MPTCP threats

MPTCP WG

IETF78 - Maastricht

Modifications

- Added text for reccomendation as agreed in last meeting

  After evaluating the different aspects in the MPTCP WG, our conclusion is that the default security mechanisms for MPTCP should be to exchange a key in the establishment of the first subflow and then secure following address additions by using a keyed HMAC using the exchanged key

Modifications

- Added reccomendation for multiple security mechanisms:

  our recommendation is that the MPTCP protocol should be extensible and it should able to accommodate multiple security solutions, in order to enable the usage of more secure mechanisms if needed.

Question

- Should we make an analysis on how to support multiple security solutions and how they interact?
  - See Erik's mail for relevant questions

What’s next?

- Please read and comment the draft
- We need reviews to move forward.