Revisiting the MIP6 Security architecture

Basavaraj Patil <basavaraj.patil@nokia.com>
Charles Perkins <charliep@wichorus.com>

March 24, 09
IETF74

Background

- Mobile IPv6 [RFC3775] relies on IPsec for securing the signaling between the MN and HA
- RFC3776 and RFC4877 specify the details of how IPsec/IKE/IKEv2 are used with MIP6
- The choice of IPsec as the security protocol for MIP6 is historical and was based on the prevailing thinking in the IPv6 community at that time

Current View

- The choice of IPsec for securing MIP6 signaling was wrong
- This conclusion is arrived by at least those people who have implemented or attempted to implement MIP6 or DSMIP6
- The complexity of implementation and hacks needed to make MIP6 work with IPsec/IKEv2 is very high

So what do we do…

- MIP6 and consequently DSMIP6 can be significantly simplified by unplugging the MIP6 dependency on IPsec/IKEv2
  - Or at the very least have a mode for DSMIP6 which can work without requiring IPsec/IKEv2

- An alternative* security architecture for Mobile IPv6 is proposed to be developed

* Note that alternative here does not automatically suggest RFC4285

Framework of the security architecture

- An initial set of guidelines to consider for the security architecture for MIP6 are as follows:

1. Dependency between MIP6 and the security module should be minimal or at least have well defined (easy) mechanisms in case of interactions
2. Include a mechanism for exchanging keys as part of the solution
3. Consider the reuse of existing security protocols
4. Others?

Proposal

- Work in a design team mode between IETF74 and IETF75 to develop an alternate security architecture for MIP6
- Solution to be proposed to MEXT WG at IETF75
- So if you are interested in working on this problem, contact Charlie and/or Basavaraj