IPv6

Layer3

Mobility & Security

Deutscher IPv6 Kongress 2012

10/11 May 2012
Frankfurt

Holger.Zuleger@hznet.de

Data network usage

- Usage patterns of data network mobility
  - ≤ 199x Fixed line usage (PC/Server) Ethernet/Dial-in access
  - 200x Fixed mobile usage (Laptop) Ethernet/Dial-in/WiFi
  - 201x Mobile usage (Smartphones/Tablet) 3G/4G/WiFi
  - ≥ 2015 Mobile network usage (Mobile Router Car/Train/Ship)
- Today, mobility is based on Layer 2 technologies
  - WiFi roaming between access points
  - 3G/4G GTP tunnel to GGSN/PGW
- Issues with layer 2 mobility
  - scaling problems
  - suboptimal traffic flow (3G/4G)
  - no mobility between different access technologies (3G/WiFi) or ISPs
- Why not use layer 3 mobility ?

The Locator / Identifier Problem

IP address is used as Identifier **and** Locator

Identifier part

- OS needs a way to map incoming IP packet to application
- Both peers use 5-tuple as endpoint identifier

```
$ netstat -n -t
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 88.198.13.165:43162     74.125.39.125:5269      ESTABLISHED
tcp6       0  10920 2a01:4f8:130:1261::5222 2a00:0:1801:1:216::7744 ESTABLISHED
```

- The application associated with the tuple is shown by `netstat -p`

```
# netstat -t -A inet6 -p
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address        Foreign Address     State       PID/Program na
tcp6       0  10920 2a01:4f8:130:12:5222 2a00:0:1801:12:7744 ESTABLISHED 16450/c2s
```

- If IP address or port is changed, session is stalled
  That's only one reason why NAT (NAPT) is evil (just like stateful firewalls)
- L3 mobility issue: IP address prefix depends on subnet

The Locator / Identifier Problem

IP address is used as Identifier **and** Locator

Locator part

- For scalability reasons IP adresses are aggregated
  Nevertheless the IPv4 full table has about 500,000 prefixes
- Address aggegration is more efficient in IPv6
  Just because of huge address space
  - All customers of one ISP using the same prefix
    DTAG `2003::/19`, VF `2a00::/22`
  - Customer of the same region (pop) are using the same prefix
    e.g. out of one `/32`
  - All subnets of one customer site are using the same prefix
    Out of the same `/48`
- Change of subnet/pop/ISP means change of IP address also
  All active sessions get stuck

Layer 3 mobility solutions

Requirements

- Roaming across different access technologies
  WiFi, WiMAX, UMTS, LTE, fixed
- Seamless handover between layer 3 networks
- Application continuity
  Session persistence
- Reachability of mobile nodes
  Even if they are not connected to the home network
- Mobility of both endpoints

