MIPv6 bootstrapping with the Authentication Option protocol

MIP6 WG, IETF 65

Vijay Devarapalli, Alpesh Patel,
Kent Leung, Kuntal Chowdhury

Why?

- Current bootstrapping protocols focused on IKEv2. Work only when IKEv2 is used
- Home Address configuration
  - Requires IKEv2 CFG Payloads for HoA assignment and auto-configuration
- Security Association Setup
  - IKEv2 dynamically sets up security associations between the MN and the HA
  - EAP is used to authenticate to infrastructure elements like the AAAH

RFC 4285

- RFC 4285 is an alternative to IPsec (and IKEv2), but does not provide all the features
  - But still used
- Developing bootstrapping mechanisms in the IETF is essential
  - Otherwise we end up with multiple proprietary mechanisms

Bootstrapping a Home Agent

- No new mechanism

- Existing mechanisms can be used
  - DNS lookup
  - DHCP based assignment
  - DHAAD

Home Address Configuration

- Mobile node sends a Binding Update with 0::0 home address
  - The MN MUST include the MN Identifier Option (RFC 4283)
- The Home Agent sends the home address in the Binding Ack
- Two new mobility options
  - Home Address Request Option
  - Assigned Home Address Option

Home Address Auto-configuration

- Currently only works for /64 home prefixes
- The MN sends the interface identifier in the lower 64 bits of the Home Address field in the Home Address option
- The Home Agent fills in the prefix and sends the home address back to the MN.

Security Association Setup

- RFC 3957-like mechanism for MIPv6
- Assumptions
  - The MN depends on a AAA infrastructure for authentication and authorization
  - There is a long lived security association between the MN and the AAA (AAAH server)
- An MN-HA SA is dynamically derived from the MN-AAA SA
  - Based on a nonce generated by the AAAH

Security Association Setup (contd.)

- First BU is authenticated by the AAAH
  - Subsequent BUs are authenticated by the HA
  - A nonce used for key generation is sent by the AAAH in the first binding ack
- Two new mobility options
  - Key Generation Nonce Request
  - Key Generation Nonce Reply

Reachability

- No new mechanism
- DNS Update mechanism as described in draft-ietf-mip6-bootstrapping-split re-used