Changes in -05

• Bump version number v1
  – We don't need to worry about ADD_ADDR(2)
  – This means we can now change the handshake!
  – So we did…
  – Inspired by draft-paasch-mptcp-syncookies we now have a new handshake, to assist stateless webservers
  – MP_CAPABLE now has some additional DSS features…
New Handshake

- **SYN (A->B):** only the first four octets (Length = 4).
- **SYN/ACK (B->A):** B's Key for this connection (Length = 12).
- **ACK (no data) (A->B):** A's Key followed by B's Key (Length = 20).
- **ACK (with first data) (A->B):** A's Key followed by B's Key followed by Data-Level Length, and optional Checksum (Length = 22 or 24).
Why this helps

- The ACK carries both A's key and B's key. This is the first time that A's key is seen on the wire, although it is expected that A will have generated a key locally before the initial SYN.
- The echoing of B's key allows B to operate statelessly, if it is generated in a verifiable way.
- Therefore, A's key must be delivered reliably to B, and in order to do this, the transmission of this packet must be made reliable.

- If B has data to send first, then the reliable delivery of the ACK can be inferred by the receipt of this data with an appropriate MPTCP Data Sequence Signal (DSS) option.
- If, however, A wishes to send data first, it would not know whether the ACK has successfully been received, and thus whether the MPTCP is successfully established. Therefore, on the first data A has to send (if it has not received any data from B), it MUST also include a MP_CAPABLE option, with additional data parameters.
Other changes

- Clarifications on requirements for 64-bit and 32-bit sequence numbers
- Clarifications on HMAC generation
- Formalising the experimental option, from draft-bonaventure-mptcp-exp-option
Outstanding issues

• MPTCP and (front-end) proxies

• Anything else?