

Network Attachment and Address configuration using HIP

Seppo Heikkinen, Hannes Tschofenig, Boaz Gelbord

Abstract

The Host Identity Protocol introduces a public key based host identifier and a lightweight protocol for establishing IPsec SAs. This paper discusses the possibility of using HIP as a protocol for network attachment which includes the procedure of exchanging configuration information to establish connectivity for the end host.

Key words:

Internet, HIP, configuration, DHCP

1. Introduction

In HIP [3] parties exchange a total of four messages that result in the SA between the entities. This exchange also takes into account the possibility of denial of service and makes use of puzzles to impose some computational burden on the initiator of the communication in order to prove the legitimacy of its intentions. In HIP hosts have host identities which have cryptographic characteristics and can be used to provide security properties to the message exchange.

This proposal suggests to

- use cryptographic identities for networks based similar to the host identities used by HIP. This seems to be an approach which provides minimal organisational and administrative overhead when configuring networks.
- enhance the protocol exchange to piggyback some additional information with the messages. Namely, DHCP alike messages (see [1] and [2]) can be included and they can benefit from the integrity protection provided by HIP. The benefit of including these address configuration messages already in the HIP base exchange is mainly efficiency. This approach was already considered in other protocols, such as IKEv2 [5].
- use mechanisms for non-identity-based authorisation. Since we assume identifiers for networks might be anonymous (i.e., not available in a directory) or even be ephemeral, it is necessary to provide a solution for the case where the identifier is not known to everyone. Therefore, we consider the usage of SPKI certificates [4] or the usage of SAML assertions [5]. Note that the aspect of compensation can still be solved in the traditional way (when subscription-based access is desired). For alternative means of network access the usage of credential-based authorization seems to be an applicable concept (see also [7] and [8]).

2. Proposal Overview

Figure 1 depicts the HIP message exchange enhanced with the proposed modifications.

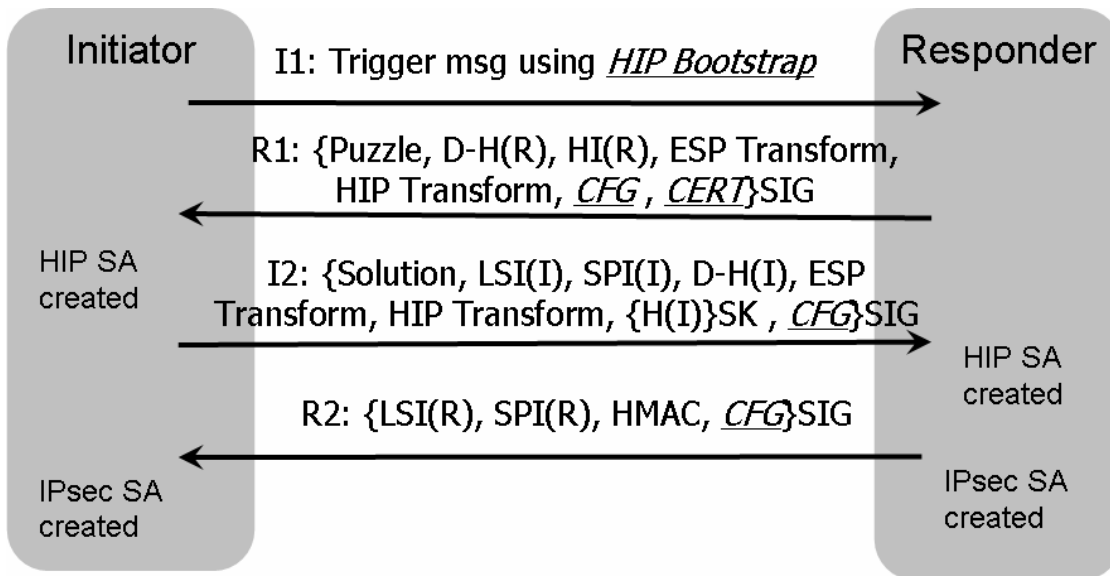


Figure 1: Enhanced HIP Exchange

The message I1 needs to incorporate a discovery mechanism. One feasible approach is to use a link local broadcast to a specific multicast address. A number of other approaches are possible, as discussed in a number of IETF working groups. The selection of the best discovery mechanism is left for further study.

