HIP, IPv6 and Mobility

Some random rants

Pekka Nikander

Ericsson Research

Host Mobility vs Host Multihoming

- **IP addresses are bound to topological locations**
- **Thus, a host in move must change its IP address(es)**
- **To avoid triangular routing, all peers should be informed**
- **The basic security problem:**
  - How does the peer know that the mobile host is really moving?
  - How does it know that it is the same host at the new location?
- **Compare to Host Multihoming:**
  - How does it know that the address(es) belong to the same host?
  - How does it know that the host is reachable at the address(es)?
- **Ergo: From security point of view, host mobility and host multihoming could (and maybe should) be handled together**

Name Spaces and Mobility

- **Current IP (v4 and v6) uses addresses to identify hosts**
- **MIPv6 creates temporary "host routes" at peer hosts**
  - The Mobile Node (MN) sends a Binding Update (BU)
  - The peer creates a Binding Cache Entry, i.e. a temporary route Home Address -> Care-of-Address
  - Result: the Home Address is "shadowed"; all packets destinated to the Home Address are actually sent to the Care-of-Address
  - I.e. the peer performs "source routing" before sending the packet
- **Consequence: the address "ownership" problem**
  - i.e. who is authorized to create BCEs for a given Home Address (see draft-nikander-ipng-address-ownership-00.txt)
- **With separate name spaces this problem doesn't exist**
  - Mobility merely means that the HI -> Address(es) mapping is changed as requested by the HI "owner"

HIP and mobility

- **HIP creates an ESP SA between peers**
- **Thus, the addresses don’t matter so much any more**
  - If the ESP integrity protection verifies OK, the packet was sent by the peer no matter what the src and dst addresses are
  - Thus, by binding IPsec SPIs to HIs instead of addresses, the destination address becomes pure routinting information, and the source address becomes almost obsolete
  - (Consider these as observations, not suggestions)
- **Basic mobility can be made very easy**
  - Using the ESP SA, the mobile node sends the new address
  - The next message is sent to the new address
  - If there is response, the new address is valid
  - If there are no response, we may fall back to the old address
  - Authorization is implicit, no specific protocol needed

Tackling the double jump

- **What if both nodes move at the same time and miss the packets containing the new addresses?**
- **Maybe we can use a link local router as a forwarder?**
  - Piggypack Host Identity to the Neighbor Soliciation message during Duplicate Address Detection (DAD)
  - As a result, the link local router learns the Host Identity, i.e. the Mobile Node’s public key
  - When the Mobile Node moves, it sends a Forwarding Request to the previous link local router, signed by its Host Identity key
- **Remaining problem: How does the local router authenticate the Host Identity during DAD?**
  - Maybe it can run HIP with the Mobile Node (this costs), or
  - Maybe we can use the 64 bit Interface Identifier as a HIT? (see the next slide)

A possibility: HIT in Interface Identifier

- **RFC3041 specifies random Interface Identifiers**
  - 62 of the low order 64 bits of an IPv6 address can be random
- **Maybe we could use these as a short HIT?**
  - I.e. the address itself contains info about the host's public key
  - (Compare this to Mobile IPv6 SUCV / CAM / etc)
- **Benefit: Can be authenticated without any protocol**
  - i.e. no need to do check before receiving a forwarding request
- **Collisions can be resolved if needed**
  - Interface identifier = HASH (Public Key, random number)
  - Host Identity = $\text{SIGN}_{\text{Private Key}}$ (Public Key, random number)
  - Upon collision, generate a new random number
- **Be warned: there may be IPR problems with this scheme**
  - To my knowledge, both Ericsson and Microsoft have filed patent applications that may or may not be related

Backward compatibility

- **For IPv6 hosts that don’t support HIP it is always possible to use standard Mobile IPv6**
- **As a minimal requirement, a stationary HIP host MUST support Home Address destination options**
  - It seems OK to ignore Binding Updates on the cost of suffering from triangular routing
- **A mobile HIP host may either support sending Binding Updates towards non-HIP hosts or rely on a gateway**
  - If it sends Binding Updates, it must also support Mobile IPv6 security mechanisms (that are to be defined)
  - If it relies on a gateway, it will always suffer from non-optimal routing

Stuff to read

- draft-nikander-ipng-address-ownership-00.txt
- draft-perkins-bake-01.txt
- draft-montenegro-sucv-01.txt
- “CAM: Childproof Authentication for Mobile IPv6,” in Computer and Communications Review (CCR), April 2001
- RFC3041
- http://www.tml.hut.fi/~pnr/publications/draft-nikander-ipng-pbk-addresses-00.txt