What is HIP ?

A brief introduction to the Host Identity Protocol

5. Aug 2010

Holger.Zuleger@hnet.de

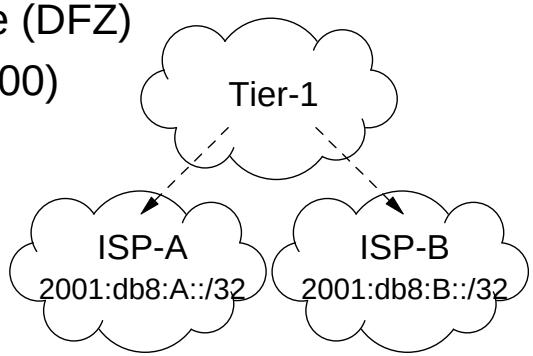
Host Identity Protocol (RFC 5201)

- Yet another locater/identifier split mechanism
  PIP, ILNP, IPNL, TRRP, APT, GSE/8+8, Shim6, LISP(+ALT), MOBIKE, GLI-Split
- Host based approach
  Some others are network based (like LISP)
- Enables multihoming
- Mobility
  IPv4 and IPv6
- Uses public key as identifier
  Or a hash of it
- Adds a new namespace
  Domain Name (User), HIT (Identifier), { IPv4 address | IPv6 address } (Locator)
- Simple key exchange protocol for IPsec

Locater / Identifier

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

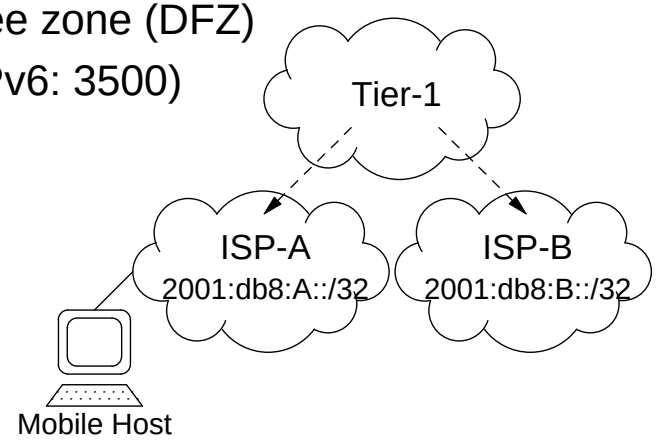
- Identifier
  - OS nedds a way to bind incoming ip packets to application
  - Both ends use 5-tuple as endpoint identifier
  - On IP address change the connection go stale
- Locator
  - Prefix aggregation needed on AS boundary
  - Just a handful prefixes in IPv6 per AS
  - Size of default free zone (DFZ)
    (IPv4: 350000; IPv6: 3500)



Locater / Identifier

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

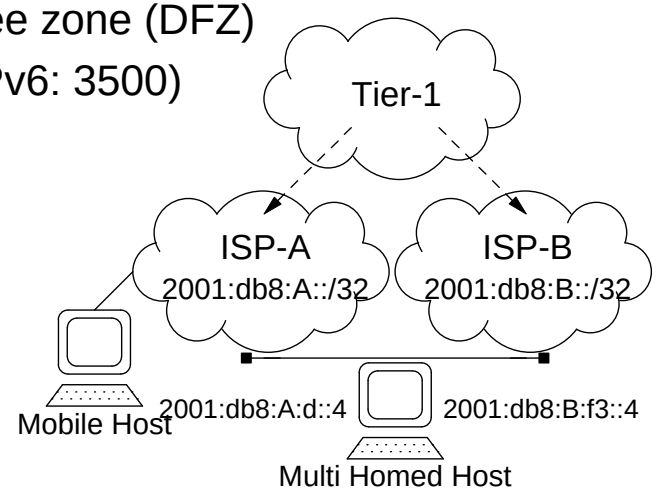
- Identifier
  - OS nedds a way to bind incoming ip packets to application
  - Both ends use 5-tuple as endpoint identifier
  - On IP address change the connection go stale
- Locator
  - Prefix aggregation needed on AS boundary
  - Just a handful prefixes in IPv6 per AS
  - Size of default free zone (DFZ)
    (IPv4: 350000; IPv6: 3500)



Locater / Identifier

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

- Identifier
  - OS nedds a way to bind incoming ip packets to application
  - Both ends use 5-tuple as endpoint identifier
  - On IP address change the connection go stale
- Locator
  - Prefix aggregation needed on AS boundary
  - Just a handful prefixes in IPv6 per AS
  - Size of default free zone (DFZ)
    (IPv4: 350000; IPv6: 3500)

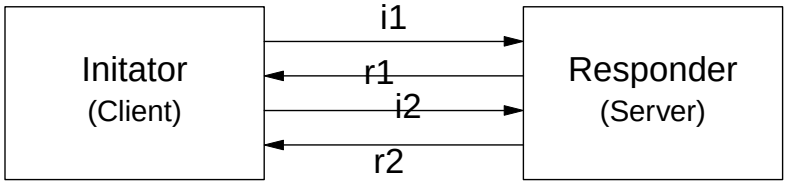


Host Identifier and HIT

- 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 more generalized presentation would be more handy
- The host identity tag (HIT) is the 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
  - Could be represented as an (reserved) IPv6 address
    Overlay Routable Cryptographic Hash Identifier (ORCHID)
  - The ORCHID prefix used is `2001:0010::/28` (RFC4843)
- Legacy applications can use the HIT instead of an IPv6 address

