HIP-RG meeting, IETF-63

Using HIP with Legacy Applications (draft-henderson-hip-applications-01.txt)

August 5, 2005

Pekka Nikander (presenting)
Tom Henderson

Draft scope

- How can one use HIP without recompiling applications?
- Informational-- should not be required for HIP interoperability
- Does not cover HIP-aware applications and API
  - assumes that applications are not recompiled for HIP
- This work re-homed to HIP-RG based on HIP-WG discussion at IETF-62

Changes since last draft

- Pekka added security section to draft
  - when IP addresses or LSIs are used, much depends on the implementation details of the system
  - when DNS is used, depends on whether the DNS maps are secure

Implementation experience

Most implementation experience uses unmodified applications

- Boeing kernel implementation returns IP addresses (v4 and v6) to apps
- Boeing user-space (Windows XP IPv4) implementation returns LSIs to apps
- HIP support being added to Berkeley OCALA proxy (returns LSIs to IPv4 applications)
- HIPL, Ericsson implementations use HITs and IPv6 applications
- Ericsson also uses LSIs for IPv4 applications

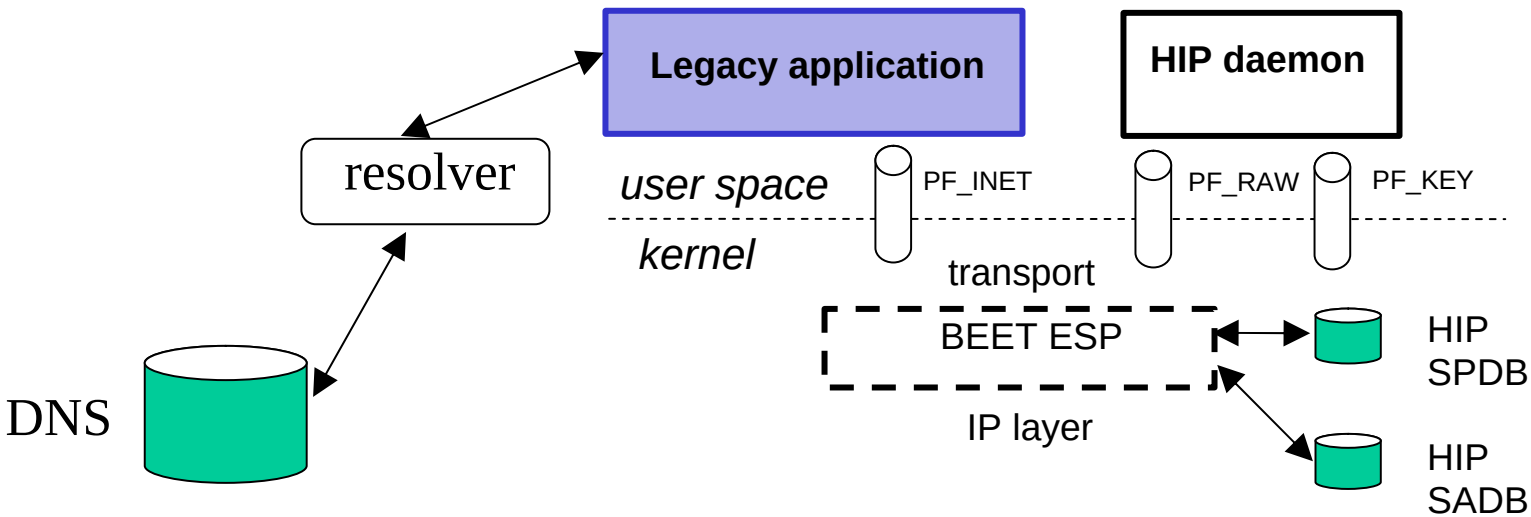
Next steps

- Draft is mostly complete at this time
- May eventually be suitable for Informational RFC
- Will consider whether part of HIP Experiment Report, or maintain as separate draft

Backup

Architecture and terminology

Referral: When an application passes what it assumes to be an IP address to another application on another host (e.g., FTP PORT command)