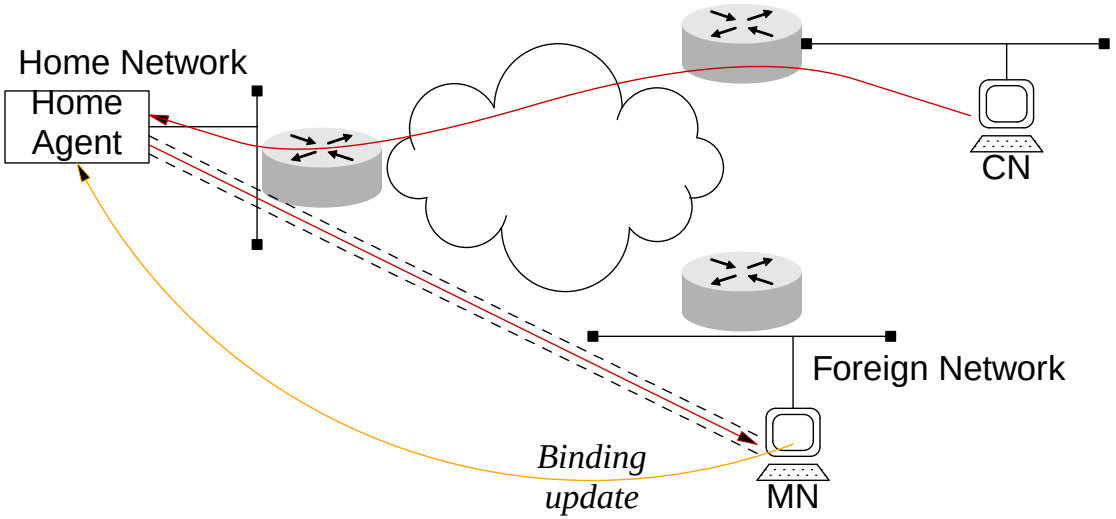
Implementations

- MIP6 Mobile IPv6
- HIP Host Identity Protocol
- And others ...

MIPv6 Definition and Terminology

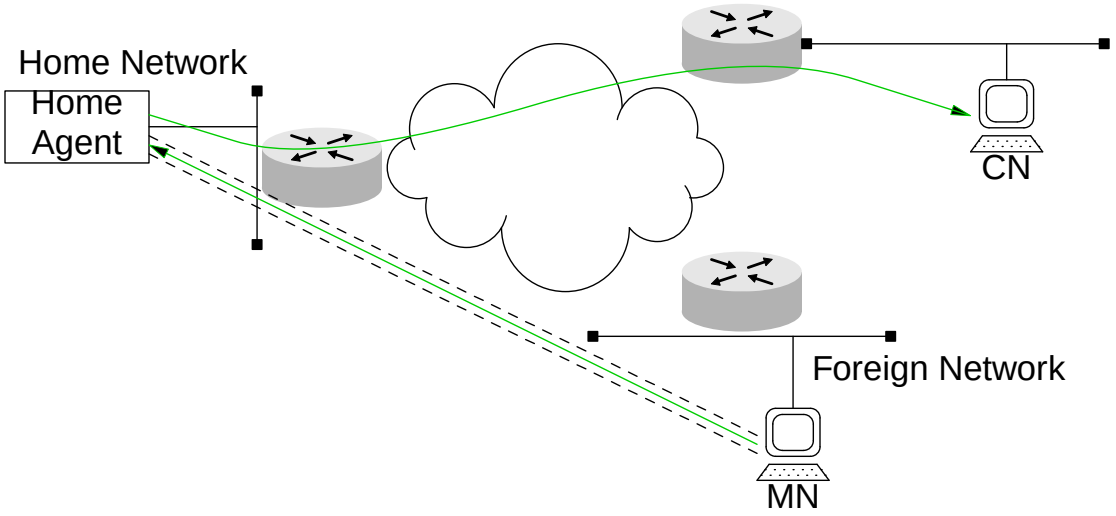
- IPv6 Mobility basics
  - RFC3775/RFC6275: Mobility Support in IPv6 (June 2004 / July 2011)
  - RFC3776: Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents (Updated by 4877)
- Mobile Node (MN)
- Home Address (HoA)
  A (static) IP address out of the mobile nodes home network
- Care of Address (CoA)
  The physical IP address of a MN while visiting a foreign network
- Home Agent (HA)
  A router on the home network which represents the MN
- Correspondent Node (CN)
  A peer node with which a MN is communicating (mobile or stationary)
- Binding
  Association of the home address with the care-of address of a MN

Bidirectional Tunnel Mode (1)



