Binding Update Backhauling (BUB)

draft-haddad-mipv6-bub-01

Wassim Haddad
Lila Madour
Suresh Krishnan
Alan Kavanagh
Ericsson Research Canada

Francis Dupont
ENST Bretagne

S. Daniel Park
Samsung

Hannu Kari
HUT

IETF59

Why BUB…?

- When two endpoints are mobile and the RO mode is used:

- *Vulnerability on both sides*…

- *Amount of signaling messages is excessive, i.e., any loss severely affects the latency*.

- BUB is a new mode, which deals with scenarios involving two mobile endpoints using the RO mode.
- BUB improves the security of the BU messages and substantially reduces the amount of signaling messages, i.e., the latency. BUB is immune to the double jumping problem.

Main Features

- New message (BUBC) to complete the BUB test.
  In order to read the “entire” shared secret (i.e., Kbm + cookie), the BUB test requires the malicious node ***to be simultaneously:***
  - on the new direct path between the two MNs
  - between the two HAs
  - between the MN and the other HA
- The CoTI/CoT and HoTI/HoT messages are eliminated.
- The BU message MAY be duplicated (i.e., one BU goes via the two HAs and another one on the new direct path).

Main Changes from Previous Version

- Duplication of the 2nd DH message. The DH messages are sent on all available paths.
- The alternate care-of address option MUST NOT contain a care-of address different than the real one. More information in: draft-dupont-mipv6-3bombing-00.
- The Nonce Index Option MUST NOT be used.
- The BA message is sent on the direct path.

Next...?

- Comments are welcome!
- WG item?
- .....
- **Thank you!**