

Experience with the Host Identity Protocol for Secure Host Mobility and Multihoming

- HIP overview
- HIP implementation experiences
 - Implementation by Henderson, Ahrenholz and Kim at Boeing Phantom Works
- Performance analysis

HIP Overview

- A cryptographic, statistically unique identity for a networking stack
- Decouple transport and network layers—layer 3.5
- Transport and application connections are bound to host identities instead of IP addresses
- Integration with IPsec ESP

- HIP handshake can replace IKE in IPsec
- Handshake is 4-way and stateless—much lighter than IKE
- Built-in DoS protection (cookie challenge)
 - Initiator has to solve n bits of cookie, n can be varied

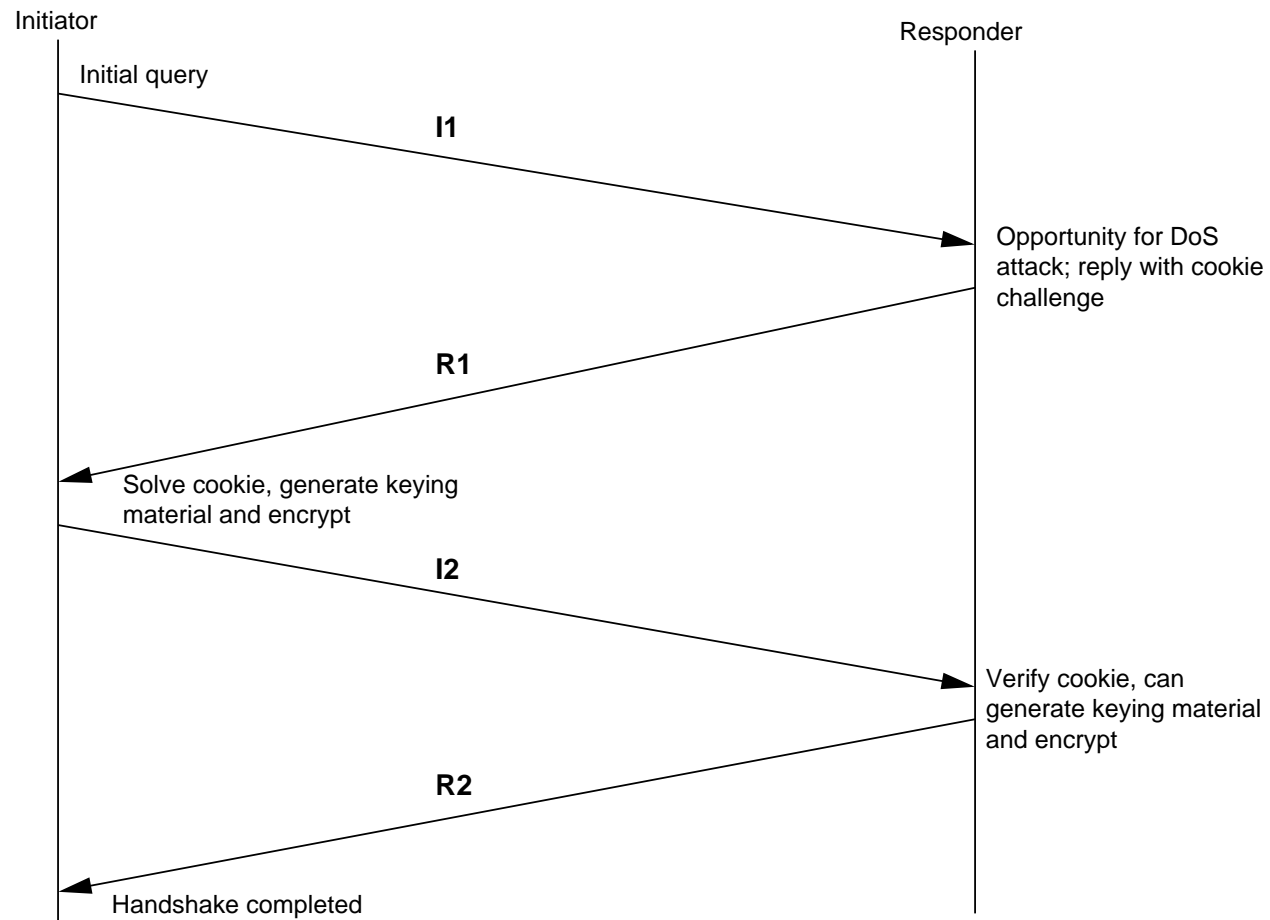


Figure 1: HIP handshake

Implementation

- Implemented on top of FreeS/WAN on Linux 2.4 kernel
- FreeS/WAN provides IPsec IKE, ESP and AH for Linux
- Implementation replaces IKE with HIP
- Also small changes to kernel module: use host identity instead of static IP address