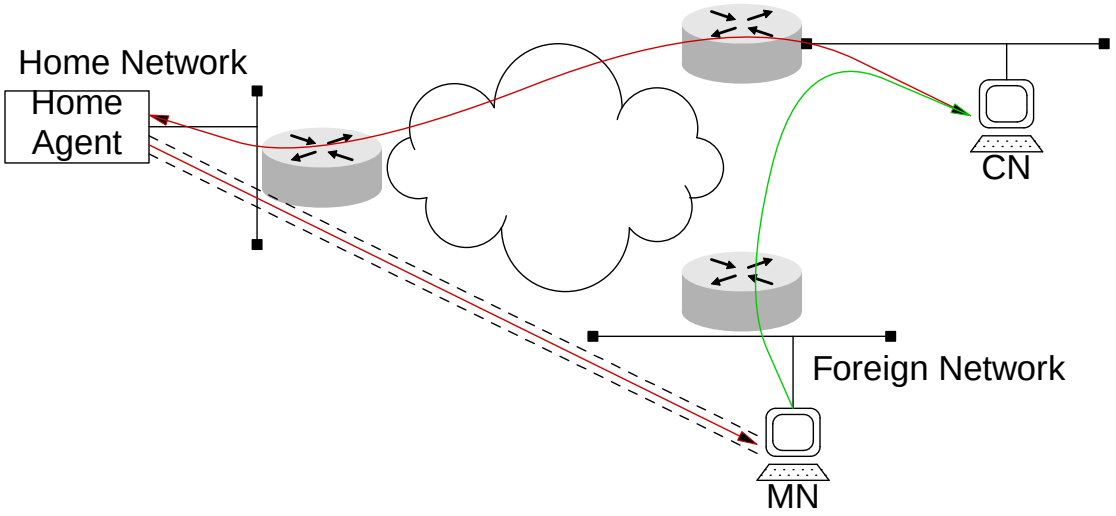
- MN connects to foreign network and gets a CoA
- MN sends binding update to HA
  Should be secured by IPsec ESP in transport mode
- HA uses proxy neighbor discovery (IPv6 equivalent of proxy ARP) to represent the MN in the home network
- All traffic destined to the MN will be encapsulated in a IPv6-in-IPv6 Tunnel and sent to the CoA of the MN

Bidirectional Tunnel Mode (2)



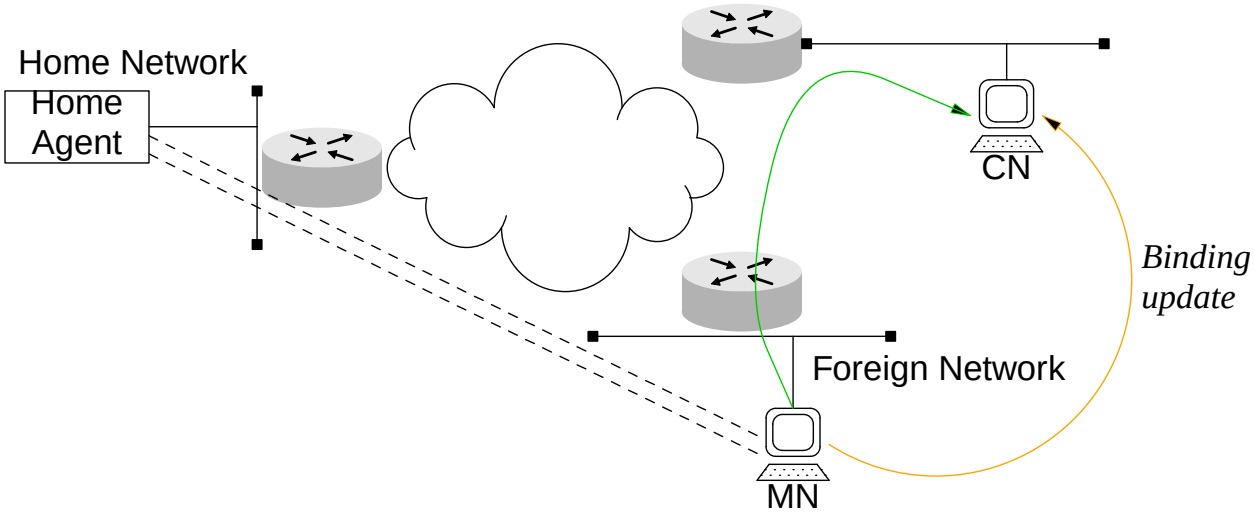
- Traffic from the MN uses the same tunnel in reverse mode
- Results in suboptimal routing, especially if both peers are far away from the home network
- Only HA and MN have to do some special packet handling
  MIPv6 is completely transparent for CN

Triangle Routing ?



