Network Working Group
Internet-Draft
Expires: September 7, 2006

J. Lindqvist
TKK

March 6, 2006

Establishing Host Identity Protocol Opportunistic Mode with TCP Option
draft-lindqvist-hip-opportunistic-01.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies an alternative opportunistic mode for the Host Identity Protocol (HIP). The opportunistic mode is initialized by adding a 128 bit Host Identity Tag (HIT) as a TCP option to a TCP SYN packet. The mode allows a TCP connection to be established directly without a timeout delay in the case the peer does not support HIP.

1. Introduction

Host Identity Protocol (HIP) architecture [HIPARCH] replaces the identity function of IP addresses. When the Host Identity Protocol (HIP) is used, Host Identities (HI) are used to identify hosts. IP addresses are used only as locators. In practice, a Host Identity (HI) is a public key of a public/private key pair. Because the public keys can be of different sizes, they are most of the time represented in a condensed form; a hash-based digest of a HI is called a Host Identity Tag (HIT). To authenticate peers and create the necessary IP-layer state, HIP defines a key negotiation state setup protocol called the base exchange. The base exchange can be used to establish IPsec ESP Security Associations [HIPESP], for example.

The base exchange specification [HIPBASE] describes how to use HIP when the peer's HIT is known. The HIT can be preconfigured or fetched from DNS [HIPDNS], for example. If the peer's HIT is not available, the base exchange can be initiated in opportunistic mode. The HIP base exchange specification specifies syntax for packets in opportunistic mode. However, the base exchange specification does not describe the handling of exceptional situations, for example, if the peer does not support HIP.

In this document, we specify an alternative way for initiating HIP opportunistic mode using a new TCP option. The motivation for the approach is that TCP provides a fallback mechanism: if the peer does not support HIP, a normal TCP handshake is done.

The use of TCP option instead of other alternatives (e.g. IP option) is also motivated by recent research that shows TCP options are widely accepted. Only 0.2 % of servers in the conducted research did not respond to TCP SYN packets with an arbitrary TCP option. [MEDINA]

2. Terms and Definitions

We assume that the readers are familiar with the terms and definitions given in [HIPBASE], hereafter referred as the HIP base specification.

2.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2.2. Definitions

HIP TCP option: A TCP option which includes the Initiator's HIT sent in TCP SYN segments.

3. Extensions to TCP and HIP

This section presents the format for the new TCP option called the HIP TCP option. A short outline how this TCP option is processed is also given.

3.1. HIP TCP option

Instead of sending an opportunistic HIP I1 packet, an implementation MAY send a TCP SYN segment that includes the following option.

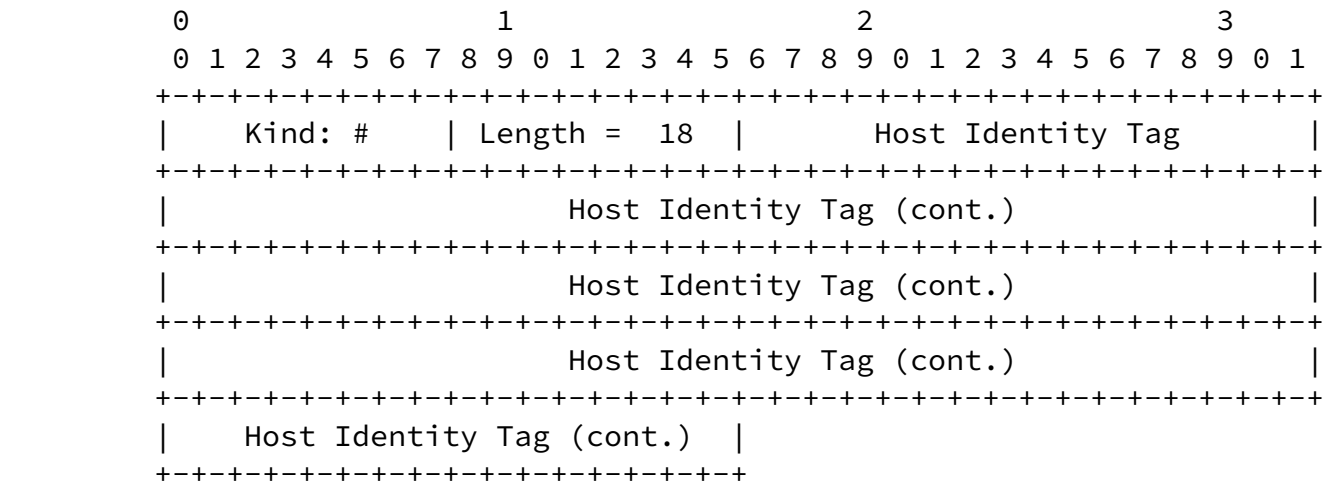


Figure 1

Kind: TBD. See the section on IANA Considerations.

