DNS Operation Working Group
INTERNET-DRAFT
Expires: September 12, 2008
Intended Status: BCP

D.Senie
Amaranth Networks Inc.
A. Sullivan
Command Prompt Inc.

March 12, 2008

Considerations for the use of DNS Reverse Mapping
draft-ietf-dnsop-reverse-mapping-considerations-06

Status of this Memo

Abstract

Mapping of addresses to names is a feature of DNS. Many sites implement it, many others do not. Some applications attempt to use it as a part of a security strategy. This document outlines what should be taken into account when deciding whether to implement reverse mappings of addresses to names, suggests that site administrators implement reverse mappings if there are no strong considerations against such mappings, and provides considerations to be taken into account when using reverse mappings.

1. Introduction

1.1 Overview

The Domain Name System allows for providing mapping of IP addresses to host names. The feature allows administrators to provide both name to address, and address to name mappings for networks. This practice is documented, but without guidelines for those who control address blocks. This document provides some such guidelines, suggests that site administrators implement reverse mappings in the absence of strong counter-considerations, and also offers other guidance for the use of the reverse-mapping capability.

1.2 Terminology

In the following, the general term "reverse mapping" is used to refer to the overall capability of mapping IP addresses to host names, and "reverse tree" the portions of the DNS that provide the functionality. The term "IN-ADDR" is used to refer to the feature only as it applies to IPv4 use, and IN-ADDR.ARPA to the portion of the DNS that provides such IPv4-specific functionality. Similarly, "IP6" refers to the feature only as it applies to IPv6 use, and "IP6.ARPA" to the portion of the DNS that provides the IPv6-specific functionality. In what follows, except where the text explicitly refers only to IN-ADDR or IP6, the document can and should be applied to both address spaces.

Starting from a given IPv4 address (possibly the result of a query for an A RR), the term "existing reverse data" means that a query for <reversed-ip4-address>.in-addr.arpa. type PTR results in a response other than Name Error.

Starting from a given IPv6 address (possibly the result of a query for an AAAA RR), the term "existing reverse data" means that a query for <reversed-ip6-address>.ip6.arpa. type PTR results in a response other than Name Error.

The term "matching reverse data" means that the query for existing reverse data results in a response containing a set of one or more names which, when each queried themselves in the forward zone for A or AAAA RRs (as appropriate) return one or more results, one of which corresponds to the original query.

The term "missing reverse data" means that the query for existing reverse data results in a response of Name Error.

So, for example, a query for

```
b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.
        IP6.ARPA.
```

that resulted in a response of Name Error would be a case of missing reverse data. A query for

```
3.2.0.192.IN-ADDR.ARPA.
```

that resulted in a response containing a PTR record to example1.example.org would be a case of existing reverse data. If a corresponding query for

```
EXAMPLE1.EXAMPLE.ORG
```

resulted in a response containing an A record 192.0.2.3, then it would be a case of matching reverse data. If, however, the forward query did not result in a response containing an A record 192.0.2.3, then the reverse data could be said to exist, but not to match.

1.3 Motivation

In recent years, some sites have come to rely on reverse mapping as part of their administrative policies even as other sites have either stopped maintaining matching reverse mappings of their addresses, or else stopped implementing reverse mappings altogether.

The widespread practice of "virtual hosting" -- using one machine and IP address to host many different domains -- means that reverse mappings become sometimes difficult to maintain or awkward to use. The large IPv6 address space exacerbates the difficulty of administering reverse mapping. Finally, some administrators regard the data in the reverse tree as at best worthless and at worst a potential information leak, and so object to maintaining reverse mappings.

At the same time, some sites have attempted to use reverse mappings as a part of a security or abuse-prevention policy. Moreover, some protocols that store data in the DNS, such as those described in [RFC4025] and [RFC4322], could benefit from matching reverse mapping data, particularly when combined with the use of the DNS security extensions ([RFC4033],[RFC4034],[RFC4035]).

In light of the above conflicting pressures, this document attempts to outline some considerations for the maintenance and use of reverse mappings so that users and administrators can make informed decisions.

2. Background

In the early days of the Domain Name System [RFC883] a special domain was set aside for resolving mappings of IP addresses to domain names. This was refined in [RFC1035], describing the .IN-ADDR.ARPA domain in use today. For the IPv6 address space, .IP6.ARPA was added by [RFC3152], and its use is codified in [RFC3596].