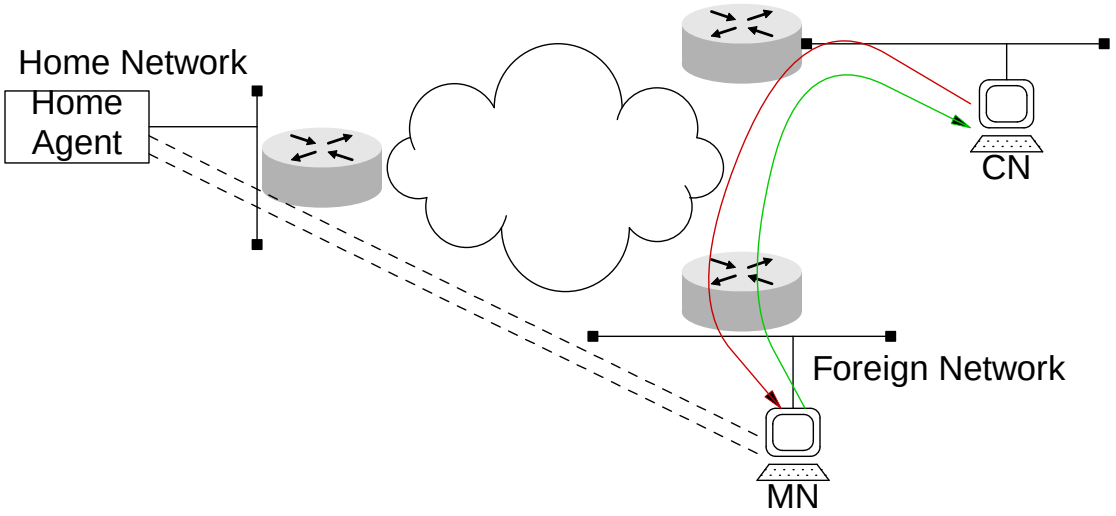
- Traffic from MN is directly sent to CN
- MIPv4 solution
- Problem: Outgoing traffic can’t use the HoA as source address
  Anti-spoofing ACLs at the foreign network usually prevent this
- Suboptimal routing anyway
- MIPv6 Solution: Route Optimization

Route optimization (1)



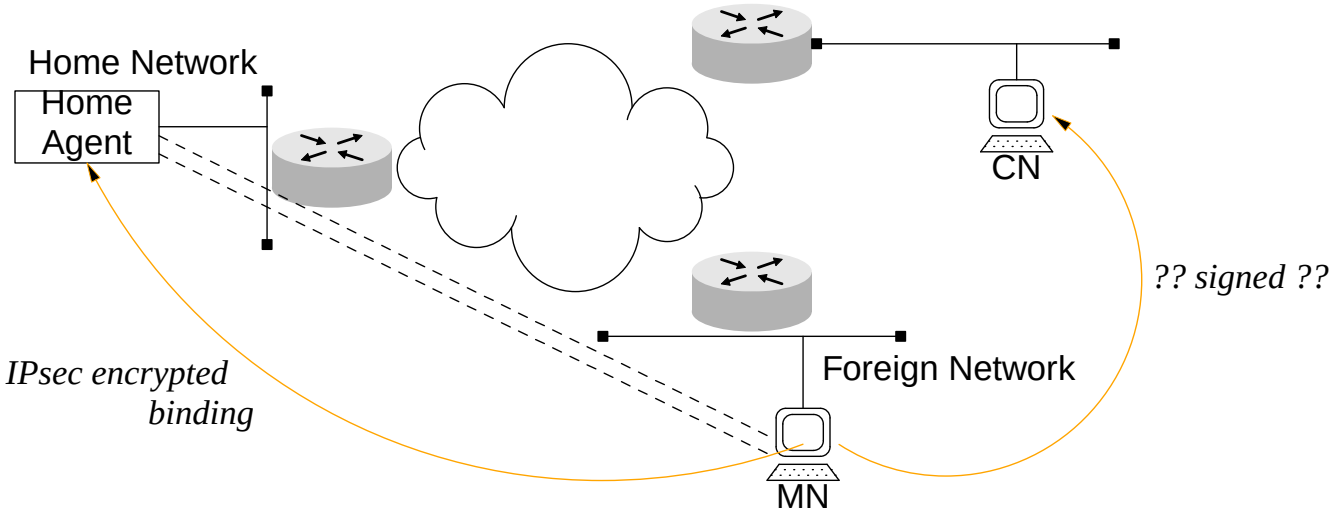
- MN sends binding update to CN
- MN sends traffic to CN with CoA as source address
  This is to bypass the anti spoofing ACLs at the foreign network
- Packet contains an HoA destination option
- CN replaces the source address with the home address before passing the packet to upper layer protocols

