Mobile IPv6 Residual Threats

draft-haddad-mext-mip6-residual-threats-02

IETF 72 July 2008

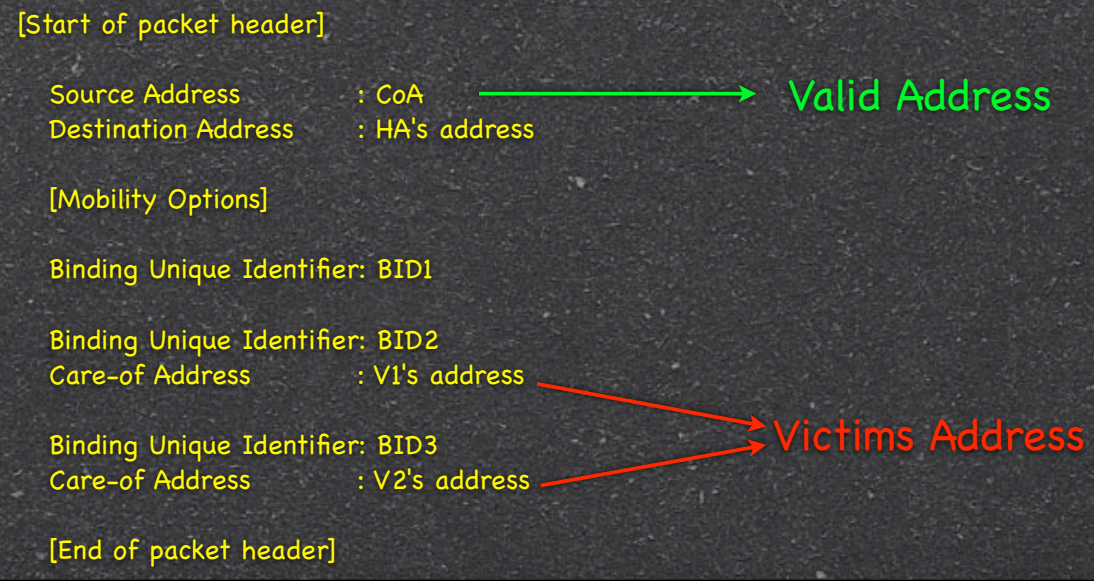
Residual Threats Associated with a Malicious Mobile Node

Violating Trust Between the MN and its Home Agent

- Trust model adopted in MIPv6 protocol assumes a "good behaving" MN towards its HA.
- This also means that the HA will always believe the MN claims regarding its current whereabouts as expressed in the care-of address (CoA).
- However, this is not always the case and such relationship may be abused by a malicious MN in order to launch flooding attacks against a targeted network/node.
- Consequently, the HA needs a mechanism which:
  1. verify the MN's reachability on the claimed CoA
  2. Enable a network to repel a possible flooding attacks

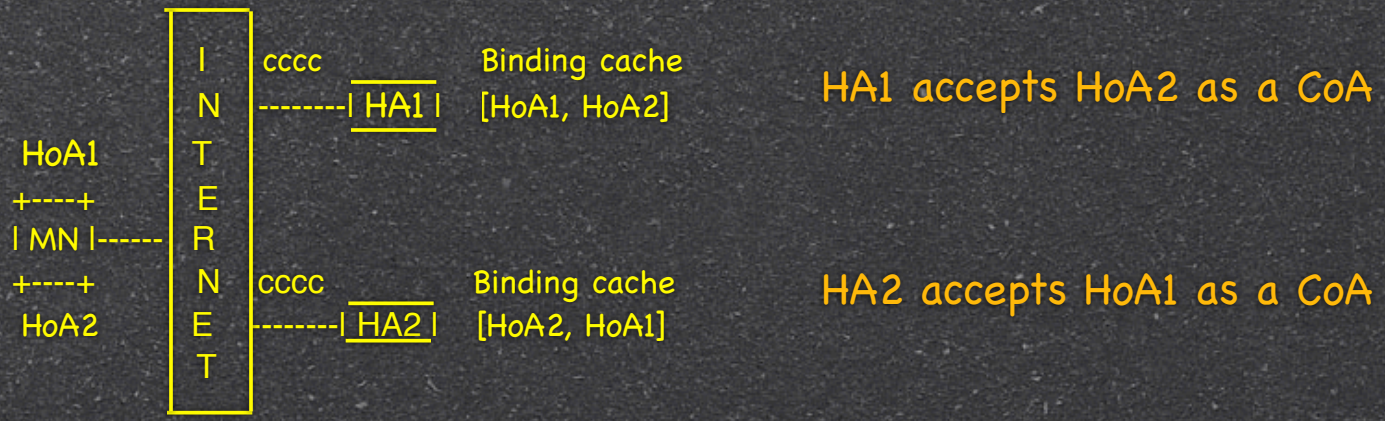
Violating Trust Between a multihomed MN and its HA

- Multiple CoAs registration extends a MN's ability to register multiple CoAs with its HA.
- Such feature enables a malicious MN to register multiple fake CoAs at the same time with one message.
- In order to bypass ingress filtering protection, the MN can use a valid CoA as the "main" address and a set of fake CoAs in the BU message:



Creating Routing Loops Among Home Agents

- In MIPv6, it is possible to create routing loops among HAs. This is achieved when a MN binds its HoA located on the first HA to its second HoA located on the second HA.
- Such type of binding force the two HAs to tunnel and re-tunnel data packets while re-routing them between themselves without knowledge that a routing loop has been created.
- Attack is limited to case where the MN has multiple HAs (e.g., 3GPP).



Exploiting Multihoming to Defeat Ingress Filtering

- A malicious multi-homed node can use its multiple interfaces to emulate a home agent and defeat ingress filtering.
- In this attack, a malicious node uses one of its interface (I1) as home network to establish multiple sessions with different CNs then at some point, triggers an RR procedure using a second interface (I2) attached to the targeted network for the CoA exchange.
- After re-directing the traffic to the targeted network, the attacker switches off I2 and keeps sending legitimate ACK messages from a legitimate topological location and using a legitimate IPv6 address.
- In such scenario, the targeted network is flooded and ingress filtering is defeated.

Threat Associated with an Attacker Located on the Foreign Link

Exploiting Neighbor Discovery In MIPv6 Environment

- A malicious node located on the same foreign link than one or a set of mobile nodes can learn the HA IP address together with the MNs HoAs and at some point, start advertising the home prefix.
- Upon detecting a home prefix advertisement, the set of MNs will send BU messages in order to de-register.
- At this point, if the BU is received by the HA, then the attacker will detect it and can start sending fake ACK to the CNs in order to attack the home network.
- However, if ingress filtering is enabled then the attacker can re-send the BU messages to their destination using another interface with no ingress filtering then start sending fake ACK.
- Note that the attacker may also advertise another foreign (fake) prefix...

Questions?
Thank You!