Since the Initiator does not know the identity of the neighbouring responder it is necessary to utilise the HIP Bootstrapping procedure. Section 7.6 of [3] mentions the possibility for a HIP Bootstrap Packet. This mechanism is reused in the I1 message in the case that the Initiator does not know the HI/HIT of the Responder. This packet might be self-signed or signed by a known trust anchor.

Furthermore, as a modification to the base HIP exchange the Initiator might not be in possession of a configured IP stack and as such it has to use the same mechanism as in DHCP. The source IP address of the I1 packet would be the unspecified IP address and the destination address would be the link local multicast address. It is, however, possible to consider an enhanced case, where a CGA-type of approach is taken and the Initiator sends the interface identifier part and subsequently the Responder receives subnet prefix that allows the Initiator to form the address and provide proof of ownership.

The message R1 uses the client-puzzle concept to prevent some denial of service attacks by moving an adjustable amount of computational. Careful selection of the issued challenge is important to prevent a denial of service attack against the initiator. This message can also provide basic configuration which does not require computation actions on the responder side. The responder is still stateless after returning this message.

After receiving R1, the Initiator learns the HI, HIT and CERT from the responder. The Initiator returns the I2 after solving the puzzle. I2 might already include, for example, a DHCP Request protected with the HIP SA and the digital signature.

With I2 the Responder is able to authenticate the Initiator based on the digital signature. Furthermore, a HIP SA is created at the Responder side. The Responder (either directly in case of a DHCP server or indirectly as part of a DHCP Relay) provides the desired configuration information. The response by the DHCP server is returned with the final base HIP exchange message R2.

After a successful completion of the described message exchange the Initiator is equipped with configuration information and both entities might have authenticated each other (if non-ephemeral host identities have been

used). Furthermore, with the established IPsec between the Initiator and the Responder it is possible to protect subsequent signalling messages exchanged between these two entities. Such signalling messages might include further DHCP messages or Quality of Service signalling messages.

If the Initiator uses a non-ephemeral host identity then authorisation of the Initiator by the Responder is possible. The Initiator could also be able to authenticate the Responder in a particular context, in a company or in a corporate. However, in the public Internet with a large number of Responders (and Responders can represent networks such as WLAN hotspots) this task is not simple. With the usage of ephemeral host identities authorisation based on host identities this task is pointless. The concept of composition introduces additional complexity in this area. The authorisation could be provided with either with SAML assertions [5] or it would also be possible to use SPKI certificates [4]. As such, they could be used with non-ephemeral identities, but the real benefit comes from the possibility of using them with ephemeral identities.

3. Conclusions

The described proposal uses HIP to convey configuration messages between entities. This enables the parties to establish an IPsec SA as well exchange configuration information that can be used for providing IP level connectivity. As DHCP messages are used it's possible to provide other kinds of information as well. In addition, some subsequent signalling can be done after the establishment of SA. Inclusion of authorisation information in the form of assertions makes it also possible to authorise ephemeral identities if privacy issues are of concern.

As part of this work a number of open issues have been identified which will be addressed in the near future as part of the Ambient Networks Project.

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] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins and M. Carney: "*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*", RFC 3315, July 2003.
- [2] R. Droms: "*Dynamic Host Configuration Protocol*", RFC 2131, March 1997.
- [3] Moskowitz, R., Nikander, P., Jokela, P. and T. Henderson, "*Host Identity Protocol*", draft-ietf-hip-base-00.txt (work in progress), June 2004.
- [4] Ellison C., Frantz B., Lampson B., Rivest R., Thomas B., Ylönen T., "*SPKI Certificate Theory*", RFC 2693, September 1999
- [5] Maler, E., Philpott, R. and P. Mishra, "*Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1*", September 2003.
- [6] C. Kaufman: "*Internet Key Exchange (IKEv2) Protocol*", Internet draft, Internet Engineering Task Force, March 2004. Work in progress.
- [7] Juha P.T. Koponen, Pekka Nikander, Juhana Räsänen, and Juha Pääjärvi, "*Internet access through WLAN with XML encoded SPKI certificates*," in Proceedings of NordSec2000, October 12-13, Reykjavik, Island, October 2000.
- [8] Matt Blaze, John Ioannidis, Sotiris Ioannidis, Angelos D. Keromytis, Pekka Nikander, and Vassilis Prevelakis, "*TAPI: Transactions for Accessing Public Infrastructure*," in Proceedings of Personal Wireless Communications, PWC2003, Venice, Italy, September 23-25, 2003, pp. 90-100, Springer, September, 2003.