Optimizing Mobile IPv6 (OMIPv6)

draft-haddad-mipv6-omipv6-01

Wassim Haddad
Suresh Krishnan
Lila Madour
Ericsson Research Canada

Francis Dupont
ENST de Bretagne

Soohong Daniel Park
Samsung

IETF59

Why an Optimization is needed?

- When the RO mode is used between one mobile and one static endpoints:
- Critical Signaling Messages are not protected.
- Critical Signaling Messages are exchanged at high frequency.
- If one signaling message is lost, the latency is severely affected.
- MIPv6 is not suitable for time sensitive applications.
- In few words, the session is vulnerable from the beginning to the end.

What about OMIPv6…?

- OMIPv6 narrows the window of vulnerability to the minimum.
- OMIPv6 offers a malicious node only **ONE** chance.
- OMIPv6 uses the result of one RR test to compute a strong shared secret.
- OMIPv6 eliminates all signaling messages except the BU messages.
- OMIPv6 substantially reduces the latency.
- OMIPv6 uses the direct path.

The only **ONE** chance trade-off

- OMIPv6 is a practical aspect of the trade-off behind the PBK framework (S. Bradner, A. Mankin, J. Schiller):

“*However, there are many circumstances where we can improve overall security by narrowing the window of vulnerability, so that if we assume that some operation is performed securely, we can secure all future transactions*”

Main Features

- The DH exchange is shielded from DoS attack by signing the messages with the Kbm (more information in SIGMA).
- DH message duplicated and each copy sent on a different path.
- When the MN switches to a new network, it sends ONLY a BU message.

Changes from the initial version

- The CoTI/CoT messages are eliminated.
- The Nonce Index option MUST NOT be used.
- The Alternate Care-of Address option (if used) MUST contain the **real** CoA (more information in draft-dupont-mip6-3bombing-00).
- The BU MAY be duplicated.

NEXT…?

- Comments are highly appreciated.
- WG item…?
- Thank You!