

Mobile IPv6 Bootstrapping Problem Statement

<http://www.arkko.com/publications/mipv6/drafts/bootstrap.html>

James Kempf

DoCoMo Labs USA

Jari Arkko

Ericsson NomadicLab

What is Dynamic Bootstrapping?

- Dynamic Home Agent and home network prefix discovery.
 - Not directly related to security.
 - Does imply changes in authorization information.
- Dynamically setting up an IPsec SA between Home Agent and Mobile Node.
 - Intended to be used when the Mobile Node comes on line initially.

Potential Benefits of Dynamic Bootstrapping

- Dynamic Home Address assignment enables wider array of address assignment choices and reduces configuration burden.
- Dynamic Home Agent assignment allows load balancing, optimal tunnel management, and location privacy.
- Security benefits by allowing integration of AAA infrastructure.
 - Leverage network access authentication for Mobile IP service authorization.
- New business models enabled, allowing non-subscriber based access networks to offer opportunistic Mobile IP service.

Current Specification

- Not fully dynamic due to restriction to manual keying or IKEv1 for SA establishment.
- Manual keying
 - SAs bound to a specific **statically** defined home address and **statically** assigned Home Agent address.
- IKEv1
 - Mobile Node must have a **statically** defined home address.
 - During Phase 1 ISAKMP exchange, home address is used to:
 - Make authorization decision.
 - Identify credentials

Specific Benefits

- Reduces RTT on Home Agent/Mobile Node tunnels.
 - Optimal HA assigned for distant locations.
- Hides Mobile Node topological location.
 - This precludes route optimization.
- Reduced configuration required on both the Mobile Node and the Home Agent.
- Strengthens Mobile Node resilience to network renumbering.
- Enables network to assign Mobile Nodes to Home Agents dynamically.
 - Allows management of Home Agent load balancing by assigning Mobile Nodes according to load.
- Authorization of a device to become an MN.

Difficulties with Current Prefix and Home Agent Discovery Protocols

- The current protocol support for pushing prefix changes to dormant Mobile Nodes has drawbacks.
 - Mobile Node must be actively listening for protocol.
 - Many Mobile Nodes will be in dormant mode or simply switched off.
 - ISP needs to keep old prefix around indefinitely or use an out of band mechanism to inform dormant Mobile Nodes of the change.
- Home Agent discovery message is sent to an anycast address in the clear.
 - Protocol uses ICMP.
 - ISPs now routinely block ICMP at firewalls to prevent ping attacks, other problems.

Four Dynamic Bootstrapping Scenarios

- Creation of an IPsec SA without any previous association.
 - Example: an access network providing non-subscription based Mobile IP services to walk-up clients.
- Turning an existing security association in the home network into an SA for Mobile IPv6.
 - Example: A VPN SA in a corporate network is changed into an SA for Mobile IPv6.
- Turning another existing security association into an SA for Mobile IPv6.
 - Example: A security association established by AAA with an access network is changed into a dynamic Home Agent SA for local Home Agent service.
- Turning a security association with a Home Agent into one for other uses.
 - Example: An SA established for one home address can be used to communicate changes in addresses or Home Agents.

→ 2, 3, and 4 of primary interest.

Conclusions

- Dynamic bootstrapping has many potential benefits to simplify deployment and network management and widen the applicability of Mobile IPv6.
- Current IPsec SA establishment mechanisms don't allow full dynamic bootstrapping.
- Home agent and prefix discovery protocols have limitations from security and network management perspectives.
- Further work required on mechanisms to facilitate dynamic bootstrapping.