POSITION PAPER

HIP Middlebox Traversal

Hannes Tschofenig, Aarthi Nagaraja, Vesa Torvinen

Abstract
The Host Identity Protocol is a signaling protocol that adds another layer to the Internet model and establishes IPsec ESP SAs to protect subsequent data traffic. HIP also aims to interwork with middleboxes such as NATs and Firewalls). This document investigates this aspect in more detail.

Key words:
Internet, HIP, Middlebox, NAT, Firewall

1. Introduction

The Host Identity Protocol has a base exchange mechanism that is used to quickly authenticate the hosts, exchange the keys to protect the rest of the Base Exchange and the payload and to form the security associations. All data packets exchanged between the two end hosts, following the base exchange, experience IPsec ESP protection. HIP hosts use the security parameter index (SPI) value to compress the HIT in the payload packets.
To allow IPsec protected traffic to traverse a NAPT it is either possible to provide UDP encapsulation or to allow the NAT to participate in the signaling message exchange. A number of proposals have been seen in the past (e.g., [4], [5] and [6]). Firewall traversal has the unplesant property that the forwarding path might not need to be symmetric with respect to the middlebox. A number of working groups have encountered this problem, such as Midcom, PANA and NSIS, and tried to design their solution with respect to this problem.
This proposal gives a summary of a more detailed IETF draft in preparation where a generic middlebox security solution for HIP is envisioned.

2. Proposal Overview

The design of the HIP protocol allows middleboxes to intercept HIP signaling messages and to learn <Dst-IP>, <SPI>, <Protocol> information for subsequent use as packet filters or NAT binding. This was enabled by including the respective parameters in a non-encrypted fashion into the protocol, unlike in other protocols such as IKEv2.

How a HIP aware NAT can use HIP to establish a NAT binding and to establish security relevant state (using hash chains, secret splitting and delayed authentication) is shown with SPINAT in [7].
To deal in addition with Firewalls (and other middleboxes) the following requirements need to be addressed:

1. *Interception* - A middlebox needs to be able to efficiently intercept the HIP signaling messages to learn the required parameters (such as SPI values and HITs). Furthermore, the established flow identifier which is mapped to a certain action (e.g., packet filtering in case of a Firewall) needs to use the <Dst-IP>,<SPI>, <Protocol> to identify packets belonging to a particular flow.
2. *Authentication* - Many middlebox traversal issues do not have any security at all. HIP aware NAT/FW must be able to authenticate the requesting HIP nodes before creating a NAT binding or a Firewall pinhole.
3. *Authorization* - A HIP aware NAT/FW must be able to authorize the requesting HIP nodes using identity independent or identity dependent methods.
4. *Denial of Service attack resistance*. – The authentication and authorization mechanisms should not introduce new DoS attacks at the middlebox.
5. *Registation Procedure* - A Firewall might require authentication and authorization of one of the end point prior to allow signaling (and data traffic) to bypass. Depending on the architecture and environment this step might be optional.
6. *Avoiding unwanted traffic* - In the wireless environment an end host might want to stop receiving unwanted traffic. A signaling protocol is needed to indicate which traffic to receive and which traffic should be dropped. As such, it must also be assumed that end-to-end communication is not, as such always possible prior to the interaction of the end hosts.
7. *Soft-state Nature* - To deal with failures and route changes it is important to design a protocol in such a way that state allocated at middleboxes times-out after a certain amount of time. Periodic transmission of refresh messages is therefore required.

2.1. HIP base exchange and NAT

HIP base exchange consists of messages I1, R1, I2 and R2. Messages I1 and R1 are used to initiate the state establishment and messages I2 and R2 are used to create the actual security associations and to form the keys. All messages carry a standard HIP header with the HIT of the initiator and the HIT of the receiver. It must be noted that IPsec SAs are unidirectional and hence two SPI values (for the Initiator and for the Responder) need to be negotiated. Subsequently, message I2 carries the SPI(I) and message R2 carries the SPI(R).
A HIP aware NAT/FW needs to inspect the HIP base exchange to learn the destination IP address, SPI and protocol type. The HIT values are also required and can subsequently be used to verify future signaling messages. The approach chosen by SPINAT is also relevant here which requires the usage of hash chains.
For authorization SPKI certificates may turn out to be useful since the Host Identities might be ephemeral and anonymity for the end hosts is an important aspect.

2.2. HIP base exchange and Firewalls

NATs force messages both in the forward and the reverse paths to flow through the NAT. This makes the interception mechanism for NATs much easier compared to that of the firewalls. In the presence of generic middlebox (or firewalls in paricular) or a topology with a mixture of NATs and firewalls, routing asymmetry needs to be considered. Firewalls are unable to intercept the SPI values as messages I1 and I2 flow in a different path as compared to messages R1 and R2. For instance, SPI(I) value is sent in message I2 which could traverse through the FW(R) of the receiver alone. However, FW(I) of the initiator would most need it. Hence new solutions need to be sought for tackling the routing asymmetry problem with respect to the firewalls and flow identifier interception. These solutions have to be handled with out changing the existing HIP base exchange (significantly). This can be challenging especially when the middleboxes are not aware of each other and more complex firewalls.