[RFC1912] suggests that it is an operational or configuration error not to have matching PTR and A records.

The assignment of blocks of IP Address space was delegated to (originally three) Regional Internet Registries (RIRs). Guidelines for the registries are specified in [RFC2050], which strictly requires RIRs to maintain reverse mapping records only on the large blocks of space issued to ISPs and others.

Each RIR has its own policy for requirements for reverse-mapping maintenance; these policies may change from time to time. Some RIRs have policies that actively encourage reverse mapping. Many address blocks were allocated before the creation of the regional registries, and thus it is unclear whether any of the policies of the registries are binding on those who hold blocks from that era.

2.1 Historical origins of reverse mapping use in security

The growth of the Internet in the late 1980s and early 1990s brought with it attackers who acquired access to machines without authorization. Many systems attached to the Internet up to that time were poorly prepared for such attacks, and administrators were forced to react using available resources rather than to redesign the network to meet the new security challenges.

The popular TCP Wrapper package was originally conceived to discover the network location of an attacker [Venema1992]. It used the reverse mapping of a connecting host to provide the hostname of that host in its output.

During the same period, the so-called "UNIX r* commands", like rlogin [RFC1282], were widely used, in spite of warnings that they were prone to abuse [Reid1987]. The r* commands allowed users to employ a list of trusted hosts, from which connections would be accepted and authenticated without password (sometimes called the "rhosts authentication" mechanism). The mechanism remained in widespread use (in spite of known flaws) because of its convenience. Since the list of trusted hosts was a simple list of hostnames or addresses, an attacker could acquire access either by by putting the target host

name in the PTR record in the IN-ADDR zone for the attacking IP address; or, by intercepting the DNS query for a hostname, and replying with the IP address from which the attacker was making the rhosts authentication attempt. Different implementations of the r* commands authenticated differently, but none of them actually checked for matching reverse data; the exact method of attack depended on the version of the r* commands being attacked and the configuration in use. (This weakness was not the only one in the mechanism, but it is the most relevant to reverse mapping.)

In an effort to strengthen the rhosts authentication mechanism, the TCP Wrapper package soon offered the ability to perform reverse mapping matching checks. If the reverse and forward mappings did not match, the wrapper program would terminate the connection before checking any of its other permissions. This mechanism could be used for all connections, on the grounds that forward and reverse mismatches were an indication either that an attack was in progress; or else that the network was badly managed, and therefore a likely origin for attack.

Other protocols than the r* commands implemented rhosts-style authentication mechanisms. In many but not all cases, this was implemented by employing features from the TCP Wrapper package.

3. Issues surrounding reverse mapping

This section discusses some of the ways in which reverse mapping is used; the effects for users of reverse mappings when those mappings are missing or do not match; and the effects on users when strong reverse mapping checks are in place, when users are unable or unwilling to implement reverse mappings. This section outlines some issues, but should not be interpreted as either approval or disapproval of a given practice.

3.1 Examples of effects of missing reverse mapping

Following are some examples of some of the uses to which reverse mapping checks are put, and some of the difficulties that can be encountered because of missing reverse data. The utility of each of these methods is discussed in section 3.2, below. Irrespective of whether they are useful, their failure in each case produces additional load on systems and additional latency in network activity.

Some applications use DNS lookups for security checks. To ensure validity of claimed names, some applications will look up records in the reverse tree to get names, and then look up the resultant name to

see if it maps back to the address originally known. Failure to find matching reverse mappings is interpreted as a potential security concern.

Some popular FTP sites will simply reject user sessions, even for anonymous FTP, if there is a missing reverse mapping or if matching reverse mapping does not exist. Some Telnet servers also implement this check.

Web sites sometimes use reverse mapping to verify whether the client is located within a certain geopolitical entity. This approach has sometimes been employed for downloads of cryptographic software -- for example, where export of that software is restricted to certain locales. Site operators may choose to refuse to allow the connection in the event they are not able to perform these checks. Credit card anti-fraud systems also sometimes use similar methods for geographic placement purposes, and may generate false alarms in the event the reverse resolution is not possible.

The popular TCP Wrapper program found on most Unix and Linux systems has options to perform reverse mapping checks and to reject any client with a missing reverse mapping. The program also has a way to check for matching reverse mapping. In the event that the checks fail, connections may be terminated.

