Privacy threats and possible countermeasures for MPTCP
draft-bagnulo-mptcp-privacy-00.txt

M. Bagnulo, A. Andersdotter, C. Paasch

IETF 105

Scope

- Analysis of the threats against privacy introduced by the use of MPTCP **compared to using regular TCP**
  - Incremental privacy threats w.r.t. TCP
- Privacy threats affecting TCP and MPTCP are out of the scope of the analysis
  - e.g. threats resulting from sending data on the clear are out of scope

Main privacy threats

- MPTCP operation binds multiple addresses in a single MPTCP connection
- Movement tracking
- More accurate positioning: the location of a device that exposes multiple addresses can be more accurately determined
  - A wifi access may be more accurate than a cellular network access
- Type of attackers
  - Partially on path
  - Fully on path

Detailed attacks mechanics

- MP_CAPABLE + MP_JOIN
  - An attacker capable of observing the token that identifies the MPTCP connection in the different packets carrying it in the MP_CAPABLE and MP-JOIN can bind the multiple addresses
- ADD_ADDR
  - An attacker observing the ADD_ADDR option can bind the addresses in the option and the source IP address of the packet.

Countermeasures

- ADD_ADDR based attack
  - Encrypt the address with the MPTCP connection key (included in the MP_CAPABLE)
- MP_CAPABLE and MP_JOIN based attack
  - Change the token in every new MP_JOIN message
  - The problem is that the token is used as a key to identify the MPTCP connection the JOIN refers to.
  - Using a token generation mechanisms that is reproducible at the receiver could work, e.g. the hash of the key and the new source address
    - Extra cost at the receiver to process incoming JOIN messages

Next steps

- Is this interesting/relevant to document?