Allocating bit in IID for Mobile IPv6

Erik Nordmark
nordmark@sun.com

- Mobile IPv6 will use return routability to authorize binding updates at CNs
  - Derives its security from the routing system
  - Doesn't seem to do any harm compared to today
  - All CNs i.e., all IPv6 nodes likely to support this
- Some residual threats association with RR

Concern

- Hopefully we can secure neighbor discovery in the future
- Thus attacker would need to attack router or switch to become a Man-in-The-Middle
- In this case RR might be the weakest link
- How can we “turn off RR” then?
  - Implemented in all CNs
  - Need to selectively turn it off for MNs that want better security

Bidding Down

- Generic security concept of bidding down
  - Multiple methods exist with different security properties
  - Node wants to use a more secure method
  - Attacker can select the least secure method
- Specific case is bidding down to use RR
  - CN receives a binding update using RR
  - Did MN want RR or something stronger?

Alternatives

- Each time BU received look in some securable infrastructure to determine the MN policy
  - E.g., DNS reverse lookup of MN's address to find the XYZ resource record which contains the policy
  - E.g., AAA infrastructure
- Ask the MN about its policy
  - Assumes a secure channel between CN and MN
  - RR will operate when no such channel – does not assume a PKI

Idea

- Bit (or bit pattern) in IID indicates that standard security does not apply
  - E.g., RR does not apply, stronger ND, anycast checks
- Asumes that the node has additional unsecured information e.g., in a binding update
- Causes node to verify the information
  - Could invoke the infrastructure
  - Could perform infrastructure-less checks

Strawman

- Assume BU has a parameter called “verification type”
  - used when the bit is set in the IID
- Verification types (just an example)
  - DNS (not advocating that we do this)
  - AAA
  - IID is hash of parameters

Infrastructure-less verification

- Note: There are IPR notifications on the IETF web site that might apply here
- IID is a hash of parameters
  - The term “Hash Generated Addresses” have been suggested
- Multiple types
  - IID is hash(type, random number, ...)
  - IID is hash(type, public key, ...) [CGA]
  - IID is hash(type, hash chain, ...)

Potential use

- MIPv6 binding updates
- Neighbor solicitations and advertisements
  - Avoid DAD attacks, ND spoofing
  - Does not handle router advertisement spoofing
- Anycast membership in MLD
  - Anycast addresses that has bit set
- The “challenge” protocol for ND and anycast is TBD