POSITION PAPER

Advanced HIP-based Firewall Traversal

Hannes Tschofenig, Vesa Torvinen, Pasi Eronen

Abstract

This paper investigates the possibility to establish security associations between the data sender and one (or more) intermediate middleboxes to address some open issues for standard path-coupled NAT/Firewall traversal. We provide some thoughts on mobility handling and address the aspect of data origin authentication and an even more secure version - source authentication.

Key words:

Internet, Signaling Protocol, HIP, Data Origin Authentication, Source Authentication, Firewall Traversal

1. Introduction

The HIP protocol introduced an identifier for an end host - the Host Identity (HI) which is a cryptographic identity. The hash of the Host Identity, the Host Identity Tag (HIT), is used by IPv6 applications as a replacement for the IPv6 address. For IPv4 applications a shorter version, the LSI, using 32 bits is used.

HIP also aims to interact with middleboxes by allowing intermediate devices to process HIP messages. Unlike IKE or IKEv2 HIP allows intermediate devices to inspect and cryptographically verify some payloads carried inside the protocol messages. This, for example, allows providing a solution for NAT traversal whereby a HIP aware NAT device uses the <SPI> <Protocol> <Dst-IP> triplet instead of the standard NAT binding. This approach is elaborated in SPINAT [4].

To also address other types of middlebox, such as Firewalls, additional aspects, such as a separate registration procedure with the Firewall or routing asymmetry has to be considered. The usage of HIP to deal with general middleboxes is dealt with in [3]. As a consequence, the middlebox is able to install firewall pinholes based on IPsec protected traffic. The classification provided by the Firewall is based on the <SPI> <Protocol> <Dst-IP> triple.

The above described approaches suffer from two problems:

a) Standard Firewall packet filters do not provide cryptographic verification of the injected data traffic.
b) End host mobility and IP address change in general requires another signaling message exchange with the Firewall(s) to update the installed packet filter (or in case of a NAT binding to modify the mapping).

In other IETF working groups, such as Next Steps in Signaling (NSIS), the aspect of mobility in relationship with middlebox was subject to extensive investigations (see, for example, [7]). The limitations of standard packet filter establishment and end host mobility was discussed in [8].

Establishing packet filter information at devices along the path provides some security against off-path adversaries injecting data packets if they are unaware of the established firewall pinhole. This might provide enough security protection for many scenarios or environments. However, due to the absence of per-packet authentication man-in-the-middle attacks of malicious nodes along the path cannot be prevented by installed packet filters. Figure 1 shows such a scenario where a malicious node injects data traffic although it is unable to tamper with the signaling message itself since it is protected (for example, if we assume that a secure middlebox traversal protocol is used). This might lead to security problems especially in ad-hoc networks where some intermediate nodes are untrusted.

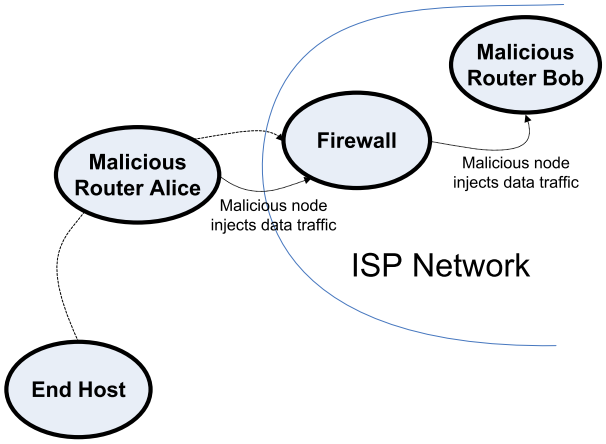

Figure 1: General Limits of Firewall Signaling

2. Protocol Proposal

As previously described standard packet filters typically consist of the classical five tuple (src/dst IP address, src/dst port number and transport protocol). It is, however, possible to construct an identifier which acts as a substitute for these identifiers. During discussions in context of the IPv6 Flow Label (which is a three tuple <Src-IP><Dst-IP><Flow-Label>) at the NSIS mailing list it was mentioned that it would also be possible to utilize the home address instead of using the end point identifiers for an installed flow identifier in case of mobility. Avoiding locators (IP addresses) within packet filters simplifies mobility handling by avoiding state updates at the shared path. To completely avoid IP addresses one could use an IPv6 extension header to embed a 128 bit random number (or even larger) which serves as a substitute for both network and transport identifiers. Using only the 21 bit IPv6 Flow label cannot provide uniqueness to serve as a flow identifier without considering the source and destination IP address. Some MULTI6 protocol proposals, such as NOID, SIM or CB64, are available which add such an identifier to every IP packet. Firewalls can use this identifier for packet classification.

HIP as a middlebox signaling protocol, as discussed in [4], could install a 128 bit flow identifier as a packet filter at middleboxes which allows data traffic to be associated with a certain behavior (and state at these devices). In case of firewalls this behavior is packet filtering and for QoS signaling this behavior is to associate a flow to a QoS class with preferential treatment. Each data packet would also carry this identifier (for example in an extension header).