HIP Session Setup

- 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
- Protocol number 139 has been assigned to HIP
- Extended Exchange for IP address registration/update
  For mobile/multihomed hosts
- Diet Exchange (DEX) under discussion (draft-moskowitz-hip-rg-dex-02))
  good to be used by sensor devices or for mac layer security

HIP and DNS

- HIP can use DNS to map hostnames (FQDN) to a HIP identity
- 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 2001001781381AE2B2BC542EEEE53CAB
                      AwEAAb1SN58eG29jZcY8HO2HPQXh6UIfSMvFF+4BM8n
                      S/Za6s2yRU0+wvSMXOHGShe6E3RD2t7uKF9cbsSz4JU
                      5J8YP2/DpJREEGR3AWBXVVcLUq06xS3XmePOvck/oQZ
                      HtNzjRjy11ey5KiH7O6jDwJBXfGuUcpsiI7qHTzu8tJ
                      Va8n
                      max.hznet.de. )
```

- DNSSEC is necessary for secure binding between FQDN and HIT

And now to something completely different...

The Root Zone is signed since
15. July 2010 20:50 UTC

HIP and DNS (2)

- HIP Test 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
```

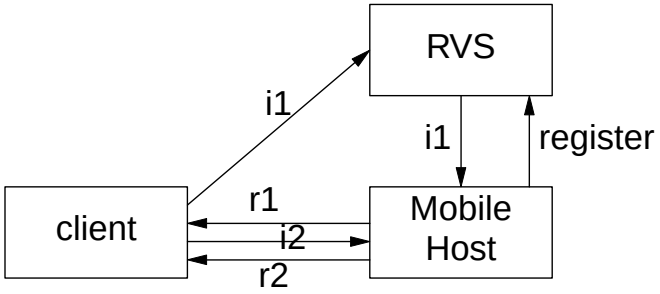
- Mobile Host

```
xt5.hznet.de.    IN HIP ( 2 2001001781381AE2B2BC542EEEE53CAB
                    AwEAAb1SN58eG29jZcY8HO2HPQXh6UIfSMvFF+4BM8n
                    S/Za6s2yRU0+wvSMXOHGShe6E3RD2t7uKF9cbsSz4JU
                    5J8YP2/DpJREEGR3AWBXVVcLUq06xS3XmePOvck/oQZ
                    HtNzjRjy11ey5KiH7O6jDwJBXfGuUcpsiI7qHTzu8tJ
                    Va8n
                    max.hznet.de. )

max.hznet.de.    IN A    213.239.204.36
max.hznet.de.    IN AAAA 2001:6f8:900:2af::2
```

HIP Mobility

- Mobile host needs rendezvous server (RVS) for initial reachability
  Mobile host register his current locator (ip address) at RVS
- 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 uses HIP base exchange to register his address at RVS
- Mobile Host send update packet to client if IP address is changing
  RVS has to be informed as well
  (Proposal to send UPDATE/CLOSE via RVS)

HIP as a key exchange protocol

Similar to ISAKMP/IKE

Disadvantages (Limitations)

- Only transport mode available
  Because HIP is for end to end communication this is intended
- Only one SA per host
  - More than one SA possible (e.g. one HI per application) but unusual
  - Not the same granularity like ISAKMP
- No AH, just ESP mode (but with null encryption)

Advantages

- Just 4 packets needed to authenticate peer and exchange key material
  Same as IKEv2
- No certificates needed
  - HIP uses key as identifier
  - No binding between key and identifier (ip address) necessary

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 addresses could be changed in between a session
  - HIP UPDATE message to inform peer
  - Rekeying allowed during ip address change
  - Protocol change possible (IPv4 ⇔ IPv6) but not defined yet
- Good for mobility
  - MIPv6 no longer needed
  - Session persistence because ip address is no longer used as identifier

Applications of HIP

- Host Mobility
  Even on different transport protocols (IPv4/IPv6)
- Multihoming
- Server load balancing / High Availability
  Shared HI on clustered servers
- End-to-end Security
- Firewall rules based on Host identifier
  Firewall for mobile users
- Long term session persistence
  SSH, IMAP
- Continuous media streaming (Voice/Video) over different L3 networks
  mobile / fixed convergence
- Apples „Back to my MAC“
  Kerberos, TSIG, TLS, IPsec, DDNS, DNS-SD, DNS Push, NAT Traversal
  IPv6 ULA used as Identifer, ...

References

RFC

- 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)

Implementations

InfraHIP / HIPL

Ubunto, Fedora, CentOS, Android, Maemo, OpenWRT (http://infrahip.hiit.fi/)

OpenHIP

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

HIP for FreeBSD

(http://www.hip4inter.net/)

Comparison / Interoperability

http://www.openhip.org/wiki/index.php?title=Interoperability

Questions ?

DNSsec, VoIPsec, IPsec, XMPPsec, SMTPsec, WLANsec ...

... DKIM, Kerberos, IMAP, LDAP, ENUM, SIP, ...

... NTP, DNS, DHCP, IPv6, Routing, Switching

Holger.Zuleger@hznet.de

CONTENTS