IKEv1 based Mobile IPv6 bootstrapping

Vijay Devarapalli

MIP6 WG, IETF 64

IKEv1 based bootstrapping

- Important for those who don’t have ready IKEv2 implementations yet

- Uses industry standard extensions to IKEv1
  - Today it is possible
    - to run IKEv1 with a VPN gateway
    - authenticate with a separate infrastructure
      - One Time Password, Secure ID, CHAP, etc..
    - setup a tunnel
    - configure a tunnel inner address
  - These are described in some really old IETF specs that expired a long time ago

IKEv1 based bootstrapping

- Home agent discovery
  - DNS
  - DHCP can be used too

- Home Address configuration
  - modecfg extension
    - draft-ietf-ipsec-isakmp-mode-cfg-05
    - MN includes an INTERNAL_IP6_ADDRESS attribute in ISAKMP phase 2 negotiation with address set to 0::0
    - HA responds with a home address using the INTERNAL_IP6_ADDRESS attribute in ISAKMP_CFG_REPLY message
  - DHCPv6 on tunnel protected by a transport mode IPsec SA

IKEv1 based bootstrapping

- Infrastructure based mobile node authentication
  - Hybrid XAUTH
    - draft-ietf-ipsec-isakmp-hybrid-auth-05
  - Followed by XAUTH exchange
    - draft-ietf-ipsec-isakmp-xauth-06
  - Enables use of CHAP, one time passwords, Secure ID, MN-AAAH shared keys, etc.

- Home Agent authentication is based on public keys

- DNS update for the new home address

What do we want to do?

- Do nothing
  - Just say MIP6 bootstrapping with IKEv1 not supported
- Proposed standard
  - No
  - Not possible anyway because of normative dependencies on expired drafts
- Informational?
  - Describe briefly on how it can be done, but leave it industry standard implementations