Introduction to HIP

Pekka Nikander
Ericsson Research Nomadiclab
Presentation outline

- A Brief History of HIP
- Some architectural background
- Related WGs
- HIP in a Nutshell
- Draft status
- Implementation status
- Summary
A Brief History of HIP

• Discussed briefly at 47th IETF
• Two earlier BOFs: 50th and 51st IETFs
  • No working group formed back then
• Development has happened next to the IETF
  • Active developer community
  • Five interoperating implementations
• HIP base protocol more or less ready
  • More work needed on infrastructure issues
Some architectural background

• IP addresses serve the dual role of being
  • End-point Identifiers
    • Names of network interfaces on hosts
  • Locators
    • Names of naming topological locations
• This duality makes many things hard
• IRTF Name Space Research Group (nsrg) studied the issue without reaching consensus
Related WGs and RGs

- Mobility
  - mip6
  - mip4
  - mipshop
  - mobike
- Multi-homing
  - multi6
- Security
  - ipsec
- ID/loc split
  - nsrg
HIP in a Nutshell

• Integrates security, mobility, and multi-homing
• Opportunistic host-to-host IPsec ESP
• End-host mobility, across IPv4 and IPv6
• End-host multi-address multi-homing, IPv4/v6
• IPv4 / v6 interoperability for apps
• A new layer between IP and transport
• Introduces cryptographic Host Identifiers
The Idea

- A new Name Space of Host Identifiers (HI)
- Public crypto keys!
- Presented as 128-bit long hash values, Host ID Tags (HIT)
- Sockets bound to HIs, not to IP addresses
- HIs translated to IP addresses in the kernel

Diagram:

- Process
- Transport
- Host identity
- IP layer
- Link layer

Labels:

- `<Host ID, port>`
- Host ID
- IP address
HIP as the new waist of TCP/IP
One way to implement HIP

Client app

DNS library

HIT query

HIT

DNS reply

{IP addresses}

HIT

HIT

connect(HIT)

HIP daemon

socket API

TCP SYN to HITs

IPsec SPD

IPsec SAD

convert HITs to IP addresses

Server app

DNS server

TCP SYN to HITs

IPsec SPD

IPsec SAD

convert IP addresses to HITs

Client app

HIP daemon

socket API

TCP SYN to HITs

IPsec SPD

IPsec SAD

convert HITs to IP addresses

Server app

HIP daemon

socket API

TCP SYN to HITs

IPsec SPD

IPsec SAD

convert IP addresses to HITs
Protocol overview

Initiator

I1: HIT$_I$, HIT$_R$ or NULL

R1: HIT$_I$, HIT$_R$, puzzle, DH$_R^+$, K$_R^+$, sig

I2: HIT$_I$, HIT$_R$, solution, DH$_I^+$, {K$_I^+$}, sig

R2: HIT$_I$, HIT$_R$, sig

Responder

ESP protected messages
Internet drafts

- draft-moskowitz-hip-arch-05
  - architecture – sent to RFC editor
- draft-moskowitz-hip-08
  - base protocol – almost ready
- draft-nikander-hip-mm-00
  - mobility & multi-homing – needs work
- draft-nikander-esp-beet-mode-00
  - IPsec ESP extensions
Implementation status

• Five publicly known implementations
  • Boeing Phantom Works, Linux, IPv4 only
  • Ericsson Research Nomadiclab, FreeBSD
  • Helsinki University of Technology, Linux IPv6
  • Andrew McGregor, Python user level
  • Sun Labs Grenoble, Solaris?
• Fourth interop testing going on here in MPS
Summary

• New cryptographic name space
  • Hosts identified with public keys
• Integrates security, mobility, multi-homing
• Initial ideas at the IETF in late 1999
• Five interoperating implementations
• Base specifications start to be mature
  • Architecture draft at RFC editor