Authenticating Binding Updates in FMIPv6

draft-haddad-mipshop-fmipv6-auth-02
November 2006

Motivation

- **Simple and cheap** solution to authenticate FBU messages sent by the MN to the pAR.

What's new in this version?

- Add an integrity protection to the FBU message.
- Extend one way hash chain values to 128 bits.

First Steps

- Use SEND protocol on the MN side **only at the beginning** (i.e., with the first AR) to anchor the OWHC to the access infrastructure.
- Each OWHC value is used together with a 64-bit "Handoff Vector (HV)" to authenticate signaling messages related to one handoff.

Proposed Solution

- 64 bits of the OWHC value are used to configure the nCoA's IID (after XORing with HV).
- Remaining 64 bits are sent in a new option (after XORing with HV).
- The OWHC 128-bit value is used to generate the MAC.
- pAR decodes the two values, concatenates them and compares the new value to the stored one, then checks the MAC.
- pAR sends Hash(HV) and current OWHC to nAR.

Next Step?

- This solution is built on draft-kempf-mipshop-handoff-key
- Merge the two drafts?
- Adopt it as WG item?

Questions?
Thank You!