the IAB
 - The RFC Editor or the Internet-Drafts function
- All IETF Contributions are subject to the rules of [RFC 5378](#) and [RFC 8179](#).
- 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 5378](#) and [RFC 8179](#) 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.

IETF-99 Agenda

-- Tuesday (1550-1750 Athens/Barcelona) --

0. Chairs – WG Status etc [5 mins]

1. Implementation updates

1.1 Christoph Paasch - iOS and Linux implementation update [10mins]

1.2 Fabien Duchene - updates on the implementation and some results [15mins]

1.2 Other updates - open call

1.3 Hackathon news - Olivier Bonaventure [10mins]

2. RFC6824bis

2.1 Update - Alan Ford [10mins]

2.2 Progressing to WGLC, SecArea review etc – Chairs [10mins]

3. Proxies

3.1 Olivier Bonaventure - MPTCP converters [20mins + 20mins discussion]

3.2 Vladimir Olteanu - SOCKS Protocol Version 6 [20mins]

-- Friday (1150-1320 Congress Hall I) --

4. Markus Amend - "A proposal for MPTCP Robust session Establishment (MPTCP RobE)" [20mins]

5. Quentin De Coninck - "Proposal for Fast Subflow Creation" [20mins]

6. Wrap up – next steps, interim? ... [10 mins]

WG status (1) - Completing the bis

- From charter:
 - The working group now re-charters to progress various aspects of MPTCP. The **primary** goal of the working group is to create a **bis** version of the protocol document on the **Standards** track.
 - This develops the current Experimental document (item d above), incorporating experience from (for example) implementations, interoperability events, experiments, usage scenarios, protocol corner cases, and feedback from TCPM. There already exists a reference Linux implementation and other implementation and experimental activity is on-going and will continue during 2012, with the objective of progressing the protocol to Standards Track during **2013**.
- Need to complete agreement on items raised by Alan & WG
- Need to have implementation  before standards track – possible ways forward:-
 - Wait for implementation *at ietf-98 we decided to go for this choice*
 - Remove stuff not implemented
 - Go for EXPT instead of STDS
 - Some other option?

WG Status (2) - MPTCP Proxy activity

- At IETF-98 we discussed:
- Assumptions & criteria –
 - Agreed that minimising set-up time is a key criteria
- 3 high-level solution approaches
 - Most people favoured one of these
 - However, didn't find an approach that “everyone can live with”
 - More work needed
- Update to Charter not needed in order to continue discussions
- BANANA WG-forming BoF at IETF-99
 - BANdwidth Aggregation for Network Access
 - Determine how Local and Remote BANANA Boxes find each other.
 - Specify a signalling protocol that can be used to send configuration and control information between BANANA boxes, including: <various stuff>
 - Work with other IETF WGs <MPTCP> to ensure that the discovery mechanism and signalling protocol will meet their needs

IETF-99 Agenda

-- Tuesday (1550-1750 Athens/Barcelona) --

-- Friday (1150-1320 Congress Hall I) --

0. Chairs – WG Status etc [5 mins]

3.3 Follow-up discussions from Tuesday's proxy discussions [15mins]

4. A security attack (Zhiyun Qian /Chairs) [15 mins]

5. A proposal for MPTCP Robust session Establishment (MPTCP RobE)

Markus Amend - "A proposal for MPTCP Robust session Establishment (MPTCP RobE)" [15mins]

6. Proposal for a new Multipath TCP option

Quentin De Coninck - "Every Millisecond Counts: Tuning Multipath TCP for Interactive Applications on Smartphones" [15mins]

7. Better documenting interactions between MPTCP and TFO - Christoph [10mins]

8. Using MPTCP on IPv6 only hosts in networks with NAT64 - Quentin [10mins]

9. Plans for progressing MPTCP, Wrap up – next steps, interim? ... [10 mins]

MP-PRIO attack

- security flaw in the MP_PRIO message that allows a man-in-the-middle attacker on a single path to divert all traffic to its own path, effectively hijacking the entire MPTCP connection.
- a host can request a change in the sub-connection priority by sending MPTCP MP_PRIO option to the other host with the corresponding address identifier. The key property of MP_PRIO messages is that they can be sent on any sub-connection (in case the first sub-connection is already congested)
- MP_PRIO option has no authentication required by the specification whatsoever, allowing an attacker controlling only one path to set any sub-connection as backup and launch traffic divergence and connection hijack attacks.
- Effectively, this attack degrades an MPTCP connection to a regular TCP connection as all traffic will be routed through the attacker-controlled path. We argue that this vulnerability makes MPTCP less secure than TCP, because the entire MPTCP connection can be compromised (fully controlled by an attacker) as long as any one of the communication paths is compromised
- Possible solution: remove address identifier from the MP_PRIO option
- See upcoming ICNP paper
- Zhiyun Qian zhiyunq@cs.ucr.edu; Zubair <zubair-shafiq@uiowa.edu>; Franck Le <fle@us.ibm.com>; Alex Liu <alexliu@cse.msu.edu>; Ali Munir <munirali@msu.edu>

Next steps

- Progress rfc6824bis
- Proxy work
- Interim?