Authenticating FMIPv6 Handoffs

draft-haddad-mipshop-fmipv6-auth-01
IETF66 - MIPSHOP WG
July 2006

Motivation

- In FMIPv6, each time the MN switches to a new AR (nAR), it has to send an FBU message to its pAR.
- ARs are only *ONE* hop away from the MN.
- Infrastructure can be trusted.
- MN has (very) limited energy and processing power => better to use them for exchanging data and not on signaling messages!

Requirements

- pAR must ensure that an FBU message is sent by a “legitimate” node.
- The target of an FBU message *cannot* be any node.
- Avoid creating new privacy issues between the MN and the CN.
- Minimize signaling messages!

Proposal (1)

- MN generates a 64-bit OWHC and sends the tip to its first AR in a RtSol message signed with CGA. Such action is needed ONLY at the beginning.

- AR sends a unicast RtAdv message signed with CGA and carrying a 64-bit HV. HV is encrypted with the MN’s CGA public key.

- MN uses OWHC sequence to autoconfigure each nCoA, then it “XOR” the new IID with HV before sending it in a FBU message.

Proposal (2)

- pAR validates an FBU message by decoding the nCoA and pCoA IIDs then verifying if the nCoA IID belongs to the OWHC.
- pAR sends HV to the nAR in the HI message.
- pAR sends an FBA message to the MN as a proof for receiving a valid FBU message and HV.

Questions?