MOBIKE Working Group
Internet Draft
Document: draft-mohanp-mobike-nat-00.txt
Expires: January 2005

M. Parthasarathy
Nokia

July 2004

IKE extensions for mobility through NAT

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at anytime. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 2004.

Copyright Notice

Abstract

This document discusses a simple NAT traversal method to support mobility for IKEv2 when the node moves behind a NAT. The method proposed here allows for the address change only after authenticating the new address.

Table of Contents

1.0 Introduction

The NAT traversal mechanism of IKEv2 as specified in [1] allows IPsec to work through NATs. If a NAT is detected during the initial IKE negotiation, it allows the node to maintain the same IKE and IPsec security association (SA) across movement. This works by changing the address without authenticating the new address. The peer updates the address from the latest authenticated packet coming from the other end, if the other end is behind the NAT. Though this allows mobility, it allows the attacker to launch a bombing attack [6] by modifying the source IP address of the packet to an arbitrary victim. This causes all the future packets to be sent towards the victim.

This document proposes a new mechanism to update the address when a node moves behind a NAT, without opening up the possibility of third party bombing attack. This document focuses mainly on the movement behind NAT. It assumes that proposals in [2] or [3] can be used for the base MOBIKE protocol.

2.0 Applicability Statement

The solution described in this document may not work with all NAT devices. It assumes that Network address Port Translation (NAPT) is used by the NAT device. It also does not work with multiple NAPT devices in the path. The solution is mainly targeted for SOHO type environments where there is a NAPT with public address on one side

and a DHCP server to allocate private addresses on the other side.

3.0 Protocol details

Assume a node has already established an IPsec SA with some remote peer. For simplicity, it assumes that the peer of this node is not

behind a NAT. The node moves to a new network behind a NAT. Following are the sequence of steps.

1) The node moves to a new network and invokes DHCP [2] to obtain a new address.

2) The node obtains a new address, which is most likely a private address (w.x.y.z) as it is behind a NAT. A new DHCP option defined below allows the node to discover the public address (a.b.c.d) of the NAT.

3) IKE gets notified of the new address (w.x.y.z) along with the public address (a.b.c.d). It invokes MOBIKE protocol as defined in [2] or [3] to notify the peer about the address change. As part of the address update payload, it includes the public address of the NAT a.b.c.d.

4) When the MOBIKE packet traverses the NAT, the external source IP address is changed from w.x.y.z to a.b.c.d. It also changes the UDP port number from 500 to port P.

5) The peer on receiving the MOBIKE address update packet verifies that the public address in the payload matches the address on the IP header. If not, it drops the packet as it implies that some attacker is modifying the packet. If the address verifies, the peer does the return routability test to verify that the address is a valid address, where the other end can be reached.

6) If RR succeeds at step (5), the peer updates to the new address. Both ends start using UDP encapsulation on port 4500.

In the rare cases where the public address changes as soon as the DHCP is completed, the return routability would fail and it will result in negotiating a new SA. If the public address of the NAT

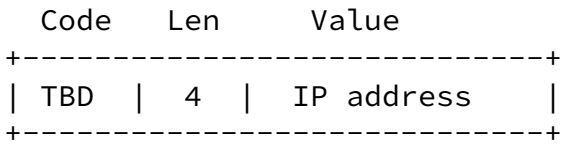
changes after the successful completion of MOBIKE, the dead peer detection would end up negotiating a new SA. It is not clear whether this is in the scope of MOBIKE.

When the node starts off behind a NAT and moves out of NAT, it can continue to use the UDP encapsulation negotiated as part of NAT-T. Hence, MOBIKE can ignore address changes during such movements.

4.0 DHCP option

This option is used to indicate the presence of NAT in the network by including the public address of the NAT. The option SHOULD be included by the DHCP server in the DHCPACK packet if there is a NAT

present in the network and the public address of the NAT is known. The format of the option is as follows.



The IP address is the public address of the NAT. The client on receiving this data infers that there is a NAT in the network, which uses the public address given in the option as the source address of all the packets. It is assumed that the operation performed by the NAT device is Network address port translation (NAPT) as defined in [5].

5.0 Security Considerations

The peer verifies the public IP address of the NAT only. It does not verify the port allocated by the NAT as it is not included in the address update payload. The attacker can modify the port on the UDP header, which can bomb the host behind the NAT. This assumes that the attacker has the ability to learn that there is more than one host behind the NAT, which may not be easy always. The attacker just sees one IP address and varying source ports if NAPT is used which could be one host establishing multiple connections or multiple hosts

establishing one connection each.

The security of the DHCP protocol itself is described in [4].

6.0 IANA Considerations

A new value for the DHCP option needs to be allocated as specified by the policy in [4].

7.0 Normative References

[1] C. Kaufman, ed. "Internet Key exchange (IKEv2) protocol", draft-ietf-ipsec-ikev2-14.

8.0 Informative References

[2] Francis Dupont, "Address management for IKE version 2", draft-ikev2-addrmgmt-05.txt

[3] T. Kivinen, "MOBIKE protocol", draft-kivinen-mobike-protocol-00.

[4] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[5] P. SriSuresh, K. Egevang, "Traditional IP Network address translator", RFC 3022, January 2001.

[6] F. Dupont, "A note about third party bombing in Mobile IPv6", draft-dupont-mipv6-3bombing-00 (work in progress), February 2004.

9.0 Acknowledgments

The author would like to thank Pasi Eronen for pointing out the bombing attack with untested port numbers.

10.0 Author's Address

Mohan Parthasarathy
Nokia
313 Fairchild Drive
Mountain View, CA-94303

Email: mohanp@sbcglobal.net

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

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.