Length = 18.

The format of the Host Identity Tag is defined in [HIPBASE]. The HIT is the Initiator's HIT as in a regular I1 SRC HIT field.

3.2. Opportunistic Mode Processing

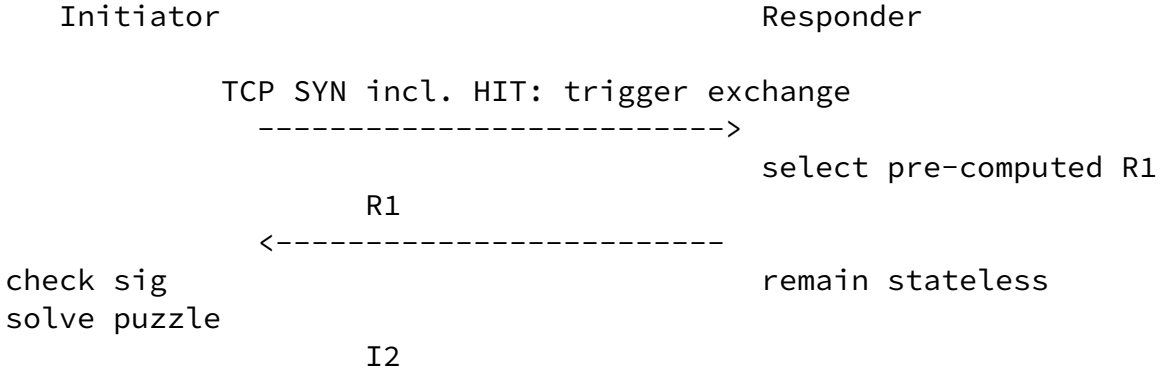
A recipient that implements this specification SHOULD interpret the HIP TCP option defined above as if it had received a corresponding opportunistic I1 packet. In such a case it MAY ignore the TCP SYN segment and reply with an R1. This causes the peer to retransmit the TCP SYN segment once the HIP connection has been established. However, the Responder SHOULD NOT create any state at the TCP level before the base exchange is completed. The approach used for processing the TCP segments has the same Denial of Service resistance motivation as in the HIP base protocol. We do not want to create unnecessary state in the Responder before verifying with the puzzle that the Initiator is sincere.

4. Overview of Opportunistic Base Exchange

This section presents the opportunistic base exchange initiated with the TCP option.

4.1. Opportunistic Base Exchange

The opportunistic base exchange is illustrated below. The R1, I2 and R2 defined in the HIP base specification. TCP SYN is defined in [RFC0793]. The packets contain other parameters in the HIP messages not shown in this figure.



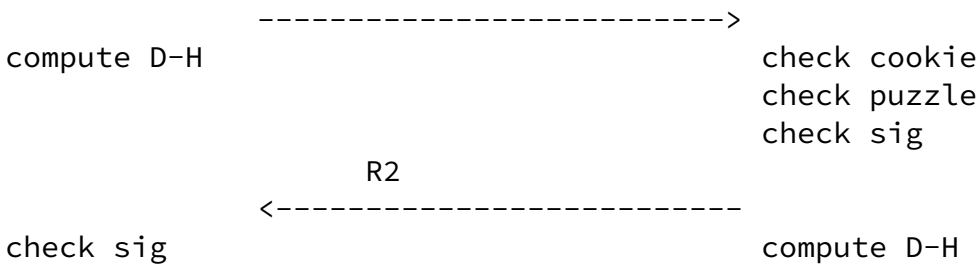


Figure 2

The Initiator starts the opportunistic mode by sending a TCP SYN. The TCP SYN segment includes the HIP TCP option defined above.

