Mapping Autonomous Systems Number into the Domain Name System

Donald E. Eastlake 3rd

Status of This Document

This draft, file name draft-ietf-dnssec-as-map-05.txt, is intended to be become a Best Current Practice RFC concerning utilization of the Domain Name System (DNS) to support routing security. Distribution of this document is unlimited. Comments should be sent to the DNS Security Working Group mailing list <dns-security@tis.com> or to the author.

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. Internet-Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet-Drafts as reference material or to cite them other than as a ``working draft'' or ``work in progress.''

To learn the current status of any Internet-Draft, please check the 1id-abstracts.txt listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (East USA), ftp.isi.edu (West USA), nic.nordu.net (North Europe), ftp.nis.garr.it (South Europe), munnari.oz.au (Pacific Rim), or ftp.is.co.za (Africa).

Abstract

One requirement of secure routing is that independent routing entities, such as those identified by Internet Autonomous System Numbers, be able to authenticate messages to each other. Additions have developed to the Domain Name System to enable it to be used for authenticated public key distribution [RFC 2065]. This draft maps all Autonomous System numbers into DNS Domain Names so that the DNS security can be used to distribute their public keys.

[Changes from previous version are to accommodate AS numbers larger than 16 bits and to delegate on decimal boundaries rather than binary boundaries.]

Acknowledgements

The contributions of the following persons, listed in alphabetic order, to this draft are gratefully acknowledged:

Ran Atkinson

Christian Huitema

Tony Li

Michael A. Patton.

Table of Contents

1. Introduction

There are a number of elements required to secure routing in the Internet. One of these is a way that independently operated routing domains be able to authenticate messages to each other.

Sharing a private symmetric key between each pair of such domains is impractical. Assuming 2**16 Autonomous System routing entities, which is what is allowed in current versions of BGP, [RFC 1771], this would imply approximately 2**31 pairs, an impractical number of keys to securely generate, install, and periodically replace.

The solution is to use public key technology whereby each routing domain has a private key it can use to sign messages. Other domains that know the corresponding public key can then authenticate these messages. Such authenticated messages can be used to set up and maintain efficient symmetric keys on an as needed basis.

But how do the domains securely obtain the Autonomous System number to public key mapping?

Extensions have been developed for the Domain Name System that enable it to be conveniently used for authenticated public key distribution [RFC 2065]. A variety of key types can be supported. All that is required is a mapping of Autonomous System numbers into domain names, which is provided by this draft.

It should be noted that the public keys retrieved from DNS will likely be used primarily to authenticate initial connection set up messages. Autonomous Systems that need to converse with any frequency will probably negotiate more efficient symmetric session keys.

2. Autonomous System Number Mapping

Autonomous System (AS) numbers are usually written as decimal number and when blocks of AS numbers are delegated to a registry, it is normally on decimal boundaries. Their current use in BGP is limited to 16 bits providing a maximum value of 65,535. For example, ANS is autonomous system 690. However, there is no inherent size limit in the AS concept. AS numbers are mapped into a domain name as described below.

Write the AS number, as usual, as a decimal number without any "thousands" punctuation. If it is less than 5 digits, add leading zeros to bring it up to five digits. Then simply reverse the order of the digits, put a period between them, and append ".length.in-as.arpa" where "length" is the number of AS digits. This mapping is analogous to the IPv4 address mapping into the in-addr.arpa DNS domain.

Thus the domain name correspond to Autonomous System 690 (decimal) is

0.9.6.0.0.5.in-as.arpa.

the domain corresponding to the largest possible AS number in BGP is

5.3.5.5.6.5.in-as.arpa.

the domain corresponding to AS number 65,000 is

0.0.0.5.6.5.in-as.arpa.

and the domain correspond to a hypothetical future greater than 16 bit AS number 1,234,567 is

7.6.5.4.3.2.1.7.in-as.arpa.

3. Meaning of RRs

The following guidance is given for some resource record (RR) types that could be stored under the names mapped from AS numbers. The KEY RR is given first, followed by the SIG RR, the NXT RR, and then some additional RR types in alphabetic order.

KEY: This type of RR associates a public key with the owner name which, in this case, corresponds to an Autonomous System (AS). Under DNS security as proposed in RFC 2065 the KEY RR can be used to store a variety of digital keys. A KEY for use in securing routing communications between ASs will have the end entity flag bit on, the authentication use prohibited flag bit off, and a protocol byte or flag bit indicating routing communications use. Such a public key can be used to authenticate communications with or between ASs. The existence of such KEY RRs in the primary reason for mapping AS names into the DNS.

SIG: The SIG signature resource record authenticates the RRs that it signs as described in RFC 2065. Assuming the signer who generated the SIG is trustworthy, such as the in-as.arpa zone owner, then the signed RRs can be trusted.

NXT: An NXT RR is used in DNS security to provide authenticated denial of the existence of types and names as described in RFC 2065.

A, AAAA: Type A or AAAA RRs SHOULD NOT be placed at AS nodes. AS domain names are reserved for Autonomous Systems only and should NOT be used for a host or any type of end entity other than an Autonomous System.

CNAME: This type of RR is an alias pointing to another domain name. An AS could have a CNAME pointing to a different AS but this is not likely to be very useful as AS RRs will normally be looked up when the AS number is actually encountered in use.

MX: There is no special use for an MX RR for an AS name. It could point to a host that would accept mail related to that AS.

NS: The presence of NS records under an AS name means that it has been carved out as a subzone. This gives the AS complete control over the zone refresh parameters and control over the creation of inferior names. No special meaning is currently assigned to such inferior names so, although this is not advised, they could be used for hosts or whatever. In this case, the will also be a zone KEY at the AS name, indicated by having the zone flag bit on.

PTR: The part of the forward domain tree that administratively corresponds to the AS SHOULD be indicated by a PTR RR. If some

entity, say example.xx, has several ASs, there would be PTRs to

example.xx from several names in the in-as.arpa hierarchy.

RP: A Responsible Person RR SHOULD appear under each AS name telling you who you should contact in the case of problems with that AS

TXT: Text RRs can be used for comments, postal address, or similar notes under an AS name.

4. Security Considerations

This document concerns a means to map Internet Autonomous System numbers into the Domain Name System (DNS) so that DNS can be used to provide secure distribution of Autonomous System's public keys. The security of the resulting AS to key mapping is dependent on the security of the DNS security extensions and of the DNS zone where the key is stored.

The most obvious way of using the AS keys retrieved from DNS is to authenticate communications with a directly connected AS. However, this does not prove that any routing information exchanged is actually correct and note that routing information communicated over this secured path may be indirectly forwarded from or to yet other ASs.

References

[RFC 1034] - Domain Names - Concepts and Facilities, P. Mockapetris, November 1987

[RFC 1035] - Domain Names - Implementation and Specifications, P. Mockapetris, November 1987.

[RFC 1771] - Y. Rekhter, T. Li, "A Border Gateway Protocol 4 (BGP-4)", 03/21/1995.

[RFC 2065] - Domain Name System Security Extensions, D. Eastlake, C. Kaufman, January 1997.

Author's Address

Donald E. Eastlake 3rd
CyberCash, Inc.
318 Acton Street
Carlisle, MA 01741 USA

Telephone: +1 508 287 4877
+1 703 620-4200 (main office, Reston, VA)
FAX: +1 508 371 7148
EMail: dee@cybercash.com

Expiration and File Name

This draft expires January 1998.

Its file name is draft-ietf-dnssec-as-map-05.txt.