

Security Concern of Network Prefix

Prepared for 61st IETF NEMO WG

By

Chan-Wah NG, Jun HIRANO

2004 11 10

`draft-ng-nemo-rrnp-00.txt`

Sending of Prefix-Scoped BU

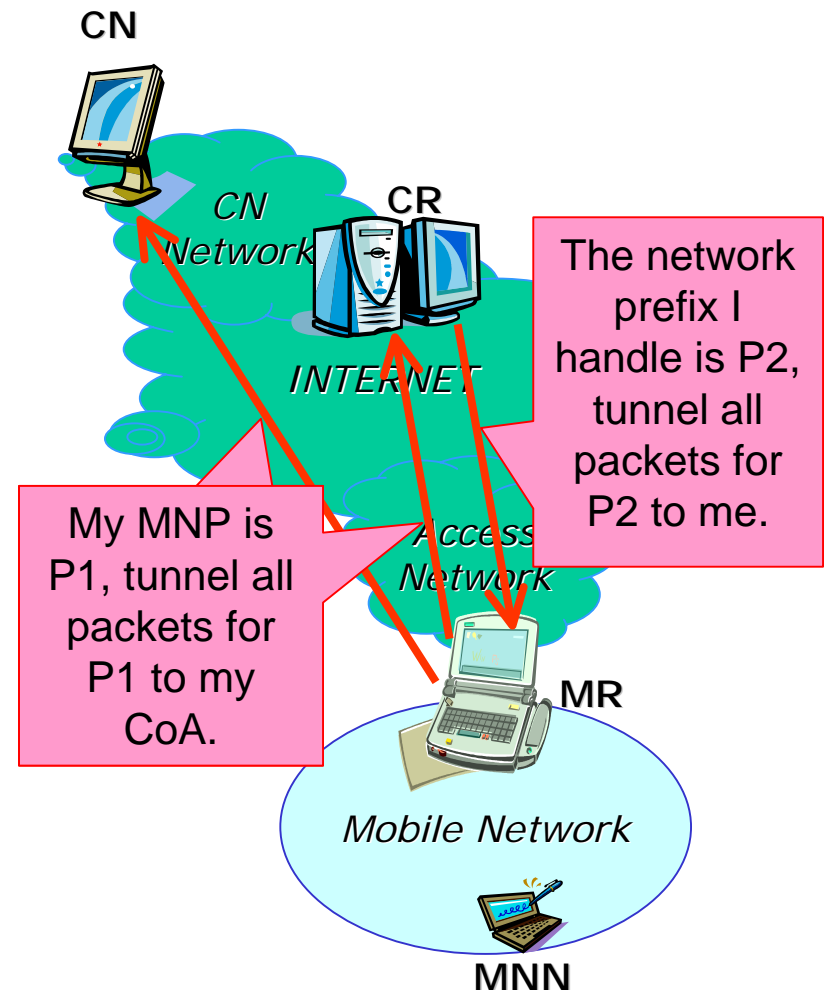
To achieve NEMO RO, one possible approach is for mobile router to send BU with Mobile Network Prefix option:

❖ MR-to-CN optimization

- MR sending BU with MNP to CN

❖ Infrastructure Optimization

- MR sending BU with MNP to CR
- CR informing MR the network prefix CR is managing