Route optimization (2)



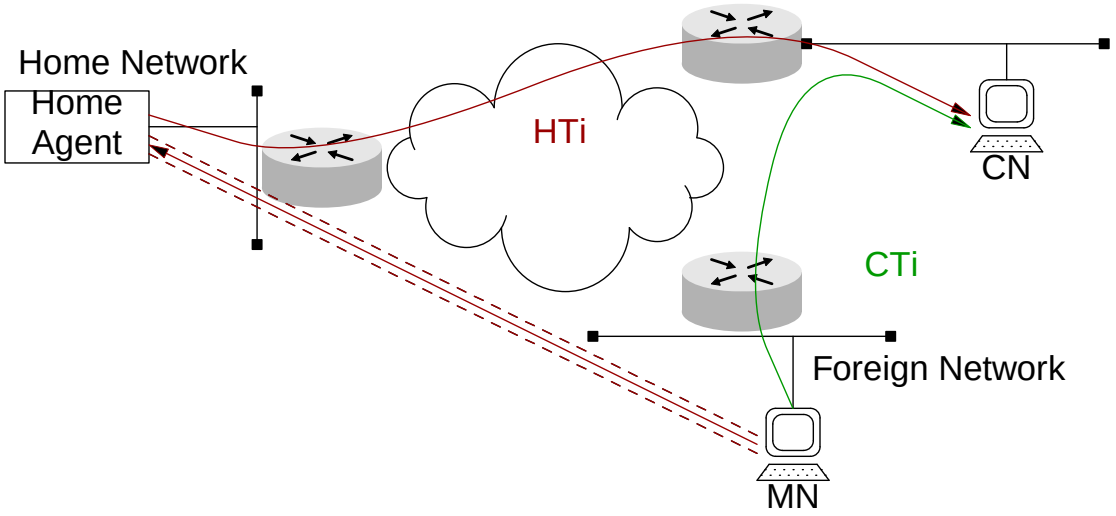
- CN sends traffic to MN with CoA as destination address
- Packet contains a special Routing Header with HoA as second hop
- MN removes the routing header and „forwards“ the packet to the next hop specified by the routing header
- Upper layer protocol is only aware of HoA
- But: Binding update **must** be secured

Secure Binding



- Trust relationship between MN and HA
  IPsec with ESP in transport mode must be used for binding update message
- No trust relation between MN and CN
  Return Routeability mechanism used to prove the reachability of MN

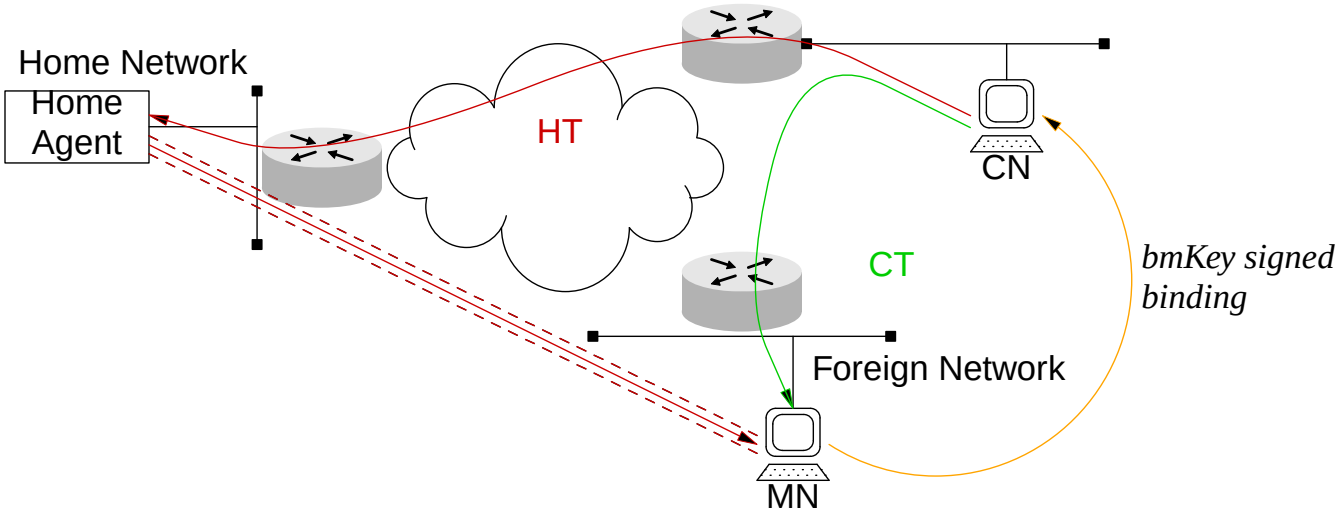
Return Routeability Procedure (1)