Mobility, multi-homing, address changes due to DHCP lease expire or address changes due to privacy changes would not require flow identifer updates and hence data packets can still be correctly identified by firewalls as long as they carry the same identifier.

There are, however, also some problems:

- A route change hitting a new firewall requires signaling to this new device. This is always required regardless of the approach. Periodic retransmission of the signaling messages is necessary from this point of view (but also as part of the soft-state principle).
- The security properties of the classical 5 tuple is different to a 128-bit identifier when used as a flow identifier. Including locators (such as source and destination IP addresses) provides additional security since an adversary can only send packets to certain end points and to certain applications only. An adversary needs to be at special places along the path to mount attacks and he is certainly not able to arbitrarily inject packets. With the 128-bit identifier the situation is slightly different since an adversary must first eavesdrop the identifier and reuse it for his purpose from any location on the Internet to the target behind the firewall.

- The security properties of the 128-bit identifier are similar to those of "authorization tokens" which allow everyone knowing the "token" to be authorized to perform certain actions. In this context the action is to pass the firewall policies. These "authorization tokens" do not allow the owner to actively participate in the protocol exchange (other than attaching the identifier).

To improve the security of this initial proposal it would be possible to add data origin authentication. This would allow each intermediate middleboxes to cryptographically verify the incoming data traffic. To allow intermediate middleboxes to select the correct security association it is either possible to use the triple <SPI> <Protocol> <Dst-IP> or a separate identifier. The latter approach is benefitial in case of mobility.
As a strawman proposal the key derived as excerised in [4] can be used. The details are left for future study.

3. Conclusion and Outlook

This paper gives a problem statement about future work on advanced middlebox traversal. We propose to investigate the usage of data origin authentication between the data sender and one (or more) middleboxes and to address mobility handling in face of distributed state establishment in a novel way.
Recently a few attempts have been made to address negative aspects of end-to-end network layer encryption on the performance of TCP. This work includes TF-ESP (see also [5]) and attempts for layered encryptionand finally resulted in the ALIAS BOF (see [11], [10] and [9]). These areas are possible usage scenarios for this approach. Furthermore, more near future relevant scenarios are VPN traversal for Mobile IP signaling. There signaling messages must traverse a VPN gateway protected network. An additional area of interest is security for adhoc networks where the end host initiated traffic will be verified by a number of intermediate nodes.
To provide even stronger security guarantees it is possible to use source authentication since the firewalls represent a degenerated multicast tree (without using multicast addresses itself). Results from the multicast security community are available such as TESLA [12] or MESP [13] which can be used without severe modifications. Further work in this area will investigate the usage of TESLA for source authentication. The middlebox signaling protocol would therefore bootstrap the relevant parameters for subsequent usage of TELSA. As a difficult aspect it is important to prevent intermediate middleboxes to buffer packets (such as required in TESLA).

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. Moskowitz, P. Nikander, P. Jokela, and T. Henderson: "*Host Identity Protocol*", draft-ietf-hip-base-00.txt (work in progress), June 2004.
[2] J. Ylitalo and P. Nikander: "*BLIND: A Complete Identity Protection Framework for End-points*", to appear in *Security Protocols, Twelfth International Workshop,* Cambridge, 24-28 April, 2004.
[3] H. Tschofenig, A. Nagarajan, V. Torvinen, J. Grimminger: "*NAT and Firewall Traversal for HIP*", unpublished manuscript, October 2004.
[4] 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.
[5] S. Bellovin: "*Transport Friendly ESP or Layer Violation for Fun and Provit*", presentation available at: http://www.research.att.com/~smb/talks/tf-esp.pdf, (September., 2004).
[6] Access Link Intermediaries Assisting Services (ALIAS), http://mailman.berkeley.intel-research.net/mailman/listinfo/alias, (October, 2004).
[7] S. Lee, S. Jeong, H. Tschofenig, X. Fu, J. Manner: "Applicability Statement of NSIS Protocols in Mobile Environments**",** draft-manyfolks-signaling-protocol-mobility-01.txt (work in progress), July 2004.
[8] A. Fessi, M. Stiemerling, S. Thiruvengadam, H. Tschofenig, C. Aoun: "Security Threats for the NATFW NSLP", draft-fessi-nsis-natfw-threats-01.txt (work in progress), July 2004.
[9] S. Dawkins: "Problem Statement for Triggers for Transport(TRIGTRAN)", draft-dawkins-trigtran-probstmt-01.txt (work in progress), March 2003.
[10] U. Blumenthal: "Securely Enabling Intermediary-based Transport Services", draft-blumenthal-intermediary-transport-01.txt (work in progress), October 2003.
[11] M. Shore: "Communicating With Transport Intermediaries: Discussion and Framework", draft-shore-alias-fw-00.txt (work in progress), February 2004.
[12] Ran Canetti, Bob Briscoe, Dawn Song, and Doug Tygar: "TESLA: Multicast Source Authentication Transform Introduction", draft-ietf-msec-tesla-intro-03.txt (work in progress), February 2005.
[13] M. Baugher, R. Canetti, P. Cheng, P. Rohatgi: "MESP: A Multicast Framework for the IPsec ESP", draft-ietf-msec-mesp-01.txt (work in progess), March 2003.