2.3. HIP readdressing and NAT/Firewall

Even after the HIP base exchange is finished, a NAT/FW still needs to keep updating its state for the flow identifier in case of IP address change of the end host. For example, whenever a HIP endpoint roams and informs its peer about the new IP address, communication between the HIP Initiator and the Responder takes place. This requires updating the IP address of the state at FW(I) and updating the SPI(R) at the FW(R). Routing asymmetry may cause added complications here as well at the time of updating state information. Middleboxes must authorize state modifications to avoid a number of attacks including redirection, black-holing or third-party flooding. A desired property in this case is sender invariance which states: "A party is assured that the source of the communication has remained the same as the one that started the communication, although the actual identity of the source is not important to the recipient." (Section 3 of [8]).

2.4. HIP Registration Protocol

Middleboxes might need to authenticate and authorize signaling initiators prior to allow bypassing of signaling messages. A protocol is needed to convey this information to the middlebox. As such, it is necessary to deal with the general protocol design issues, such mutual authentication capability, Denial as Service attack resistance and efficiency with regard to the number of roundtrips. Furthermore, it is helpful if the end-to-end protocol and the Registration protocol support the same credentials. These requirements motivate to reuse the HIP protocol for the purpose of authentication, authorization and the establishment of a security association. Note, however, the establishment of IPsec security association is not necessary. Other concepts of HIP (such as the shim layer between the transport and the network layer) are not relevant in this context.

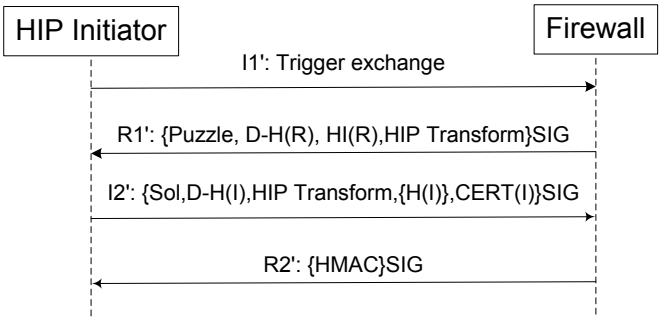

Figure 1: HIP Registration Protocol

Figure 1 shows the simplified HIP exchange with the establishment of IPsec SA negotiation removed. The usage of authorization certificates is not shown. To deal with mobility it is necessary to periodically refresh the state at the firewall. The update of packet filters can either be sent directly to the firewall or indirectly with the help of an end-to-end HIP exchange. The former might be necessary for a data receiver installing packet filters to prevent unwanted traffic from consuming an expensive wireless resource where the data receiver might get charged for.

3. Conclusions

For a long time the focus of HIP was solving problems effecting mainly the two endpoints. The research group will also address middlebox traversal using HIP. To avoid including a HIT into every data packet and to provide end-to-end protection of data traffic IPsec ESP is used between the end points. Unfortunately, IPsec protected data traffic is known to cause problems with middleboxes (particularly with regard to NAT traversal). Middleboxes need to participate in the HIP signaling exchange to allow these devices to perform their function. This interaction requires certain security goals to be met. A solution can be complicated by a number of factors including routing asymmetry, combination of different types of middleboxes and state updates due to mobility. This proposal tries to raise attention of the communitity based on a strawman proposal.

4. Acknowledgements

This document is a byproduct of the Ambient Networks Project, partially funded by the European Commission under its Sixth Framework Programme. It is provided “as is” and without any express or implied warranties, including, without limitation, the implied warranties of fitness for a particular purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Ambient Networks Project or the European Commission.

5. References

[1] Moskowitz, R., Nikander, P., Jokela, P. and T. Henderson: "*Host Identity Protocol*", draft-ietf-hip-base-00.txt (work in progress), June 2004.
[2] Ellison C., Frantz B., Lampson B., Rivest R., Thomas B., Ylönen T., “*SPKI Certificate Theory*”, RFC 2693, September 1999
[3] Maler, E., Philpott, R. and P. Mishra, "*Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1*", September 2003.
[4] Kivinen, T., "*Negotiation of NAT-Traversal in the IKE*", draft-ietf-ipsec-nat-t-ike-08.txt (work in progress), February 2004.
[5] A. Huttunen et al, A., "*UDP Encapsulation of IPsec Packets*", draft-ietf-ipsec-udp-encaps-07.txt (work in progress), Jan 2003.
[6] Kaufman, C., "*Internet Key Exchange (IKEv2) Protocol*", draft-ietf-ipsec-ikev2-14.txt (work in progress), May 2004.
[7] Ylitalo, J., Melen, J., Nikander, P. and V. Torvinen, "*Re-thinking Security in IP based Micro-Mobility*", 7th Information Security Conference (ISC-04), Palo Alto,", September 2004.
[8] "*Deliverable D6.1: List of selected problems*", Automated Validation of Internet Security Protocols and Applications (AVISPA), IST-2001-39252, Deliverable v1.0, November, 2003.