Network Working Group
Internet-Draft
Intended status: Experimental
Expires: February 21, 2010

J. Melen
J. Ylitalo
P. Salmela
Ericsson Research NomadicLab

August 20, 2009

Host Identity Protocol-based Mobile Proxy
draft-melen-hip-proxy-02

Status of this Memo

Copyright Notice

Abstract

This document defines a HIP-proxy node that enables non-HIP host to communicate with HIP host through a proxy node without requiring changes to the non-HIP host.

Table of Contents

1. Introduction

The Host Identity Protocol (HIP) [RFC5201] has been designed to allow hosts to preserve existing security associations and higher-layer protocol sessions by defining host mobility and multihoming mechanisms [RFC5206]. Specifically, a mobile or multihomed host that changes its IP address, or acquires new addresses, can securely notify its corresponding peers of the new address(es). Similarly, a mobile HIP-aware host can update information about its current IP address(es) by updating records in HIP Rendezvous Servers [RFC5204] or other name services.

This draft describes HIP protocol extensions that allow a non-HIP host to use the services of a HIP-aware proxy node and have capabilities to communicate with a HIP host and to be mobile when moving together with the HIP-proxy node. The HIP-proxy node functions as a middle node that will encapsulate and decapsulate the packets that are destined to a HIP host or to a non-HIP host behind another HIP-proxy. The HIP-proxy will handle all the HIP signaling on behalf of the non-HIP host and thus no modifications are required to the connection end-points.

The HIP-proxy node MUST reside on the normal routing path of the packets. HIP-proxy will capture and encapsulate/decapsulate packets coming from or going to non-HIP host. The encapsulation procedure will also apply encryption as specified by the HIP association that is created during the HIP base exchange. HIP-proxy node MAY also be aided by the DNS resolver in order to resolve the destination host's host identity. While the HIP-proxy resides on the routing path of the non-HIP host's outgoing traffic, it MAY also function as a DNS proxy in which case all the DNS queries will pass through it.

2. HIP-Proxy Architecture

This section describes the extensions for the basic HIP [RFC5201] that are required to support proxying of the traffic.

2.1. Assigning Host Identity to non-HIP host

The HIP-proxy MAY generate a Host Identity for each legacy host it will represent in the network. In this case, the HI is bound to a certain IP address. The HIP-proxy will create point-to-point tunnel between the HIP-proxy and HIP end host. The generation of each new Host identity MAY be triggered by DHCP or it MAY be generated manually before hand.

Alternatively, the HIP-proxy MAY generate a Host Identity for a group of network hosts. In this case, the HI is bound to a certain network prefix. The HIP-proxy will create point-to-multi-point tunnel between the HIP-proxy and HIP end-host.

The difference on whether the to create a single host identity to represent multiple hosts or whether to create a one identity per IP address is a trade-off between the whether the HIP-proxy needs to carry the IP header between the HIP-proxy and the HIP-node or not.

2.2. Registering Host Identity IP address mapping to RVS

HIP-proxy MAY register the non-HIP aware host's IP address in to rendezvous server for HIP hosts or proxies using the same rendezvous system. The HIP host creates a opportunistic I1 packet (destination

HIT null) and includes the IP address of the non-HIP aware host as a parameter to the I1 packet. HIP host's I1-packet is forwarded via rendezvous system to the non-HIP host's proxy using the IP address of the non-HIP host. When the I1 packet reaches the HIP-proxy that registered the address that HIP-proxy will respond to the I1 packet with R1 including the non-HIP aware host's IP address as a parameter and the HI that represents non-HIP aware host.

The rendezvous system SHOULD verify that the HIP-proxy is authorized to add the mapping between non HIP IP address and HI before accepting the registration of the mapping. Rendezvous system SHOULD NOT add any HI non-HIP IP mappings that it cannot verify to belong to that HIP-proxy as this might cause unwanted behavior in the routing system.

2.3. Registering Host Identity to DNS

The HIP-proxy MAY register the Host Identity (HI) resource record in to the DNS as defined in the [RFC5205]. The HIP-proxy will associate

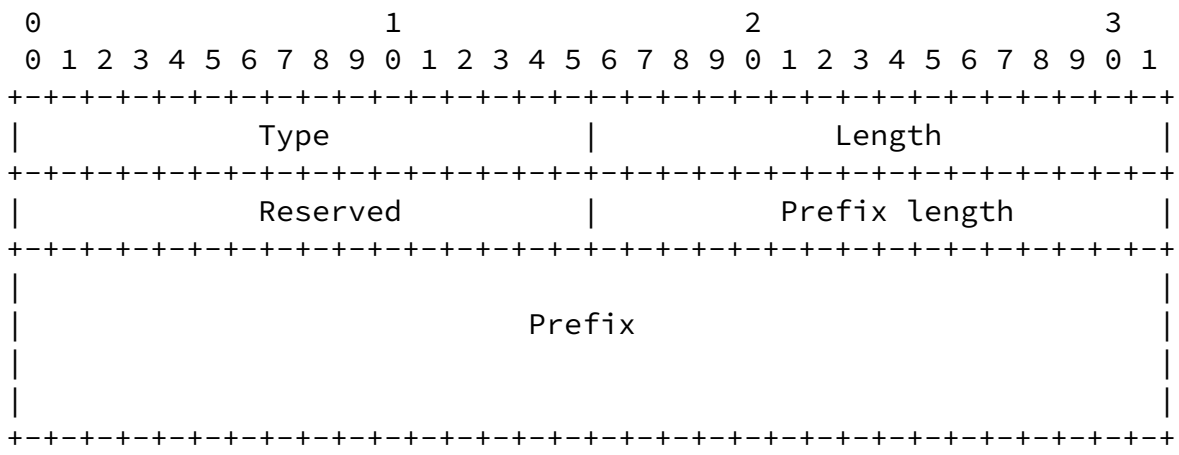
the HI with the FQDN of the non-HIP host. When the HI is resolved from the DNS the resolving host will get the HI and address of the host or HI and address of the rendezvous server of the HIP-proxy depending on the local configuration policy.

