Security Threats to NETLMM

Revision of draft-ietf-netlmm-threats

James Kempf ⟨kempf@docomolabs-usa.com⟩
Christian Vogt ⟨chvogt@tm.uka.de⟩

Overview of Changes

- Included threats analysis for AR-LMA i/f
- Revised MN authentication
  - Network access identity replaces MN-ID
    - "…allows the network to unambiguously identify the mobile node for signaling purposes"
    - Can be link-layer session key, NAI, SEND public key, etc.
- Removed threats existing in regular IPv6
  - Location privacy threats
  - Attacks on data plane
  - Attacks on AR functions

Threats to MAG-LMA Interface

- Unauthorized AR
  - Spoof NETLMM signaling
    - Redirect MN's traffic
    - Drop MN's traffic
  - MitM threat same as in regular IPv6
- Unauthorized LMA
  - Spoof NETLMM signaling
    - Redirect MN's traffic
    - Drop MN's traffic
  - Gateway position ⇒ MitM threat
  - Malware might corrupt routing table ⇒ all traffic forwarded to single link ⇒ DoS

Threats to MAG-LMA Interface

- MitM from between AR and LMA
  - Intercept + analyze NETLMM signaling
  - Spoof NETLMM signaling
    - Redirect MN's traffic
    - Drop MN's traffic
- Flooding of entities inside NETLMM domain
  - Interior IP addresses not communicated in protocol
  - Compromised MN cannot pass IP addresses off
  - $\Rightarrow$ Vulnerability lower than, e.g., in H-MIPv6
  - Address scanning possible, but expensive in IPv6

Threats to MAG-LMA Interface

- Flooding of IP addresses from access links
  - IP address unused?
    - LMA discards packets after routing table look-up
    - ⇒ Vulnerability lower than in regular IPv6
  - IP address registered?
    - LMA performs routing table look-up, encapsulates packet
    - Packet forwarded through NETLMM domain
    - MAG decapsulates packet, possibly performs address resolution, delivers packet to MN
    - MN discards packet
    - ⇒ Vulnerability slightly higher than in regular IPv6

Threats to MN-MAG Interface

- Attacks on NA-ID
  - Impersonation of NA-ID upon initial attachment to NETLMM domain
  - Binding false IP addresses to NA-ID
- Impersonation upon handoff
  - Redirect MN's traffic
  - MitM if attacker can interpose during router discovery and address configuration
- Off-link attacks
  - Impersonation of MN from different link