- HIP LSI replaces IP address in local system calls
- HIP daemon monitors host's active network interfaces for address change, notifying other ends of active connections if that happens
- Local information is also updated
- Sockets API should be augmented with a new socket option (request for HIP)
- Also, a `getlsibynname ()` call instead of `gethostbyname ()`

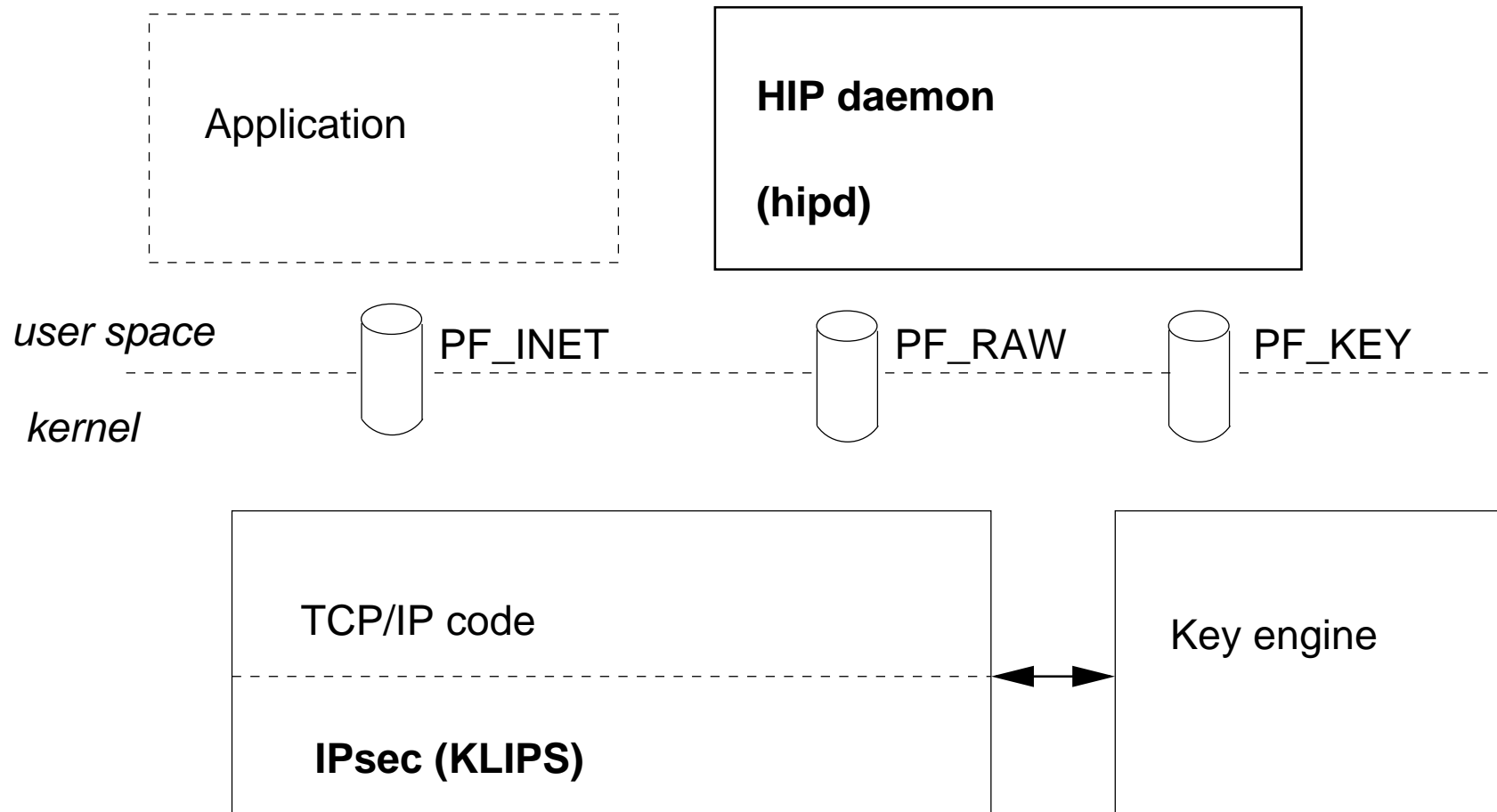


Figure 2: HIP implementation structure

Performance

- HIP exchange takes a bit under 1 sec in a 266MHz laptop
- Responder time affected by the cookie challenge
- Most of the time is spent in DSA signing
- The time does not seem to be prohibitive

Conclusions

- FreeS/WAN architecture not the best possible for HIP
- Key management might cause the need for a MIP-like “home agent”
- Relationship of HIP and MobileIP?