HMIPv6sec

draft-haddad-mipshop-hmipv6-security-04
IETF66 - MIPSHOP WG
July 2006

Quick Overview

- HMIPv6sec protocol allows the MN to securely establish a bidirectional security association with the MAP in order to authenticate the LBU/BA messages.

- Previous versions relied on “CGA AND CBID” technologies.

- Current version simplifies the protocol by removing the reliance on CBID and removes any additional option from the RtSol message.

Protocol Description (1)

- MN sends a RtSol message signed with CGA.
- AR replies with a unicast RtAdv message signed with CGA and carrying a shared secret (Ks) encrypted with the MN's CGA public key.
- AR sends a PBU message to the MAP, which carries Ks and the MN's LCoA and RCoA. RCoA's IID is generated from Ks and LCoA.
- MAP creates a binding between Ks, LCoA and RCoA then waits for an LBU message during a *limited* period.

Protocol Description (2)

- MN sends an LBU message to the MAP. The LBU is authenticated with Ks and carries the MN's DH public value.

- After receiving a valid LBU message, the MAP sends its own public DH value and the hash of Ks in the BA message and generates a long lifetime secret (Kms) from completing DH.

- After receiving a valid BA message, the MN computes Kms and use it to authenticate all subsequent LBU messages.

Next Step?

- We believe that current version is in good shape.
- WG item?

Thank You!