

Alien Lower Layers Problem Statement

draft-haddad-momipriv-problem-statement-01.txt

Erik Nordmark
erik.nordmark@sun.com

Wassim Haddad

Identifiers

- Identifiers at multiple layers
 - IPv6 addresses
 - MAC addresses
- Visibility is different
 - Correspondents (Web servers) and on-path observers can see IPv6 addresses
 - Observers on link (or in 802.11 distribution system) can see MAC addresses
- Multiple identifiers from different layers in the same packet

Location Privacy

- Geographic location
- Topological location
- There is some relationship between them, which is deployment dependent

IPv6 addresses

- Solved problem?
 - EUI-64 derived IPv6 addresses are problematic – same EUI-64 forever
 - RFC 3041 temporary addresses provide pseudonymity

Mobile IPv6

- Route optimization
 - Avoid to disclose CoA to correspondent
 - MN can choose not to do it with some CNs
- Mobile IPv6 and RFC 3041
 - Home address fixed even if CoA is RFC 3041
 - Home address in the clear in BU to HA
 - Need to allow MN to generate RFC 3041 home addresses even when away from home?

MAC addresses (1)

- Visibility limited to local link
 - But this could still be a concern, depending on the attackers capabilities
 - Compare with cellular systems, where the visited operator doesn't know my phone is the same as the phone that visited them a week ago
- Could in theory do temporary, random MAC addresses
 - Collisions?
 - IEEE defining security schemes which tie certificate to MAC addresses (802.16)

MAC addresses (2)

- But isn't this IEEE's problem?
 - Yes, but do they think it is a problem?
- Interaction with multiple identifiers is for the IETF
 - See next slides

Layer interactions

- Assume RFC 3041 IPv6 addresses
- Assume random, temporary MAC addresses
- To avoid linking from one to the other, need to switch between identifiers sets across layers at the same time

Example Layer interactions

- MAC + IP
 - Change from IP(1) to IP(2) – need to change from MAC(1) to MAC(2) at the same time
- HoA and CoA are both RFC 3041
 - Only use CoA(1) with HoA(1) etc
- Other layers?
 - Identifiers in EAP that go in the clear? Even if pseudonyms, need to switch these when switching other identifiers

Possible actions

- Engage IEEE 802 for the MAC address part?
- Implementation advice document for switching between sets of temporary identifiers instead of being layer independent
- Mobile IPv6 RFC 3041 HoAs while away from home?
- EAP identifiers?