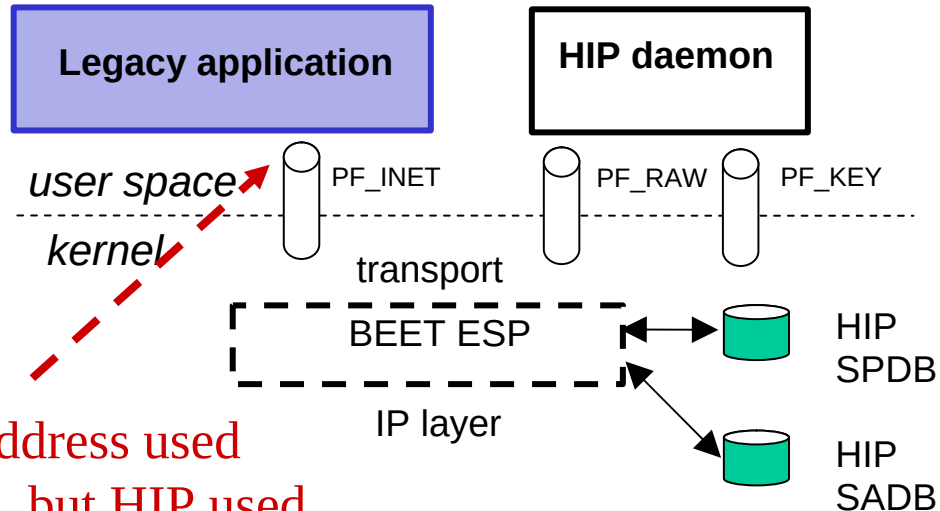


Possibilities

How does application or user cause HIP to be invoked?

1. Applications use IP addresses
2. Applications use DNS names
3. Applications use IP address-sized HITs or LSIs

1. IP address



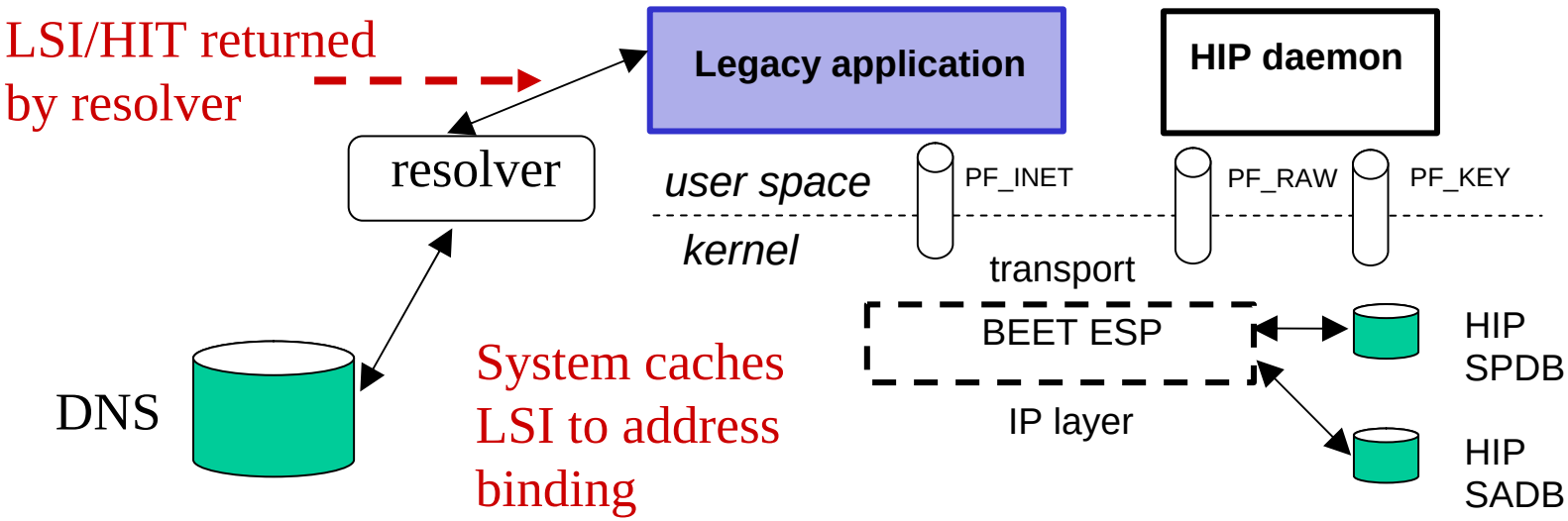
IP address used here, but HIP used by system

