Internet Engineering Task Force
Internet Draft
draft-dondeti-ipv6-anycast-security-00.txt
Expires: December 2001

L. Dondeti, T. Hardjono, B. Haberman
Nortel/ Verisign/ Nortel

June 2001

Security Requirements of IPv6 Anycast

STATUS OF THIS MEMO

Abstract

This document discusses the security issues within network-layer anycast protocols. In particular, it focuses on anycast server registration with routers in an IPv6 network. Servers need to be authenticated and authorized to provide a particular anycast service. Clients need to be able to verify that an anycast server is authentic. While infrastructure security is the main focus of this document, we also identify the need for secure communication between anycast clients and servers.

Table of Contents

1 Introduction to anycast

IP anycast is an elegant solution for service discovery in the Internet [1]. An IP anycast address is assigned to one or more network interfaces (e.g. routers or hosts/servers) that provide a given service. A packet sent to an anycast address is delivered to the "topologically nearest" network interface with the anycast address.

Anycast is an efficient way of providing a service replicated on several different devices in the Internet. It provides fault-tolerance and some load balancing. In the event of a server failure, packets addressed to an anycast address are routed to the "new nearest" node providing the desired service. Requests originating in different parts of the network may reach different anycast servers, thus providing rudimentary load balancing.

Anycast service location works as follows. When a client requires service, it sends the request to the corresponding anycast address. Note that two packets addressed to an anycast address may reach two different anycast servers. Therefore, an anycast client needs to make sure that its request fits in a single packet. The responding anycast server puts its own unicast address as the source address in the reply message. For any stateful communication with an anycast server, the client uses the responding server's unicast address. Future stateless anycast service requests, however, can be sent to the anycast address.

We differentiate between network layer anycast and application aware or simply application layer anycast.

1.1 Application layer anycast

Web caching and ftp service are examples of application layer services that can benefit from anycast. These services modify the definition of anycast to denote a protocol that finds the "best server" as opposed to the "nearest" server as defined in RFCs 1546 and 2373. The rationale in changing the definition is that it is often desirable to reach the least loaded server or in other words the server that can provide the fastest service.

Anycast requests in this case are routed by application layer devices.

1.2 Network layer anycast

Network layer anycast routes anycast requests to the "nearest" (by routing protocol's measure of distance) interface that advertises the anycast address. We list some services that use network layer anycast below [2]:

- DNS server discovery [3].
- To locate routers providing an ISP's services.
- To reach any router attached to a particular subnet [4].
- To reach any router that provides an entry point into a domain (AS).

1.3 Anycast groups

Finally, we end this section by describing the notion of an anycast group. From the perspective of a client, anycast is a service. A service provider enables several nodes to respond to a particular anycast request. We treat all the network nodes responding to an anycast request as members of an anycast group. We then control membership of the anycast group. Routers advertise routes to only authorized members of an anycast group.

2 Anycast addresses and routing in IPv6

An IPv6 anycast address is syntactically indistinguishable from a unicast address [2]. This implies that routers treat an anycast address same as a unicast address during routing. However, when an interface is configured with an anycast address, the node with the

interface knows the nature of the address and treats it accordingly.

RFC 2373 specifies that an anycast address must not used as the source address of a packet. Thus an anycast server needs to put its unicast address as the sender address in the reply packets. If a client needs followup information, it can send that request to the responding anycast server's unicast address.

RFC 2373 also states that anycast addresses can only be assigned to routers, but not hosts. Itojun et. al [5] observe that it is insecure to permit hosts to inject routes to anycast addresses. With anycast group access control [6] mechanisms in place, we may be able to remove this restriction.

Knowledge of anycast addresses

We know that anycast servers need to know whether an IPv6 address is being used for an anycast service. This is to ensure, among other things, that sender address in the reply packet is the unicast address of the anycast server. Routers in the network do not need to know that an address is being used an anycast address, since no special treatment is required for routing packets sent to an anycast address. Note that anycast clients also need to know that a particular IPv6 address is an anycast address. There are several reasons. First, recall that an anycast request must be sent in a single packet. Further, the client must not fragment anycast packets. Finally, the client cannot employ simple security checks such as verifying whether sender address of the response packet is same as the destination address in the reply packet.

3 Security issues of anycast

Anycast is vulnerable to security attacks similar to unicast and multicast. Clients send requests to an anycast address, to which one the members of the anycast group might respond.

Several security threats pertaining to anycast have been identified in earlier works [3,1]. In this document, we describe those and identify additional issues of concern pertaining to anycast data communications. Finally, we summarize the security requirements of anycast.

