Optimizing MIPv6 with Crypto-based Identifiers (OMIPv6)

draft-dupont-mipshop-omipv6-00

IETF 65

Francis Dupont
CELAR

Wassim Haddad
Ericsson Research

OMIPv6-CGA Problems

- During the first (and unique) RR procedure, a malicious node located between the CN and the MN's HA can "learn" the first home keygen token sent in the HoT message and can always keep a fresh care-of keygen token. Immediately after intercepting a HoT message, the malicious node can send a "valid" BU message on behalf of the MN => **The CN MAY NOT accept a "second" BU with CGA.**
- **CGA IPR issue has not been solved completely!**

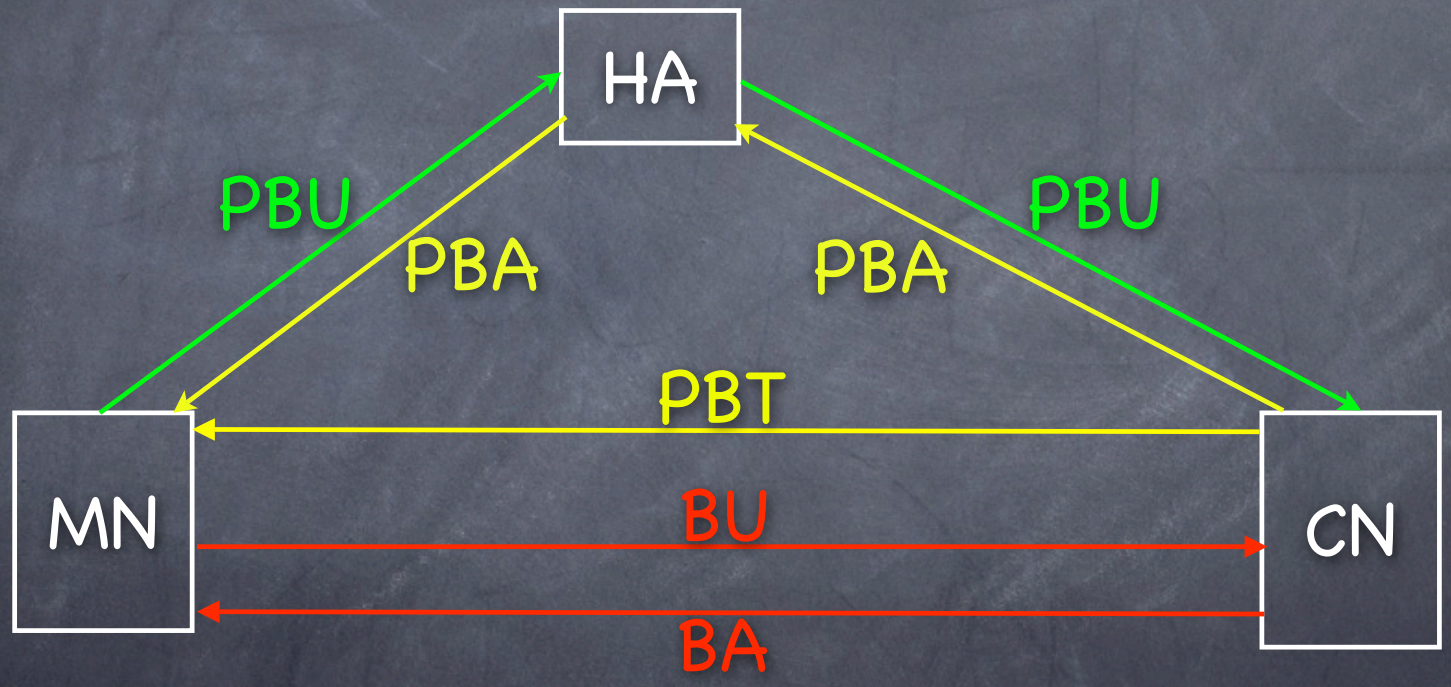
OMIPv6-CBID Enhancements(1):

- A Crypto-based Identifier CBID is a 128-bit non routable identifier derived from hashing a public key and a 64-bit imprint.
- **CBID has no IPR issues.**
- Using a modified version of the CBID technology, instead of CGA, allows the MN to address the two problems described earlier.

OMIPv6-CBID Enhancements(2):

- Using CBID in OMIPv6 requires splitting the CBID into two 64-bit identifiers, which will be used as interface identifiers (IIDs) for auto-configuring the HoA and CoA.
- After performing successful reachability tests for both MN's addresses, the MN sends a BU message to the CN, which contains the public key and the imprint only. The BU message will be authenticated with the shared key generated during the addresses reachability tests, and signed with the MN's private key.

Overview of Messages Exchange



OMIPv6-CBID Enhancements(3):

- By splitting the CBID into two interface identifiers (IIDs) and using them in auto-configuring the CoA and HoA, the CBID allows the MN to provide the CN a proof of ownership of its HoA and current CoA.
- Subsequent MN's CoA IID(s) can be derived from hashing the shared secret (SKbm) with the foreign network prefix. However, a reachability test may always be needed.

Next Step?

- Replace the CGA part in the OMIPv6_CGA_CBA with CBID

Questions?
Thank You!