Some anti-spam systems use the reverse tree to verify existing reverse mapping, or to check for matching reverse mapping. Some mail servers have the ability to perform such checks at the time of negotiation, and to reject mail from hosts that do not have matching reverse mappings for their hostnames. These PTR checks sometimes include databases of well-known conventions for generic names (for example, PTR records for dynamically-assigned hostnames and IP addresses), and may allow complicated rules for quarantining or filtering mail from unknown or suspect sources. Even some very large ISPs are reported to refuse mail from hosts without a reverse mapping. Often, the reverse map check is not used on its own, but is used as part of a scoring system in an attempt to indicate the probability that a given email message is spam.

Many web servers query for reverse mappings for visitors, to be used in log analysis. This adds to the server load, but in the case of reverse mapping unavailability, it can lead to delayed responses for users. Moreover, some statistics packages perform such lookups in retrospect, and missing reverse mapping will prevent such packages from working as expected.

Traceroute output with descriptive reverse mapping proves useful when

debugging problems spanning large areas. When this information is missing, the traceroutes can take longer, and those performing troubleshooting are left without useful hints.

3.2 Utility and effectiveness of some reverse mapping uses

Especially in the absence of strong anti-spoofing mechanisms, like the DNS Security Extensions, a check for matching reverse DNS mapping should be regarded as an extremely weak form of authentication. Even moderately skilled attackers have available to them tools to spoof DNS responses. Because of the dearth of experience with the DNS Security Extensions, it is currently unknown whether they add any additional security to what will always be fundamentally a weak form of authentication. The use of the DNS Security extensions also does nothing to indicate the intentions behind the attempted connection. In any case, there are stronger mechanisms for authentication available.

Especially given the widespread deployment of Virtual Private Networks [RFC2764] and Network Address Translation [RFC3022], reverse mapping is not a reliable indicator of actual geopolitical location. In the context of fraud prevention and export restriction, false rejection may be an acceptable compromise, but administrators and policy makers should be aware of the unreliability of the measure.

Reports from operators suggest that scoring mail on the basis of missing or non-matching reverse mapping remains an imperfect but useful measure of the likelihood that a given message is spam, particularly in combination with other measures. It is clear that the presence of reverse mapping, and a match between the forward and reverse zones, is neither a necessary nor sufficient condition for a candidate message to be spam.

The reliance on reverse mapping for logging may result in undesirable delays for users. To the extent that reverse mappings are not widely implemented, it is also likely to produce poor data. Performing the reverse lookup in retrospect may introduce errors, because in the period of dynamic assignment of IP addresses, it is possible that the reverse data at different times will not be the same.

3.3 The difficulty with blanket policies

Some users have reported difficulty in ensuring reverse tree maintenance by their upstream providers. (This is the user's perspective of the "reachover problem" described in section 3.4, below.) Users without many choices among providers, especially, can become the needless victim of aggressive reverse mapping checks.

Reverse mapping tests can give the administrator a false sense of security. There is little evidence that a reverse mapping test provides much in the way of security (see above), and may make troubleshooting in the case of DNS failure more difficult.

It is possible for there to be multiple PTRs at a single reverse tree node. In extreme cases, these multiple PTRs could cause a DNS response to exceed the UDP limit, and fall back to TCP or otherwise exceed the DNS protocol limits. Such a case could be one where the advantages of reverse mapping are exceeded by the disadvantages of the additional burden. This may be of particular significance for "mass virtual hosting" systems, where many hostnames are associated with a single IP.

3.4 Differences in IPv4 and IPv6 operations

RIRs allocate address blocks on ranges of numbers that may be expressed in CIDR [RFC4632] notation. Unfortunately, the IN-ADDR zones were originally based on classful allocations. Guidelines [RFC2317] for delegating on non-octet-aligned boundaries exist, but are not always implemented. There is a similar issue for IP6.ARPA, although in practical terms it is less pressing because the number of addresses affected is different.

RIRs may delegate address space to Local Internet Registries (LIRs), who may perform further delegation. Reverse mapping only works if all the intermediate delegations are correctly maintained. As a result, RIRs find they cannot enforce policies requiring reverse mappings, because they sometimes do not have any relationship with the intermediate party on whom some end-point reverse mapping depends. It is possible that IPv6 will make this "reachover problem" worse, because of the opportunity for longer delegation chains in IPv6.

The much larger address space of IPv6 makes administration of reverse mapping somewhat daunting, in the absence of good tools to help administrators. Some discussion of this issue can be found in [RFC4472], particularly section 7.

