Internet Engineering Task Force
Internet Draft

Satomi Okazaki
Anand Desai
NTT MCL, Inc.

Expires: January 2004 June 2003

NAT-PT Security Considerations

draft-okazaki-v6ops-natpt-security-00.txt

Status of this Memo

Abstract

NAT-PT (RFC2766) is an address translation mechanism designed to facilitate communications between IPv6-only and IPv4-only nodes. This mechanism was designed to be used when tunneling transition mechanisms cannot be used.

This document is intended to be a compilation of known security issues related to NAT-PT and includes a few new ones. These issues are discussed in some detail, and suggestions on how to deal with them are included in this document.

Table of Contents

1.0 Introduction

Given the current deployment of IPv4 and the infrastructure changes necessary to adopt IPv6, there is guaranteed to be a long period in which the two must coexist. Various mechanisms have been proposed to allow for a smooth transition from IPv4 to IPv6. These techniques may be divided into two general types: tunneling mechanisms and translation mechanisms. Translation mechanism documents such as NAT-PT (Network Address Translation û Protocol Translation) [RFC2766] and SIIT (Stateless IP/ICMP Translation Algorithm) [RFC2765] indicate that they are to be used when tunneling techniques are not applicable. Translation mechanisms are intended for use between IPv6-only nodes and IPv4-only nodes.

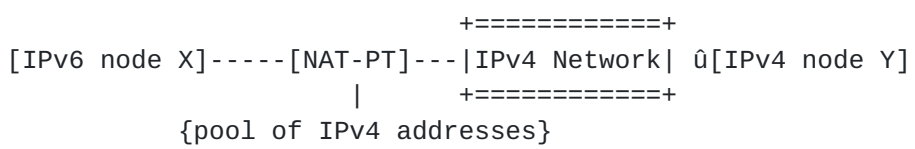
Security issues in tunneling have been examined ([TunSec][SecCon]) to some extent. We are not aware of any dedicated security analysis documents related to translation techniques. In this document, we examine the security of NAT-PT, one of the prominent translation mechanism proposals. We list a few new security issues in addition to those that have been noted in the original draft and some others that have been mentioned in other drafts [DNSALG] [TransUnman] [TransIss] or on the v6ops mailing list. We propose solutions for the security issues that we have found.

2.0 Description of Scheme

NAT-PT defines a method for allocating a globally unique temporary IPv4 address to an IPv6-only node to allow transparent routing between an IPv6-only node and an IPv4-only node. It is designed to work with a scheme like SIIT, which is a specification for a box that translates IPv4 headers into IPv6 headers and vice versa.

The NAT-PT specification defines the functionality of an address translation box that sits on a border router. The NAT-PT box has a pool of globally unique IPv4 addresses to assign to IPv6-only nodes that need to communicate with IPv4-only nodes. There are two types of sessions û those that are initiated by an IPv6 node and those that are initiated by an IPv4 node. Here, we focus on the basic NAT-PT address translation functionality.

Suppose that an IPv6-only node X behind a NAT-PT box has the IPv6 address FEDC:BA98::7654:3210, and suppose that an IPv4-only node Y in an IPv4 network has the IPv4 address 136.40.1.1. Furthermore, let us say that the NAT-PT box has a pool of globally unique IPv4 addresses in the range 140.32.1.1 to 140.32.1.20.



IPv6 address of X: FEDC:BA98::7654:3210
IPv4 address of Y: 136.40.1.1
NAT-PT pool of IPv4 addresses: 140.32.1.1 to 140.32.1.20

2.1 IPv6-node-initiated communications

Suppose IPv6-only node X wishes to initiate communications with IPv4-only node Y. The NAT-PT box in XÆs network is associated with some prefix, which we will denote by ôPREFIX.ö

X prepends this prefix to YÆs IPv4 address to get an IPv6 address that looks like ôPREFIX::IPv4 address of Yö. The source address and destination address of the packets that X sends to Y look like the following:

src: FEDC:BA98::7654:3210
dst: PREFIX::136.40.1.1

All packets with destination address beginning with PREFIX are routed to the NAT-PT box, as the prefix is chosen to be unique in the stub domain, and the NAT-PT box advertises the prefix for routing purposes.

The NAT-PT box then replaces the source address in the packets with the temporary IPv4 address (say 140.32.1.1) it chooses from its pool for X, and the box then strips ôPREFIXö from the destination address so that the IPv4 address of Y remains:

src: 140.32.1.1
dst: 136.40.1.1

2.2 IPv4-node-initated communications

The case in which a session is initiated by an IPv4 node is a bit more complicated and involves Domain Name Servers (DNSs). The IPv4 node YÆs DNS resolver would send a name look-up request (type ôAö) for X. This request gets sent through XÆs NAT-PT box to the DNS server on XÆs network.

The NAT-PT contains a DNS-ALG (Application Level Gateway) that translates an ôAö query to an ôAAAAö or ôA6ö query and sends it to the DNS server on XÆs network. When the IPv6 DNS server responds with an ôAAAAö or ôA6ö record, it is sent through the NAT-PT box, where DNS-ALG translates it into an ôAö record and replaces the IPv6 address of X with the corresponding temporary IPv4 address from the pool.