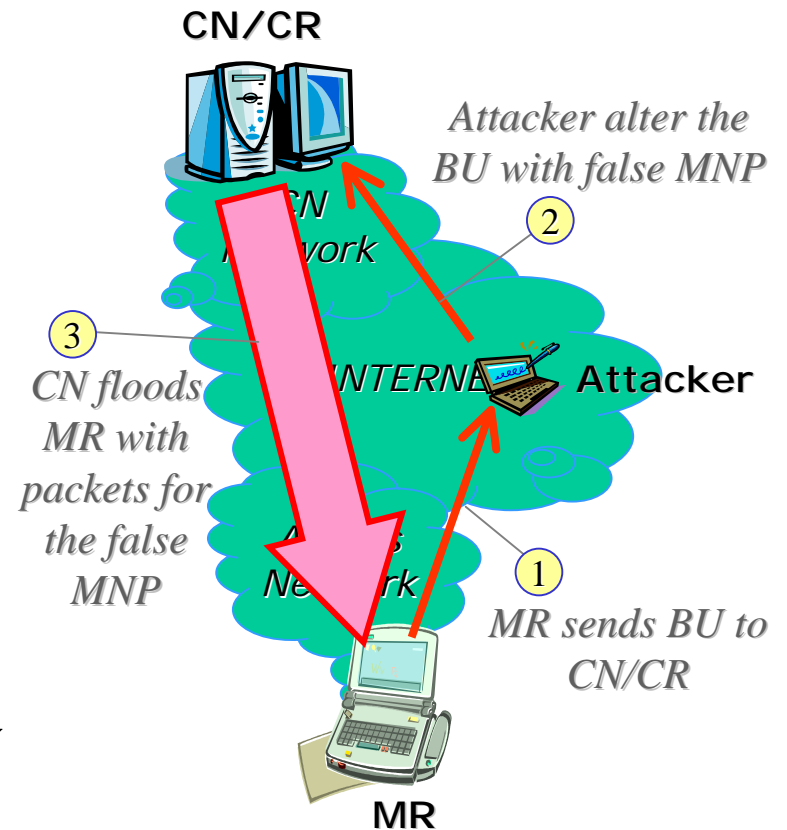
Security Threat 1

❑ The BU with Mobile Network Prefix option is

- ❖ Changed en-route
- ❖ Inserted with extra, bogus MNP options

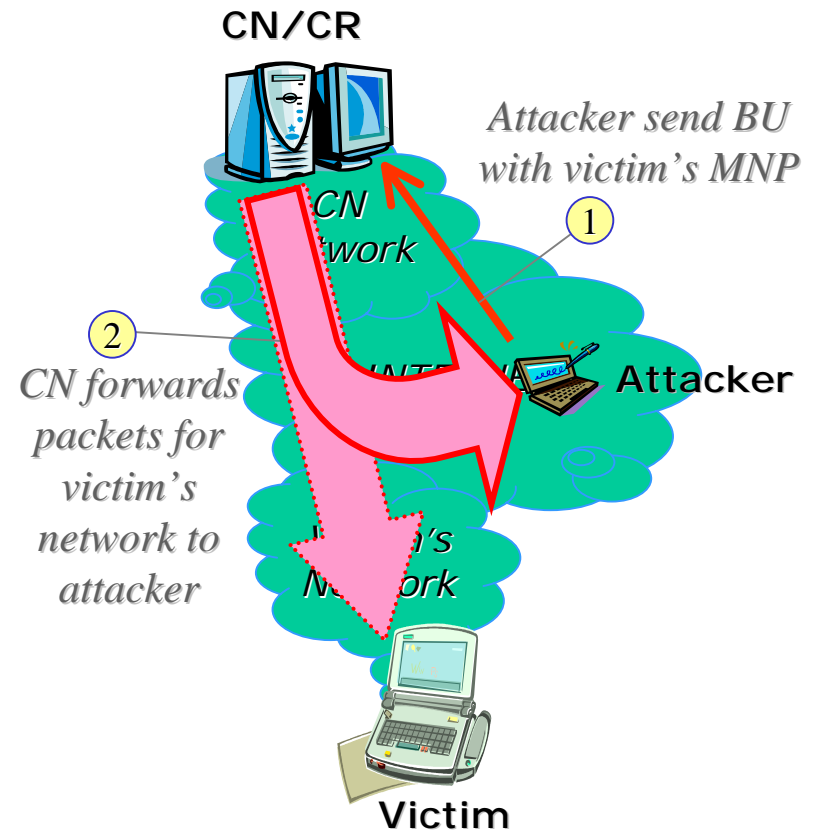
so that CN or CR unknowingly flood the MR with packets not destined for the mobile network

❑ This threat is protected by Return Routability procedure, since BU message is protected by binding management key.



Security Threat 2

- ❑ The mobile router itself is malicious, claiming to manage mobile network prefixes it doesn't actually own.
- ❑ This threat is **NOT** protected by Return Routability, since RR only verifies collocation of CoA and HoA, not MNP.



Return Routability with Network Prefix

- ❑ Possible protection is to extend RR
- ❑ Basic idea is for CN to send a Keygen Token, NPK, to a random address configured from the network prefix in a Network Prefix Test message
- ❑ MR must intercept this packet, and use it to generate the binding management key