The larger address space of IPv6 also makes possible "hiding" active hosts within a large address block: the impracticability of scanning an entire IPv6 network for running network services means that an administrator could effectively conceal running services in an IPv6 network in a way not possible in an IPv4 network. Such hiding would be prevented by a reverse mapping that revealed only existing hosts. If such "hiding" is desirable, it is possible nevertheless to provide reverse mapping for (a large segment of) the network in question, and

then use only a small number of the so-mapped hosts. This approach is consistent with the suggestion outlined in section 4.2, below.

4. Recommendations

4.1 General

There are two sets of actors in respect of reverse mapping: producers of data, who are network operators; and consumers of data, who are users of the Internet. It is desirable that operators of networks produce and maintain reverse mappings. At the same time, consumers of reverse mapping should be careful in relying on reverse mappings. Reverse mappings can be useful, but only when they are used with the appropriate degree of caution about their reliability.

4.2 Delegation considerations

In general, the DNS response to a reverse map query for an address ought to reflect what is supposed to be seen at the address by the machine initiating the query.

It is desirable that Regional Registries and any Local Registries to whom they delegate encourage, or continue to encourage, reverse mappings.

Network operators should define and implement policies and procedures which delegate reverse mappings to their clients who wish to run their own reverse tree DNS services. By the same token, network operators should provide reverse mapping for those users who do not have the resources to do it themselves.

Unless there are strong counter-considerations, such as a high probability of forcing large numbers of queries to use TCP, IP addresses in use within a range and referenced in a forward mapping should have a reverse mapping. Those addresses not in use, and those that are not valid for use (zeros or ones broadcast addresses within a CIDR block) need not have mappings, although it may be useful to indicate that a given range is unassigned. This principle is not intended, however, to create new reverse mapping considerations for addresses discussed in [RFC3330] (and more specifically, the [RFC1918] addresses). While these private use addresses are "assigned", they are assigned in a local way. Therefore, policy with respect to reverse mappings for these addresses is also a local issue. This principle is also not intended to impose undue burden on network operators. It is nevertheless worth considering that not all benefit from an administration practice accrue to the administrator of a network. The consumers of reverse mapping data are often not

the operators of the network that provides the reverse mappings. Users of reverse mapping data report that it is valuable to them.

It should be noted that due to CIDR, many addresses that appear to be otherwise valid host addresses may actually be zeroes or ones broadcast addresses. As such, attempting to audit a site's degree of compliance can only be done with knowledge of the internal routing structure of the site. Nevertheless, any host that originates an IP packet necessarily will have a valid host address, and ought therefore to have a reverse mapping.

4.3 Application considerations

Applications should not rely on reverse mapping for proper operation, although functions that depend on reverse mapping will obviously not work in its absence. Operators and users are reminded that the use of the reverse tree, sometimes in conjunction with a lookup of the name resulting from the PTR record, provides no real security, can lead to erroneous results and generally just increases load on DNS servers. Further, in cases where address block holders fail to properly configure reverse mapping, users of those blocks are penalized.

4.4 Usage and deployment considerations

Site administrators are encouraged to think carefully before adopting any test of reverse delegation, particularly when that test is intended to improve security. The use of reverse mapping does not usually improve security, and should not be a default policy. This is especially true of reverse checks that try to detect matching reverse data. In the absence of the DNS security extensions ([RFC4033],[RFC4034],[RFC4035]) it is not hard for an attacker to falsify the reverse data.

In the context of anti-spam efforts, administrators are reminded that complete rejection of a connection (on the basis of missing or non-matching reverse mapping) is extremely controversial. It may interrupt or prevent the transmission of legitimate mail.

Some users continue to report difficulty in ensuring complete population of the reverse tree by upstream providers. This situation can be corrected by the provision by those providers of reverse mapping; but until the day reverse mapping is universal, complete connection rejection on the basis of missing reverse mapping should be regarded as a last resort.

At the same time, site administrators are cautioned that

administrators at other sites sometimes use reverse mapping as one of several pieces of evidence in evaluating connection traffic, particularly in the context of mail systems and anti-spam efforts. It may be that such evaluations will not cause complete connection failure, but that the evaluations will cause recipients of messages to disregard them as spam.

Administrators are advised to keep in mind the effects of adding a very large number of PTR records for a given reverse mapping. In particular, sites where a very large number of "virtual" host names resolve to the same host may, if the foregoing advice is followed too rigorously, force DNS responses to use TCP. Such cases should be treated as exceptions to the usual rule that reverse mapping entries are to be added for each entry in a forward zone on the Internet, notwithstanding the apparent advice in [RFC1912] that failing to have matching PTR and A records is a configuration or operational error.