- MN sends two messages with a cookie to CN
  - Home Test init (HTi) is sent via HA
    (traffic to HA must be encrypted)
  - Care-of Test init (CTi) is sent directly to CN
- CN uses pre-generated key and nonce to build two keygen tokens
  (Key: random number of 20 octets; Nonce: random octet string of any length)

```
home keygentok    := FIRST (64, HMAC_SHA1 (key, (HoA | nonce | "0")))
care-of keygentok := FIRST (64, HMAC_SHA1 (key, (CoA | nonce | "1")))
```

Return Routeability Procedure (2)



- CN sends keygen tokens and cookies back to MN
  Home Test (HT) and Care-of Test (CT) messages
- MN builds binding message key

  `bmKey := SHA (home keygen token | care-of keygen token)`
- MN sends binding update message signed with bmKey
- CN can prove that the MN is reachable via both paths

MIPv6 Summary

- Two IPv6 adresses used to overcome the Locator/Identifier problem
  - Home address is used as identifier
  - Care-of address is used as locator
- Suboptimal traffic flow if CN does not support MIPv6
- Direct communication between MN and CN is possible
  Return Routeability procedure used to exchange binding key
- Solves most of the security challenges introduced by mobility
  - IPsec has to be used for traffic through the Home Agent tunnel
  - MIPv6 introduces no new security threats
- Extensions to MIP
  - Network based mobility solutions (Proxy Mobile IPv6) RFC5213
  - Dual stack mobility (RFC5555)
  - Multicast Mobility (Multimob WG)
  - Network Mobility (NEMO) RFC3963

Host Identity Protocol (RFC 5201)

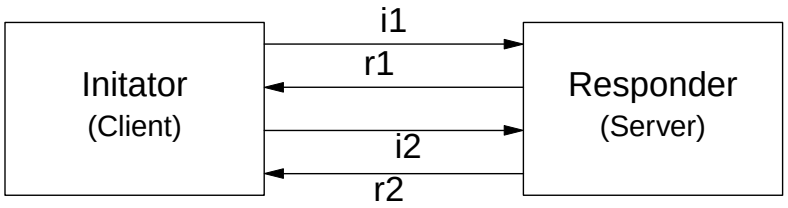
- Yet another locator/identifier split mechanism
- Host based approach
  Some others are network based (e.g. LISP+ALT)
- Enables multihoming
- Mobility
  IPv4 and IPv6
- Secure communication channel
  Simple key exchange protocol for IPsec
- Public key is used as identifier (instead of IP address)
  In fact, a hash of the public key is used
- Adds a new namespace
  Domain Name (User), HIT (Identifier), { IPv4 address | IPv6 address } (Locator)