3.0 Security analysis

In this section, we list all of the security threats that we know of - a number of security threats that have been outlined in the original draft itself, in external documents, and those that we have isolated.

3.1 End-to-end security

As noted in [RFC2766], NAT-PT and end-to-end security do not work together. When IPv6-only node X initiates communications to IPv4-only node Y, the packet that X forms has an IPv6 source address (FEDC:BA98::7654:3210) and an IPv6 destination address (PREFIX::136.40.1.1), which are used in IPsec (ESP or AH) computations, including TCP/UDP/ICMP checksum computations.

Since NAT-PT assigns X an IPv4 address (140.32.1.1) that has no relationship to XÆs IPv6 address, there is no way for recipient Y to determine XÆs IPv6 address, which is involved in verifying TCP/UDP/ICMP checksum computations.

3.2 Prefix assignment

The draft [RFC2766] does not describe how the IPv6 nodes learn the prefix that is used to route packets to the NAT-PT box. If the prefix is pre-configured in IPv6 nodes, the IPv6 node would prepend the pre-configured prefix to the address of any IPv4-only node with which it want to initiate communications. However, with a fixed prefix, there might be a reachability problem if the NAT-PT box were to shut down.

If an attacker were somehow able to give the IPv6 node a fake prefix, the attacker would be able to steal all of the nodeÆs outbound packets to IPv4 nodes.

3.3 DNS-ALG

The DNS-ALG is required when allowing IPv4-only-node-initiated communications in the NAT-PT setting. Since DNS-ALG will translate ôAö record requests into ôAAAAö or ôA6ö request and conversely, ôAAAAö or ôA6ö records into ôAö records, DNS-SEC will not work with NAT-PT, as noted in [RFC2766].

This means that it is possible for an attacker to modify records from DNS-ALG to the IPv4 nodes.

3.4 Source address spoofing attack

We consider attackers that will use NAT-PT resources. There are two cases: in the first, the attacker is in the same stub domain as the NAT-PT, and in the second, the attacker is outside of the NAT-PT stub domain.

3.4.1 Attacker in the NAT-PT stub domain

Here, we suppose that an attacker in the same stub domain as NAT-PT sends a packet destined for an IPv4-only node Y on the other side of NAT-PT. We look at the more interesting case in which the attacker forges its source address to be an address that is topologically inside the stub domain. (This address could belong to another node, or it could be unassigned.)

Address depletion attack - If the IPv6 attacker sends many such packets, each with a different source address, then the pool of IPv4 addresses may get used up, resulting in a Denial of Service attack. (This vulnerability is also noted in [RFC2766] and [TransIss].)

The other attacks exist even without NAT-PT. These are reflection attacks, resource exhaustion attacks, and broadcast/multicast attacks. In a reflection attack, the IPv6 source address is set to that of an existing node. That node will be the recipient of a reflection attack, as the IPv4 node will send response packets to the victim node. In a resource exhaustion attack, the IPv6 source address is set to that of a non-existent node. The return packets will be dropped, but this may still result in a resource exhaustion DoS attack on Y. Finally, in a multicast attack, the IPv6 source address is a multicast address. The return packet from the IPv4 node will be sent to the multicast address, resulting in a multicast attack.

3.4.2 Attacker outside of NAT-PT stub domain

Here, we suppose that an attacker on the other side of NAT-PT sends a packet destined for an IPv6-only node X behind NAT-PT. We look at the more interesting case in which the attacker forges its source address to be an address that is topologically outside the stub domain. (This address could belong to another node, or it could be unassigned.) The same attacks are possible here as in the case described in the previous section.

3.5 An external attacker node

In this case, an attacker that knows the IP address of the NAT-PT box can send packets directly to the box. It can use NAT-PT resources, preventing legitimate IPv6-only nodes from accessing NAT-PT services.

4.0 Possible solutions

4.1 End-to-end security

End-to-end security is not possible with NAT-PT. One reason is outlined in section 3.1.

4.2 Prefix assignment

Though it is not specified in [RFC2766], DNS servers and DNS-ALG may be used in outgoing connections to return the prefix information to the IPv6 node. This is a way to avoid the problem of a statically pre-configured prefix. When an IPv6-only node wishes to initiate communications with an IPv4-only node, its resolver would send an ôAAAAö query. This query can be passed through the DNS-ALG, which would receive an ôAö record in response. In this case, the DNS-ALG can prepend the appropriate prefix for the NAT-PT and translate the ôAö record into an ôAAAAö or ôA6ö record and return it to the IPv6 node.

The DNS-ALG can also monitor the state of a number of NAT-PT boxes (multiple boxes for scalability) and return the prefixes of those that are running. This idea was stated in [DNSALG] and [mNATPT], as well as in e-mail communication on the v6ops mailing list.

As mentioned in [mNATPT], the method by which DNS-ALG determines the state and validity of a NAT-PT box must be secure. The DNS-ALG and each NAT-PT box should be configured with a pairwise unique shared key that will be used for integrity-protected communications.