3. Parameters and packet formats

In this section we define the additional HIP parameters needed to carry the non-HIP host information between the two proxies or proxy or HIP node.

3.1. Proxy information parameter

The Proxy Information (PINFO) parameter is used to carry the IPv4 or IPv6 address the non-HIP node is using. Thus, the parameter will have different type value depending on whether the parameter is carrying the information of the initiator proxy's network or information of the responder HIP-proxy's network.



Type [TBD by IANA:
PINFO_INITIATOR: 989 =
(2^9 + ... + 2^6 + 2^4 + ... + 2^2 + 2^0)
PINFO_RESPONDER: 991 =
(2^9 + ... + 2^6 + 2^4 + ... + 2^0)
]
Length 20
Prefix Length Length of the prefix or length of netmask
Prefix an IPv6 prefix or an IPv4 address in "IPv4-Mapped IPv6 address" format

4. Packet processing

4.1. Opportunistic I1

4.1.1. Rendezvous node

The rendezvous node parses the PINFO_RESPONDER parameter and searches all the registered HIP-proxy client contexts through for an prefix

that was in the received PINFO_RESPONDER parameter.

4.1.2. HIP-proxy or HIP-node

The responder verifies the I1 as specified in the [RFC5201]. As a additional step the responder MUST verify that the prefix included in to the PINFO_RESPONDER parameter of I1 packet contains a prefix that belongs some Host Identity which the host owns

4.2. I1

The responder verifies the I1 as specified in the [RFC5201]. As a additional step the responder MAY verify that the prefix included in to the PINFO_RESPONDER parameter of I1 packet contains a prefix that belongs to the host identity represented by the destination HIT field in the HIP protocol header.

4.3. R1

The initiator verifies the R1 as specified in the [RFC5201]. As a additional step the initiator MUST verify that the prefix included in to the PINFO_RESPONDER parameter of R1 packet contains a prefix that it sent out in the PINFO of the I1 packet.

The initiator SHOULD first try to find the right HIP association using the responders HIT or HI. If previous check returns empty HIP association, then the initiator SHOULD check if it has sent any opportunistic I1s and if any of those contains a matching prefix to the prefix in PINFO_RESPONDER parameter in received R1 packet.

After parsing and verification of the R1 packet the initiator will add mapping between the HI and the prefix provided by the PINFO_RESPONDER in to the HIP association context.

4.4. I2

The responder verifies the I2 as specified in the [RFC5201]. As a additional step the responder MUST parse the prefix included in to the PINFO_INITIATOR parameter of I2 packet and add a mapping between the HI and prefix in to the HIP association context.

4.5. R2

The initiator verifies the R2 as specified in the [RFC5201]. No additional information is included in to the R2 message.

4.6. Data packets

4.6.1. Sending data over ESP SA

When receiving data packets from non-HIP node that are destined to a host that is either HIP or another HIP-proxy node the HIP-proxy will capture the packet and remove the IP header and send it through the ESP SA.

4.6.2. Receiving data over ESP SA

When receiving data packets from ESP SA the HIP or HIP-proxy node will reconstruct the original IP header and send it back to IP stack for further processing.

5. Security Considerations

Address theft by registering a invalid non-HIP IP address HI mapping. The Rendezvous node should verify that the IP address claimed by the HIP-proxy is really residing behind HIP-proxy.

6. IANA Considerations

7. Acknowledgments

A number of people have contributed to the text and ideas. The list of these people include Pekka Nikander, Petri Jokela, Raimo Vuopionpera, and Jari Arkko. Our apologies to anyone whose name is missing.

8. Normative References

[RFC5201] Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, "Host Identity Protocol", RFC 5201, April 2008.

[RFC5204] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 5204, April 2008.

[RFC5205] Nikander, P. and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", RFC 5205, April 2008.

[RFC5206] Nikander, P., Henderson, T., Vogt, C., and J. Arkko, "End-Host Mobility and Multihoming with the Host Identity Protocol", RFC 5206, April 2008.

Authors' Addresses

Jan Melen
Ericsson Research NomadicLab
JORVAS FIN-02420
FINLAND

Phone: +358 9 299 1
Email: jan.melen@nomadiclab.com

Jukka Ylitalo
Ericsson Research NomadicLab
JORVAS FIN-02420
FINLAND

Phone: +358 9 299 1
Email: jukka.ylitalo@nomadiclab.com

Patrik Salmela
Ericsson Research NomadicLab
JORVAS FIN-02420
FINLAND

Phone: +358 9 299 1
Email: patrik.salmela@nomadiclab.com