Security Concern of Network Prefix

Prepared for 62nd IETF NEMO WG
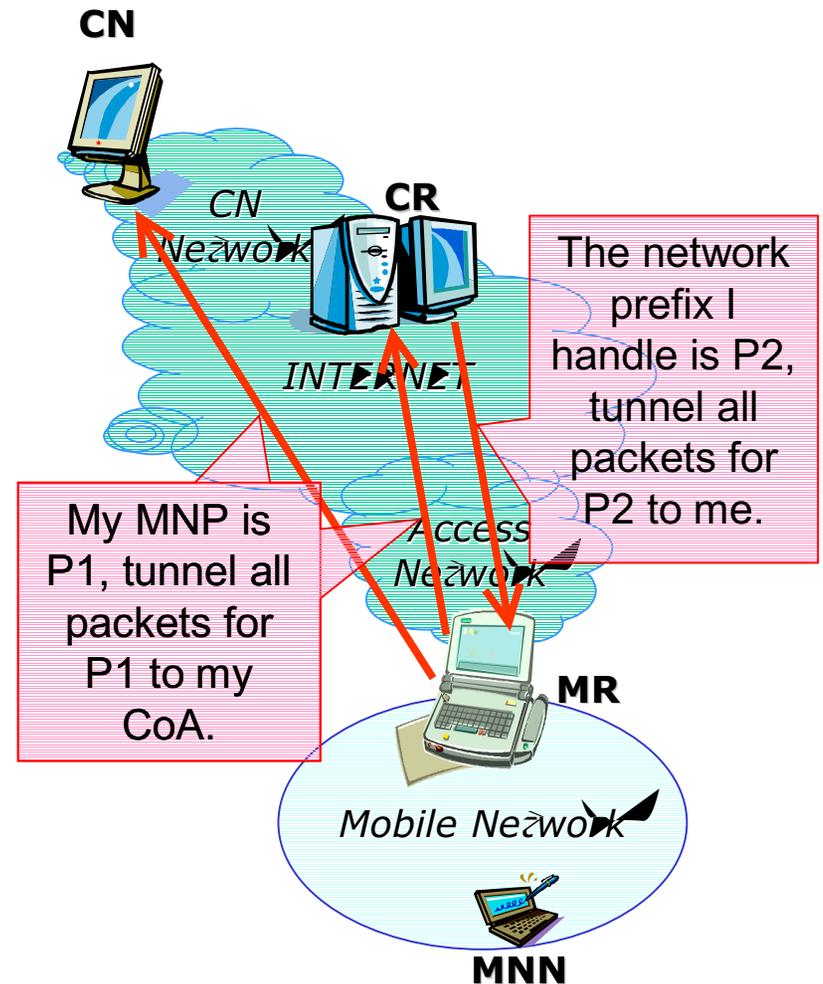
By

Chan-Wah NG, Jun HIRANO

20050309

```
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

CN

CN Network

CR

INTERNET

The network prefix I handle is P2, tunnel all packets for P2 to me.

My MNP is P1, tunnel all packets for P1 to my CoA.

Access Network
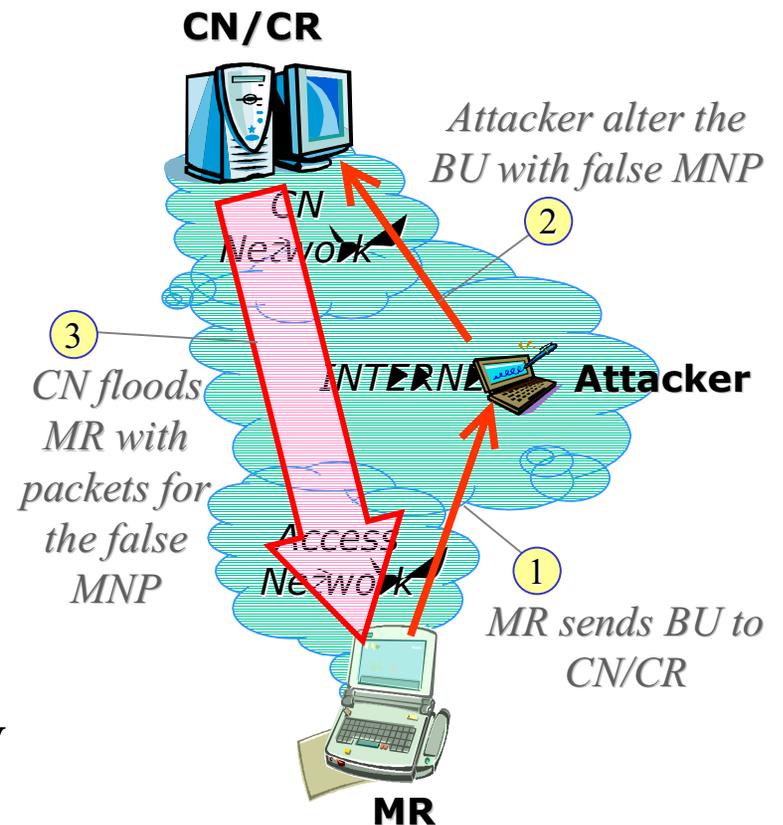
MR

Mobile Network

MNN

Security Threat 1

❑ The BU with Mobile Network Prefix option is

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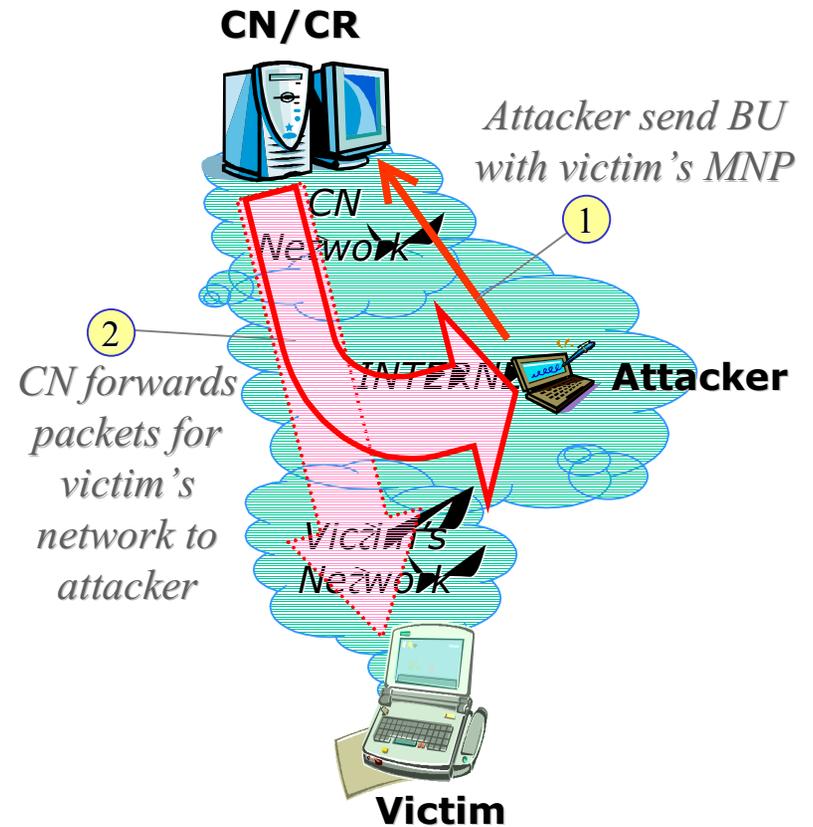- ❖ Inserted with extra, bogus MNP options

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.

CN/CR

Attacker alter the BU with false MNP

2

CN
Network

3

INTERNET **Attacker**

CN floods MR with packets for the false MNP

Access Network

1

MR sends BU to CN/CR

MR

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.

CN/CR

Attacker send BU with victim's MNP

1

CN Network

2

CN forwards packets for victim's network to attacker

INTERNET **Attacker**

Victim's Network

Victim

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

MR   **HA**   **CN/CR**

CoTI

CoT + CoK

HoTI with MNP option

HoT + HoK + num-of-NPT

NPT + NPK

MR starts inspecting packets destined for MNP to intercept NPT

BU + MNP + Authenticator = f (BU, HoK|CoK|NPK)