Note that messages from DNS-ALG are not integrity-protected and can therefore be modified. To prevent such a modification, DNS-ALG can sign its packets. DNS-ALGÆs public key can be made available like that of a DNS server (see [RFC2535]) or presented in a certificate that has a root CA that is well known to all nodes behind NAT-PT. A shared-key technique may not be as practical.

4.3 DNS-ALG

The end host (IPv6 node or IPv4 node) will not be able to verify the signature on a DNS record because of the translation that the DNS-ALG performs.

However, as is pointed out in [DNSALG], if the host sets the "AD is secure" bit in the DNS header, then it is possible for the local DNS server to verify the signatures.

Another option is for DNS-ALG to verify the received records (like a DNS resolver), translate them, and sign the translated records (like a DNS server). DNS-ALGÆs public key can be made available like that of a DNS server (see [RFC2535]).

A third option would be for a host to have an IPsec security association with the DNS-ALG to protect DNS records.

4.4 Source address spoofing attack

4.4.1 Attacker in the NAT-PT stub domain

The NAT-PT (which sits on a border router) should perform ingress filtering. This would prevent an attacking node in its stub domain that forges its source address from performing a reflection attack on nodes in other stub domains. However, this does not prevent such an attacker from performing a reflection attack on other nodes in the same stub domain. These are not attacks introduced by NAT-PT.

The NAT-PT should drop packets whose IPv6 source address is a multicast address. This would prevent the multicast attack. This is not an attack introduced by NAT-PT.

One way to get around the address depletion attack is to employ NAPT-PT (Network Address Port Translation - Protocol Translation)[RFC2766], which translates TCP/UDP ports of IPv6 nodes into TCP/UDP ports of the translated IPv4 addresses. However, as the draft points out, IPv4-node-initiated NAPT-PT sessions are restricted to one server per service.

Another method of dealing with address depletion is to have a list of nodes to which NAT-PT will offer its translation services. Or for more security, an IPsec security association could be required between the NAT-PT and nodes to which it will offer its services.

4.4.2 Attacker outside of the NAT-PT stub domain

The NAT-PT should drop packets whose IPv4 source address is a broadcast/multicast address to prevent a broadcast/multicast attack. Furthermore, NAT-PT should filter out packets from outside that claim to have a source address behind NAT-PT. These are not attacks introduced by NAT-PT.

The address depletion attack is discussed in the previous section.

4.5 An external attacker node

NAT-PT should drop packets that are sent directly to its IP address rather than being routed to it via the prefix PREFIX. If NAT-PT maintains a list of nodes to which it will offer its services, this type of attack will be minimized as well. Or for more security, an IPsec security association could be required between the NAT-PT and nodes to which it will offer its services.

5.0 Acknowledgements

The authors would like to acknowledge DoCoMo USA Labs for support of this work and in particular, James Kempf for helpful comments and insights.

6.0 Security Considerations

This draft is itself a document about security considerations for NAT-PT.

7.0 References

[TunSec] Di Battista et al. ôOperational procedures for secured management with transition mechanisms,ö 28 February 2003.

[DNSALG] Durand, A. ôIssues with NAT-PT DNS ALG in RFC2766,ö <draft-durand-v6ops-natpt-dns-alg-issues-00.txt>, Internet-Draft, 29 January 2003.

[RFC2535] Eastlake, D. ôDomain Name Security Extensions,ö RFC 2535, March 1999.

[TransUnman] Huitema, C. et al. ôEvaluation of Transition Mechanisms for Unmanaged Networks,ö <draft-huitema-ngtrans-unmaneval-01.txt>, Internet-Draft, 1 November 2002.

[RFC2765] Nordmark, E. ôStateless IP/ICMP Translation Algorithm (SIIT),ö RFC 2765, February 2000.

[mNATPT] Park, S.D. et al. ôScalable mNAT-PT Solution,ö <draft-park-scalable-multi-natpt-0.txt>, Internet-Draft, May 2003.

[SecCon] Savola, P. ôSecurity Considerations for 6to4,ö <draft-savola-v6ops-6to4-security-02.txt>, Internet-Draft, January 2003.

[RFC2766] Tsirtsis, G. and Srisuresh, P. ôNetwork Address Translation û Protocol Translation (NAT-PT),ö RFC 2766, February 2000.

[TransIss] Van der Pol, R. et al. ôIssues when translating between IPv4 and IPv6,ö <draft-vanderpol-v6ops-translation-issues-00.txt>, Internet-Draft, 27 January 2003.

8.0 AuthorsÆ Contact Information

Satomi Okazaki
NTT MCL, Inc.
250 Cambridge Avenue, Suite 300
Palo Alto, California 94306
USA

Phone: +1 650 833 3631
Fax: +1 650 326 1878
Email: satomi@nttmcl.com

Anand Desai
NTT MCL, Inc.
250 Cambridge Avenue, Suite 300
Palo Alto, California 94306
USA

Phone: +1 650 833 3638
Fax: +1 650 326 1878
Email: anand@nttmcl.com

9.0 Full Copyright Statement