5. Security Considerations

This document has no negative impact on security. While it may be argued that lack of PTR record capabilities provides a degree of anonymity, the same goal can be achieved by providing reverse mappings that are opaque to remote users, for all the assigned IP address space. To the extent that forward delegations are already published in the DNS, the anonymity cannot be realized anyway; and delegations not published in the forward zone cannot be distinguished if an opacity strategy is adopted.

By recommending applications avoid using reverse mapping as a security mechanism this document points out that this practice, despite its use by many applications, is an ineffective form of security. Applications should use better mechanisms of authentication.

6. IANA Considerations

There are no IANA considerations or implications that arise from this
document.

7. References

7.1 Normative References

[RFC1035] Mockapetris, P.V., "Domain Names: Implementation Specification", STD13, RFC 1035, November 1987.

[RFC1918] Rekhter, Y., B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2050] Hubbard, K., M. Kosters, D. Conrad, D. Karrenberg, J. Postel, "Internet Registry IP Allocation Guidelines", BCP 12, RFC2050, November 1996.

[RFC2317] Eidnes, H., G. de Groot, P. Vixie, "Classless IN-ADDR.ARPA delegation", BCP 20, RFC 2317, March 1998.

[RFC3596] Thompson, S., C. Huitema, V. Ksinant, M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[RFC4033] Arends, R., R. Austein, M. Larson, D. Massey, S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., R. Austein, M. Larson, D. Massey, S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., R. Austein, M. Larson, D. Massey, S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4632] Fuller, V., T. Li, "Classless Inter-Domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, August 2006.

7.2 Informative References

[Reid1987] Reid, B., "Reflections on Some Recent Widespread Computer Break-Ins", Communications of the ACM, v. 30 no. 2, February 1987, pp 103-105.

[RFC883] Mockapetris, P.V., "Domain names: Implementation specification", RFC883, November 1983.

[RFC1282] Kantor, B., "BSD Rlogin," RFC 1282, December 1991.

[RFC1912] Barr, D., "Common DNS Operational and Configuration Errors", RFC 1912, February 1996.

[RFC2764] Gleeson, B, A. Lin, J. Heinanen, G. Armitage, A. Malis, "A Framework for IP Based Virtual Private Networks", RFC 2764, February 2000.

[RFC3022] Srisuresh, P., K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[RFC3152] Bush, R., "Delegation of IP6.ARPA", BCP 49, RFC 3152, August 2001. (RFC 3152 is obsoleted by RFC 3596, which is not a BCP document.)

[RFC3330] Internet Assigned Numbers Authority, "Special-Use IPv4 Addresses," RFC 3330, September 2002.

[RFC4025] Richardson, M., "A Method for Storing IPsec Keying Material in DNS," RFC 4025, February 2005.

[RFC4322] Richardson, M. and D.H. Redelmeier, "Opportunistic Encryption using the Internet Key Exchange (IKE)," RFC 4322, December 2005.

[RFC4472] Durand, A., J. Ihren, and P. Savola, "Operational Considerations and Issues with IPv6 DNS," RFC 4472, April 2006.

[Venema1992] Venema, W., "TCP Wrapper: Network monitoring, access control, and booby traps," Proceedings of UNIX Security III Symposium, USENIX: Berkeley, 1992, pp 85-92.

8. Acknowledgments

Thanks to Joe Abley, Dean Anderson, Mark Andrews, Stephane Bortzmeyer, Steven Champeon, Kevin Darcy, Kim Davies, John Dickinson, Bruce Gingery, Olafur Gudmundsson, Alfred Hoenes, Tatuya Jinmei, Shane Kerr, Peter Koch, Ed Lewis, George Michaelson, Gary Miller, Russ Mundy, Pekka Savola, and Paul Wouters for their specific input, and to many people who encouraged the writing of this document.

9. Authors' Addresses

Daniel Senie
Amaranth Networks Inc.
324 Still River Road
Bolton, MA 01740

Phone: +1 978 779 5100

EMail: dts@senie.com

Andrew Sullivan
Command Prompt Inc.
176 E Jewett Boulevard
POB 50 PMB 161

White Salmon, WA 98672

Phone: +1 503 667 4564

EMail: ajs@commandprompt.com

9. Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.