3.1 Unauthenticated anycast server announcements

Any entity in the network can advertise itself as an anycast server. In other words, anycast group membership is not controlled. First, an adversary can use this opportunity to provide false information to a

client [5]. Note that the client has no way of knowing whether the information is legitimate. Second, adversaries can create "black holes" by advertising bogus server addresses. Anycast requests routed to these bogus addresses will reach a fake server, which does not respond to the request. This constitutes a denial of service (DOS) attack.

Anycast security requirement 1:

Access to anycast group membership must be controlled. We need an anycast server registration mechanism during which access control functions can be performed.

Routers must advertise routes of legitimate anycast servers only.

3.2 Source address modification by an anycast server

An anycast address cannot be a source address [2] in an IPv6 packet. Consequently, an anycast server responding to a request puts its own address as the source address in the reply packet. Notice that the client has no way of knowing whether the source address is that of a legitimate anycast server or not. Therefore, the client cannot trust the information provided by the anycast server. Also, consider that a client may use the source address for a follow-up request, and that request might go to a bogus server, which might send false information, or not reply at all.

We need anycast source authentication. For example, the anycast server might produce a certificate, signed by a trusted certification authority (CA) that the server belongs to the specified anycast group, in its reply packet.

Anycast security requirement 2:

Responses to anycast requests may need to be authenticated.

3.3 Secure communication between anycast clients and servers

Some anycast services may require secure communication between the clients and servers. This is to imply that we may need to ensure that anycast communications are confident, authenticated and protected against replay attacks.

We describe the need for authentication of anycast replies in the previous section. Source authentication or content authentication are suggested solutions in the literature in the context of anycast [3]

or in the context of immediate applications of anycast, viz., DNS [7].

However, notice that both solutions are not protected against replay attacks. For example, a rogue entity in the network can replay outdated (possibly incorrect) information. The client would have no way of identifying the correct information. An adversary thus can cause denial of service or provide bogus service, even when anycast communications are authenticated.

Anycast security requirement 3:

We may need secure communication between anycast clients and servers. In other words, anycast communications may need to be confidential, authenticated and protected from replay attacks.

3.4 Anycast security requirements

In summary, we list several security requirements of anycast:

- Only legitimate anycast servers should be able to advertise themselves as providers of anycast service.
- Anycast clients may need to know the replying server is an authorized anycast server.
- Anycast communication may need to be confidential.
- Anycast clients may want to verify freshness of a reply.

4 Providing secure anycast communication

In the current version of the document, we concentrate on identifying the security threats and requirements of anycast communication. Note that most of the issues raised in the above discussion may be solved with existing techniques. We may, however, need to tailor them for anycast.

5 Security considerations

In this document, we identify the security issues pertaining to anycast communications. Briefly, we need to control access to anycast groups. Routers must advertise routes to only authorized members of an anycast group. Replies to anycast requests may need to be authenticated, confidential and protected against replay attacks.

6 Acknowledgements

We appreciate Dave Thaler's comments on the security needs of anycast.

7 References

[1] C. Partridge, T. Mendez, and W. Milliken, "Host anycasting service," RFC (Informational) 1546, Internet Engineering Task Force, Nov. 1993.

[2] R. Hinden and S. Deering, "IP version 6 addressing architecture," RFC (Standards Track) 2373, Internet Engineering Task Force, July 1998.

[3] DNS Discovery Design Team, Thaler D. (Editor), "Analysis of DNS server discovery mechanisms for IPv6," Internet Draft, Internet Engineering Task Force, Mar. 2001. Work in progress.

[4] D. Johnson and S. Deering, "Reserved IPv6 subnet anycast addresses," RFC (Standards Track) 2526, Internet Engineering Task Force, Mar. 1999.

[5] J. Itojun and K. Ettikan, "An analysis of IPv6 anycast," Internet Draft, Internet Engineering Task Force, Oct. 2000. Work in progress.

[6] B. Haberman and D. Thaler, "Host-based anycast using MLD," Internet Draft, Internet Engineering Task Force, Feb. 2001. Work in progress.

[7] D. Eastlake, "Domain name system security extensions," RFC (Standards Track) 2535, Internet Engineering Task Force, Mar. 1999.

8 Authors' contact information

Lakshminath R. Dondeti
Nortel Networks
600 Technology Park Drive
Billerica, MA 01821, USA
(978) 288-6406
ldondeti@nortelnetworks.com

Thomas Hardjono
Verisign Inc.
401 Edgewater Place, Suite 280
Wakefield, MA 01880, USA
thardjono@verisign.com

Brian Haberman

Nortel Networks
4309 Emperor Blvd.,
Durham, NC 27703, USA
(919) 992-4439
haberman@nortelnetworks.com