- Manually configure address-to-HIT binding
- Opportunistically (don't care about peer HIT)
- Use reverse+forward DNS lookup

Pros: Naturally supports application-level referrals

Cons: May have weaker security properties than use of HITs (depends on several factors); may be cumbersome (manual configuration)

2. DNS hooks



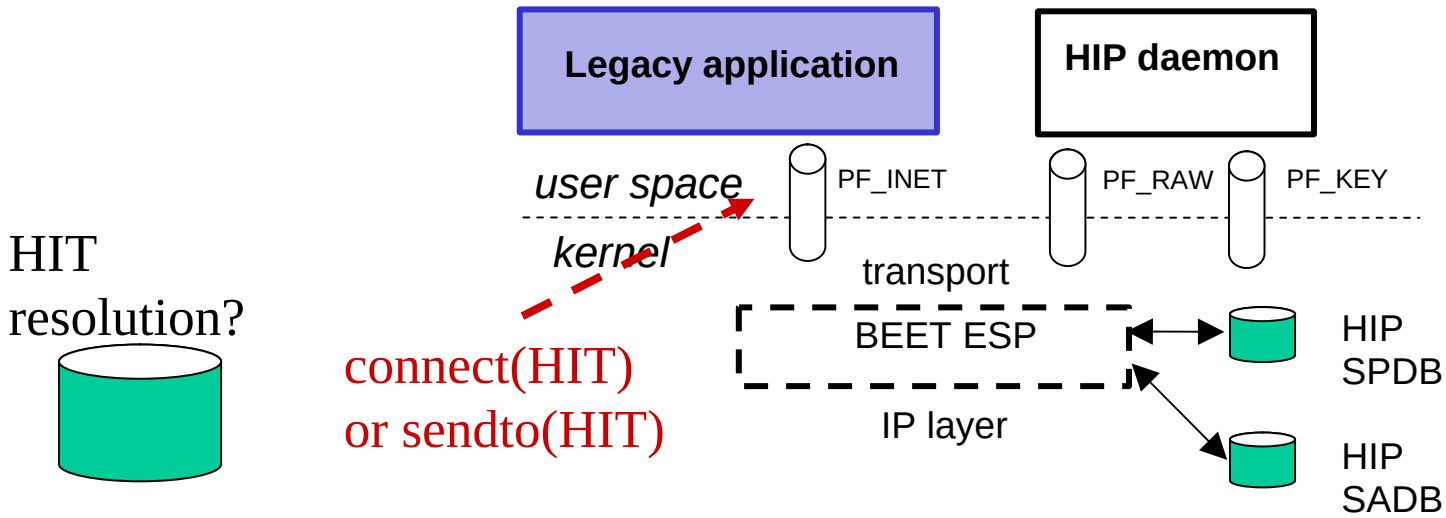
Options:

1. Have resolver return LSIs (HITs) instead of IP addresses
2. Use HIP-suffix in FQDN (e.g., www.ietf.org.hip)

DNS issues

- Should we spoof IP addresses in resolver calls?
  - i.e., replace A record IPs with LSIs or HITs
- Referrals
  - Non-routable LSIs do not support referrals
  - Routable LSIs may work, but may require infrastructure support
- When should system garbage-collect the LSI to address bindings?

3. Connecting to HITs directly



Pros: Most direct and secure naming semantics

Cons: Application-level referrals; HIT-to-address resolution; distinguishing between HIT and IPv6 address