Draft summary
Reviewers' comments
Mailing-list discussion

NETLMM Security Threats on the MN-AR Interface

draft-kempf-netlmm-threats-00.txt

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

65th IETF, Dallas, TX, March 21, 2006

New Terminology

- **MN authentication**: Initial authentication of MN for network-access authorization
- **MN identifier**: String based on which MN authentication can be accomplished
- **Data-origin verification**: Sender verification for IP packets sent by a MN for network-access and accounting purposes
- **Data-origin identifier** (formerly called a "per-packet identifier"): String/property based on which MN can be identified for data-origin verification of its IP packets
- **Locator**: Destination address of an IPv6 data packet (This is not a definition specific to NETLMM.)
- Thanks to Julien for raising the need for a better terminology

Roaming at a Victim's Costs

- Problem: Spoofed data-origin ID
  - Attacker sends packets on behalf of victim
  - Attacker roams at a victim's costs
  - After initial MN authentication
- Data-origin verification can prevent this
  - May have to be bound to initial MN authentication
  - Only in MN-2-CN direction
- External protection against bogus packets from malicious CN

Off-Path Eavesdropping

- Problem: Impersonation during DNA
  - Impersonator mimics victim during DNA
  - NETLMM redirects victim's packets to impersonator
  - ⇒ eavesdropping from off the path
- Limitation: Impersonator cannot forward packets to MN if MN is on different link
  - because impersonator uses same IP address as MN
  - Different than in Mobile IPv6, where impersonator's "c/o address" differs from victim's "home address"

Denial of Service

- Problem: Impersonation during DNA
  - Similar to off-path eavesdropping,…
    - Misuse of DNA
    - Redirection of victim's packets
  - …but intended to cause DoS to victim
- Limitation: Attacker must redirect packets to itself
  - because NETLMM delivers packets to where a MN is believed to be seen
  - Again different than in Mobile IPv6

Threats to AR Functions

- Problem: Rouge AR acts as man in the middle
  - May eavesdrop on packets,
  - modify packets,
  - forward packets via a path outside NETLMM
- Limitation: Return packets go through NETLMM
  - Rouge AR may see return packets,
  - but may not be able to modify them
- But: Rouge AR may act as NAT box

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

Threats to IPv6 Neighbor Discovery

- Problem: Vulnerabilities of ND6/DNA
  - Apply to NETLMM…
  - …because NETLMM uses ND6/DNA
- SeND can prevent some attacks

Location Privacy

- Problem: MN identifier associated w/ IP address
  - MN identifier leaks during MN authentication
  - Attacker associates identifier w/ IP address
  - Attacker then tracks victim's IP address
- Threat 1: Attacker on access link
  - Sends NS for victim
  - Address resolution or DAD
- Do ARs forward ND6 signaling to other links?
  - DAD requires this given that links have common prefix(es)
  - NA indicates that victim is inside NETLMM or on the same link

Location Privacy (2)

- Threat 2: Attacker btw. ARs and MAP
  - Attacker eavesdrops on NETLMM signaling
  - Most effective close to MAP
  - Encryption can prevent this
- Threat 3: IP address tells victim is inside NETLMM
  - Limitation: NETLMM prefix not very precise
  - Traceroute, too, may not produce meaningful information due to the MAP-AR tunnel

Some comments related to AR-MAP interface.

This summary focuses on MN-AR interface.

Reviewers' Comments

Mailing List Discussion

Implicit Data-Origin Identifier

- Data-origin ID may not show up in packets
  - Can be port of switch,
  - frequency slot,
  - time slot, etc.
- Identified by Julien

- Data-origin ID can be MN-MAP security context
  - MN perceives all ARs as a single, "virtual" MAP
- Identified by Gerardo

Flooding Mobile Nodes

- Draft does not mention flooding of MN's IP address
  - Mentions only flooding of ARs or MAPs
- More dangerous for existing IP addresses
  - Bandwidth of MAP's Internet attachment
  - Routing-table look-up at MAP
  - Encapsulation at MAP (special in NETLMM)
  - Bandwidth w/in NETLMM domain
  - Decapsulation at AR (special in NETLMM)
  - Neighbor Cache look-up at AR
  - New Neighbor Cache entry at AR
  - ND6 signaling w/in access network
- Less dangerous for non-existing IP addresses
  - MAP discards packet after routing-table look-up
- Identified by Julien

See also RFC 3756, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", section 4.3.2

IGP Security vs. NETLMM Security

- IGP security vs. NETLMM security unclear
  - Draft relates IGP security to NETLMM security, but…
    - routing protocol is hop-by-hop
    - NETLMM protocol is end-to-end (i.e., AR-to-MAP)
  - Clarify that in the draft
- Identified by Vidya