Host Identifier and HIT

- A host identifier is the public part of an asymetric key (RSA or DSA)
  - Size of identifier depends on key length / algorithm
  - Representation depends on key algorithm
  - A generalized presentation would be more handy
- The host identity tag (HIT) is the sha-1 hash of the host identifier
- A HIT is the 128 bit representation of a host identifier
  - Constant length
  - Same size as an IPv6 address
  - Fits in a socket data structure used by the kernel
  - Represented as a (reserved) IPv6 address
    Overlay Routable Cryptographic Hash Identifier (ORCHID)
  - The ORCHID prefix is `2001:0010::/28` (RFC4843)
- Legacy applications can use the HIT instead of an IPv6 address !
  e.g. `2001:13:10bc:aed3:2a0a:e2f8:a645:6d3c`

HIP Session Setup

- Protocol number 139 is assigned to HIP
- Base exchange
  Just 4 packets to initiate a HIP session



  - Makes HIP DoS resilient
    puzzle question/answer in r1/i2 message
  - Diffie-Hellman Key Exchange
    In r1, i2 packets
  - Authentication
    In i2, r2 packets
- Extended Exchange for IP address registration/update
  For mobile/multihomed hosts
- The HIP protocol is control plane only
  Data plane is IPsec (or SRTP)

HIP and DNS

- HIP can use DNS to map hostnames (FQDN) to a HIP identity
  Distributed Hash Tables (DHT) are also supported
- Client queries for HIP record in addition to an A and/or AAAA record
- HIP RR provides three types of information
  a. The HIP identity, which is the public part of an asymetric key
  b. The HIT (host identity tag), which is a hash of the Hi
  c. Optional a rendezvous server (for mobile hosts)
- Example RR (Mobile Host)

```
xt5.hznet.de.      IN HIP ( 2 2001001310BCAED32A0AE2F8A6456D3C
                     AwEAAeAdP1k64O50S1AptjbshjL+jTd0yeiQFyVu
                     Bb1c09JOKdrl/UrF362MCV4c2T7Bo/7rT8HYRhAb2
                     iVcvm5Bszy07uKU4fNTfUu8r2Nzti1QK8mk194HFZ
                     0IsJmR940MxEXQIO5if2crV/RN2SfinbJUirfRe+H
                     bM3BqdHSdGgTl
                     max.hznet.de. )
```

- DNSSEC should be used for a secure binding between FQDN and HIT
  BTW: The root zone is signed since July 15, 2010 20:50 UTC

HIP and DNS (2)

- HIP Server

```
crossroads.infrahip.net.   HIP ( 2 2001001BA9BEC6A634E58361C07FA990
                           AwEAAcp2OIA68skk+yPtU+UBtvScsntTvknaaXMPmJi
                           4OG2N+yszHOm/DWN7GyYZDPPsUURYWu6r3u7pzIub7J
                           rWXDpYeLIcZmr++D0ENKI9nUs1bPdfgeQTgCu0OBf1K
                           +wRtAxAQaF64rmSP/L666BEZwfTVWYgfiqZrJNcrFwn
                           hvt5 )
crossroads.infrahip.net.   AAAA    2001:708:140:220::7
crossroads.infrahip.net.   A       193.167.187.134
```

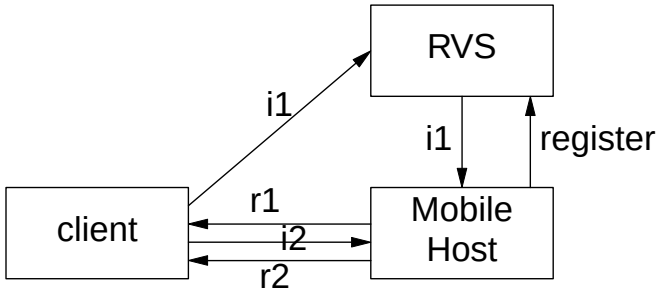
- HIP Mobile Host

```
$ dig +dnssec +noall +answer +multi hip xt5.hznet.de
xt5.hznet.de.  10800 IN HIP ( 2 2001001310BCAED32A0AE2F8A6456D3C
                        AwEAAeAdP1k64O50S1AptjbshjL+jTd0yeiQFyVu
                        Bb1c09JOKdrl/UrF362MCV4c2T7Bo/7rT8HYRhAb
                        2iVcvm5Bszy07uKU4fNTfUu8r2Nzti1QK8mk194H
                        FZ0IsJmR940MxEXQIO5if2crV/RN2SfinbJUirfR
                        e+HbM3BqdHSdGgTl
                        max.hznet.de. )
               10800 IN RRSIG HIP 5 3 10800 20120514041807 20120414041807 52469

max.hznet.de.  10800 IN A    88.198.13.165
               10800 IN RRSIG A 5 3 10800 20120514041807 20120414041807 52469  .
max.hznet.de.  10800 IN AAAA 2a01:4f8:130:1261::2
               10800 IN RRSIG AAAA 5 3 10800 20120514041807 20120414041807 52469
```