When the Responder processes the TCP SYN packet and notices the HIP TCP option, the Responder SHOULD act as if it had received an opportunistic HIP I1 packet. If the local policy allows, the Responder sends an R1 as defined in the HIP base specification. The Initiator's HIT is taken from the HIP TCP option. If the local policy does not allow opportunistic base exchange, a NOTIFY message with BLOCKED_BY_POLICY parameter SHOULD be sent, as defined in the HIP base specification.

The rest of the messages (I2 and R2) are defined and processed according to the HIP base specification.

After R2, the Initiator MUST retransmit the TCP SYN segment in order

to establish a TCP connection.

Other possibilities such as peers sending TCP SYN packets simultaneously are handled as defined in [RFC0793].

5. Open Issues

5.1. Piggybacking

The piggybacking of TCP to HIP control messages was removed from this document. A separate document for describing a generic approach is planned to be written. A fundamental problem with the piggybacking approach is that the TCP messages starting from TCP ACK may contain

data. The data should be encrypted. We could concatenate ESP to I2 and R2, but this approach was removed even from the current base specification. However, we could resend the TCP SYN concatenated to I2. This way, we would not need to encrypt the TCP segments, but only optionally sign them.

5.2. NATs

How does the approach described above work with NATs? If we need to do UDP encapsulation [HIPNAT], is there any point to use the TCP option for opportunistic mode?

5.3. Rendezvous Extension

The Rendezvous Server extension specification [HIPRVS] does not currently cover opportunistic mode.

6. Acknowledgments

Pekka Nikander picked the idea from floating around at the IETF corridors, and handed it over to the present author. Pekka Nikander and Miika Komu have given detailed comments, which have had considerable impact on this document. Lars Eggert provided information on the acceptability of TCP options in today's Internet.

7. Security Considerations

The opportunistic mode is vulnerable to man-in-the-middle attacks, because the Responder's Host Identity is not known before connection initiation. Additionally, the opportunistic mode provides a fallback mechanism to unencrypted TCP. The fallback mechanism can mislead the user to think that the connection is encrypted when it is not. Thus, applications SHOULD notify the user when the fallback mechanism is used.

8. IANA Considerations

Values in the TCP Option Kind Field are assigned following an IESG approval or Standards Action process [RFC2780].

IANA has not assigned an experimental value for TCP Option Kind field. Thus, the use of an experimental value requires IESG Approval [RFC3692].

9. References

9.1. Normative References

[HIPBASE] Moskowitz, R., Nikander, P., and P. Jokela (editor), "Host Identity Protocol", draft-ietf-hip-base-04 (work in progress), October 2005.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2780] Bradner, S. and V. Paxson, "IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers", BCP 37, RFC 2780, March 2000.

[RFC3692] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", BCP 82, RFC 3692, January 2004.

9.2. Informative References

[HIPARCH] Moskowitz, R. and P. Nikander, "Host Identity Protocol Architecture", draft-ietf-hip-arch-03 (work in progress), August 2005.

[HIPDNS] Nikander, P. and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", draft-ietf-hip-dns-03 (work in progress), October 2005.

[HIPESP] Moskowitz, R., Nikander, P., and P. Jokela (editor),

"Using ESP transport format with HIP",
draft-ietf-hip-esp-01 (work in progress), October 2005.

[HIPNAT] Schmitt, V., Pathak, A., Komu, M., Eggert, L., and M. Stiemerling, "HIP Extensions for the Traversal of Network Address Translators", draft-schmitt-hip-nat-traversal-00.txt (work in progress), February 2006.

[HIPRVS] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", draft-ietf-hip-rvs-04.txt (work in progress), October 2005.

[MEDINA] Medina, A., Allman, M., and S. Floyd, "Measuring the Evolution of Transport Protocols in the Internet", ACM SIGCOMM CCR Volume 35 Issue 2, April 2005.

Author's Address

Janne Lindqvist
Helsinki University of Technology (TKK)
P.O. Box 5400
Espoo FIN-02015 TKK
Finland

Phone: +358 9 451 5851
Email: janne.lindqvist@tkk.fi
URI: http://www.tml.tkk.fi/

Intellectual Property Statement

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.