64th IETF Meeting - Vancouver
MIPSHOP WG

# Combining CGA and CBID to secure HMIPv6

draft-haddad-mipshop-hmipv6-security-01

# Problem Statement

- Current HMIPv6 specification does not specify nor favor any security mechanism to establish a bidirectional SA between the MN and the MAP.
- HMIPv6 security has raised many concerns...

# Proposed Solution (1):

- Assume that SEND protocol will be deployed.
- Assume that paths between ARs and MAP are secure.
- Assume **(but not necessary)** that the MN gets a RtAdv message when attaching to the first AP, i.e., before sending a RtSol message.
- Avoid using CGA/CBID directly between the MAP and the MN to prevent DoS attacks and... IPRs issues!
- **No** additional signaling between the MN and the MAP, i.e., except the LBU and BA.

# Proposed Solution (2):

- The MN uses CGA to send a RtSol message to the AR (according to SEND). The RtSol message carries a 128-bit CBID.
- The AR generates a secret (Ks), encrypts it with the MN's CGA public key (Kp) and sends it to the MN in the RtAdv message.
- The AR sends a PBU message to the MAP, which carries the MN's LCoA, Kp, Ks and CBID.
- After receiving a valid PBU, the MAP creates a BCE to the MN.

# Proposed Solution (3):

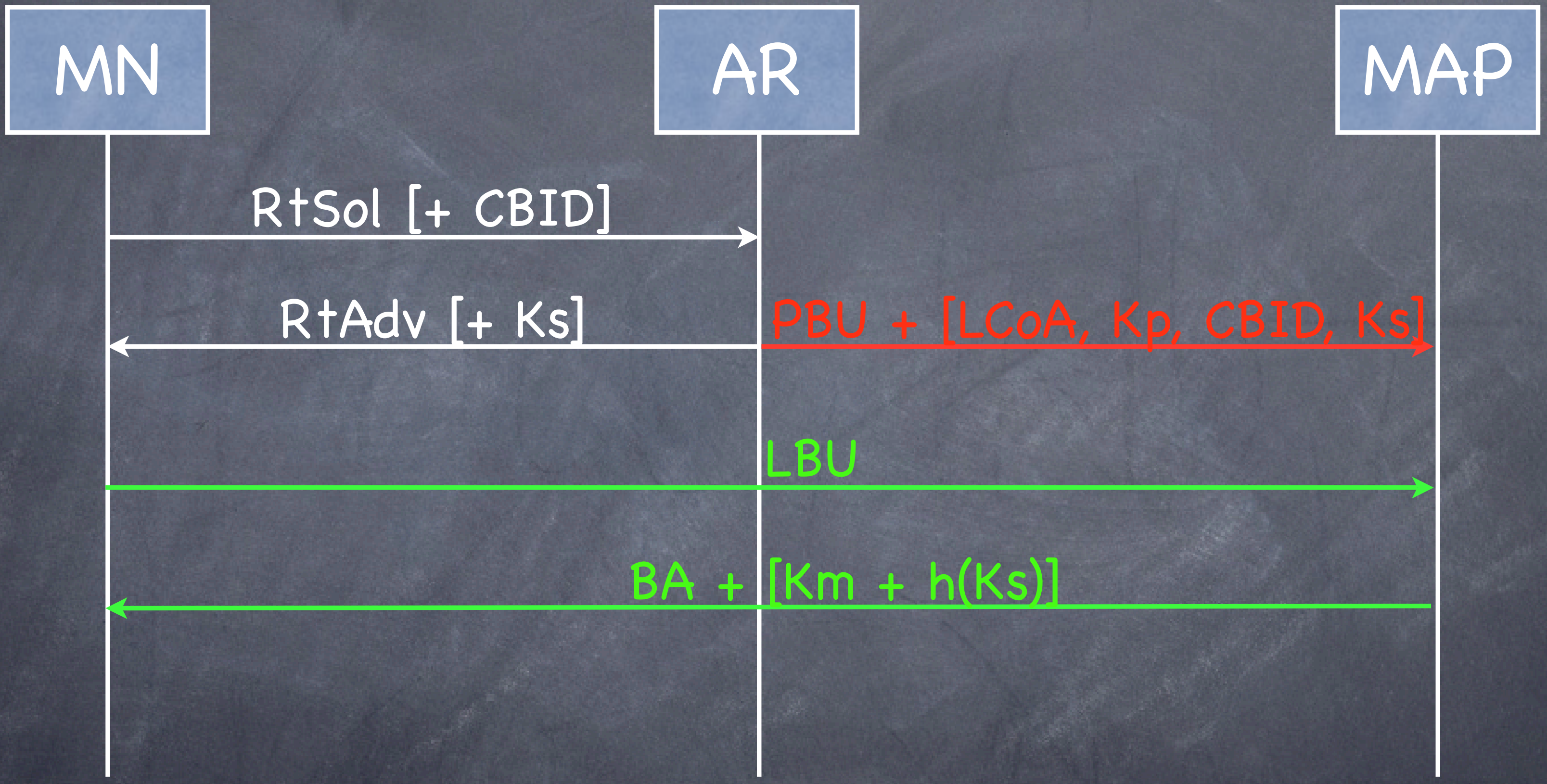
- The MN uses the 64-bit imprint used to generate the CBID, as IID to auto-configure its RCoA and sends an LBU message to the MAP.

- The MAP checks the ownership of the RCoA and CBID by recomputing it from the RCoA's IID and the MN's corresponding CGA public key (Kp).

- The MAP generates a long lifetime shared secret (Km), encrypts it with Ks and sends it in the BA message. The BA message contains also hash(Ks).

- Both nodes use Km to authenticate subsequent LBU/BA messages.

# Signaling Diagram



Questions?

Thank you!