HIP Mobility

- Mobile host requires rendezvous server (RVS) for initial reachability
  Mobile host register current locator (IP address) at RVS during base exchange
- Rendezvous server name is (optional) part of HIP DNS record
  Locator hint
- HIP initiator (client) sends first packet of HIP base exchange to RVS
- RVS forwards the packet to the host (if host is actually registered)



- Mobile Host sends update packet to client if IP address is changed
  RVS has to be informed as well
- Similar procedure is used for multihoming

HIP and IPsec ESP

- HIP uses IPsec ESP to carry the data traffic (RFC5202)
  - Pair of SA is bound to Host Identifier; SPI is used as index into SA table
  - No need to transfer the host identifier within each packet
  - Both endpoints have a local database for mapping of SPI to host identifier
- Other mechanism possible but not yet defined
- Only 2 transforms mandatory
  AES with SHA-1 and Null encryption
- IP address could be changed during IPsec session (association)
  - HIP UPDATE message to inform peer
  - Rekeying allowed during IP address change
  - Protocol change possible (IPv4 $\Leftrightarrow$ IPv6)
- Good for mobility
  - MIPv6 no longer needed
  - Session persistence because IP address is no longer used as identifier

HIP as a key exchange protocol (like IKE)

Limitations

- HIP is used for end to end security so transport mode is used
  In fact most implementations use BEET mode (Bound End to End Tunnel)
- Only one SA per host
  - More than one SA possible (e.g. one HI per application) but unusual
  - Not the same granularity as ISAKMP
- No AH, just ESP mode (but with null encryption)

Advantages

- Layer 3 mobility
- No certificates needed
  - HIP uses key as identifier
  - No binding between key and identifier (IP address) necessary
- Only 4 packets required for peer authentication and key exchange
  Same as with IKEv2

HIP References

Documents

4423 Host Identity Protocol Architecture (May 2006)

5201 Host Identity Protocol (April 2008)

5202 Using the Encapsulating Security Payload Transport Format with HIP

5205 Host Identity Protocol (HIP) Domain Name System (DNS) Extension

5206 End-Host Mobility and Multihoming with the Host Identity Protocol

4843 Overlay Routable Cryptographic Hash Identifier (ORCHID)

draft-henderson-hip-vpls
HIP-based Virtual Private LAN Service (HIPLS)

Implementations

InfraHIP / HIPL
Ubuntu, Fedora, CentOS, Android, Maemo, OpenWRT (http://infrahip.hiit.fi/)

OpenHIP
Linux / Windows / Mac (http://www.openhip.org/)

HIP for FreeBSD
(http://www.hip4inter.net/)

Summary

- Two mobility solutions with different focus shown
  - MIPv6: Wide availability, works with any host (OS support)
  - HIP: End to end security and mobility solution
- Host based solution, no network support needed
  Except Home Agent in MIPv6
- Some security threats
  Most of them are similar to threats w/o mobility
- HIP adds end-to-end protection of the traffic
- Minor privacy issues
  Mobile Node is trackable by home agent or rendezvous server
- Anyway, for MIPv6 or HIP to work we need IPv6 capable networks
- So:

Let’s start to rollout IPv6

Questions ?

DNSSEC, IPsec, VoIPsec, XMPPsec, ...

... DKIM, Kerberos, Radius, NTP, DHCP, DNS, ...

... IPv6, Routing, Switching, 802.1x

Holger.Zuleger@hznet.de

CONTENTS