Transient pseudo-NAT attacks or
how NATs are even more evil than you believed

<draft-dupont-transient-pseudonat-01.txt>

Status of this Memo

This document is an Internet Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

This document is an Internet-Draft. 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 any time. 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.

Distribution of this memo is unlimited.

Abstract

When a "NAT traversal" capability is added to a class of signaling protocols which can control some traffic aggregation points, an attack based on a temporary access to the path followed by messages exists.


This document claims this vulnerability is an intrinsic property of the NAT traversal capability, so is another point where the usage of NATs is very damaging.
1. Introduction

A Network Address Translator (NAT [8]) is a device which rewrites the source address or/and destination address as well as usually the transport protocol ports of a communication. Many kinds of NATs [9] exist but in this document the term NAT will be used for any device which modifies at least one of the IP header addresses (a pseudo-NAT when this is done for an attack).

NAT traversal capability consists in a NAT resilient transport, usually UDP, and in address "agility", i.e., addresses in the header of packets are taken as they are, especially the source address (packets with a fake destination address likely will not reach their intended recipient).

A traffic aggregation point is a place where traffic from many sources and/or many destinations is aggregated and sent to the same destination and usually arriving from the same source (the traffic aggregation point) through a tunnel. Home agents in Mobile IP and security gateways in IPsec [3] are typical examples of such traffic aggregation points (which are not necessary for the attack to work but increase its impact).

2. The Transient Pseudo-NAT Attack

An attacker acting as a NAT (i.e., a pseudo-NAT) may:
- redirect packets to another node
- make the intended recipient not receive packets to it (first form of Denial-of-Service (DoS) attack)
- flood a third party with the hijacked packets (second form of DoS attack, perhaps the most serious)

To perform the attack, the attacker must be on the path of packets during the attack.

When there is a traffic aggregation point, the effects of the attack are amplified when the attack is done "at the outgoing side" of the aggregation point.

When a signaling protocol manages the direction followed by the traffic, the attacker has only to spoof the addresses in headers of some messages of the protocol in order to hijack the traffic during a long period (i.e., until an error is detected and the correct path re-established). Since the attacker has to stay on the path only for a short moment (to the extent of some packets, one packet is enough in some cases), this attack is named the "transient" pseudo-NAT attack.
3. Attack Examples

3.1 Mobile IP

For Mobile IP the traffic aggregation point for choice is the home agent and the target signaling protocol is the binding update - binding acknowledgment exchange. If the NAT traversal capability is enabled, the care-of address of the mobile may not be protected, and therefore may be easily spoofed.

If no binding acknowledgment is required the attack can be reduced to the modification in transit of only one packet so we recommend to always require acknowledgment when NAT traversal is enabled (as a weak form of return-routability check).

3.2 IKE

The attack against IKE is worse because IKE is supposed to ensure a very high level of security, unfortunately defeated by NAT traversal which is the first short-term work item of the IETF ipsec working group charter [4]...

The attack follows the same scheme: addresses in headers of IKE exchange messages are spoofed and the traffic, for instance between two security gateways, is hijacked.

Any improvement to the IKE protocol makes the attack easier (a very unpleasant property of this attack). For instance if an implementation supports an address change between two "phases" (something desirable and supported via the SPI of the phase one) then to spoof the two or three messages of a quick mode exchange is enough, or in IKEv2 only one packet of a CREATE-CHILD-SA exchange.

Again there is no easy defense which keeps the NAT traversal capability. For instance the protection of the header addresses (very easy to provide in the IKE framework) is effective against both the vulnerability and the NAT traversal capability...

4. Security Considerations

The Mobile IP NAT traversal new document has a long description of this attack [10,5]. We believe the ipsec working group will examine in details which features can help mobility or/and NAT traversal and what are their consequences for security.

The architectural implications of the NAT document [11] do not describe this attack but it can be considered as a result of the violation of the end-to-end principle on the trust model.
5. Acknowledgments

Maryline Maknavicius-Laurent drew my attention on this attack at the IP Cellular Network 2002 conference. Phil Roberts encouraged me to point out this attack in the IETF mobileip WG mailing-list ASAP. I’d like to thank a well known NAT hater who’d like to stay anonymous for his help to write this document.

6. Normative References


7. Informative References


draft-dupont-transient-pseudonat-01.txt
8. Authors’ Addresses

Francis Dupont
ENST Bretagne
Campus de Rennes
2, rue de la Chataigneraie
BP 78
35512 Cesson-Sevigne Cedex
FRANCE
Fax: +33 2 99 12 70 30
EMail: Francis.Dupont@enst-bretagne.fr

Jean-Jacques Bernard
AFNIC / NIC France
Immeuble International
2 rue Stephenson
78181 Saint-Quentin-en-Yvelines Cedex
FRANCE
Fax: +33 1 39 30 83 01
EMail: Jean-Jacques.Bernard@nic.fr