Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 12, 2011

T. Manderson
ICANN
R L. Barnes
M. Lepinski
BBN

June 10, 2011

Providing first class geographical location statements for Internet Number Resources
draft-manderson-sidr-geo-01.txt

Abstract

This document describes the construction and use of the RPKI-GEO record. This record provides first class informational statements pertaining to the geographical attributes of the allocated Internet Number Resources.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 12, 2011.

Table of Contents

1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

The existence of this object comes from a desire from a number of Internet networking entities to use geographical awareness in designing, operating, and maintaining networks. These desires are briefly described here. There are of course many other efforts external to the IETF and won't be described here. Further awareness of these efforts is left to the reader.

This document describes the construction, use, and interpretation of the RPKI-GEO record. This record provides first class informational attestations pertaining to the geographical attributes relating to the Internet Number Resources (INRs) as published by the holder of the resources. The use of the geographical data is of an informational nature and provides a consistent and validatable approach to asserting the location properties of allocated resources. To maintain consistency implementers and readers should consider the 9 rules in section 3 of [RFC5491].

The geographic attestations made in this object are made by the certificate maintainer and their validity and accuracy is in the hands of the certificate maintainer. It is left to the relying party as how much trust is given to the geographic data provided by the certificate maintainer.

2.1. Network Providers

Customer focused network providers can use this object to categorically describe the geographical attributes of customer networks that will allow content providers (individually or via GEO IP services) to more accurately direct customer traffic. The benefits of this can be more consistent service provision, or improved traffic flows in both latency and content models.

Anycast operations [RFC4786] might also benefit from the provision of geographic information in this form. Publishing a consistent awareness of the location of anycasted service nodes may help network operators improve their network designs.

2.2. Content Providers

A number of content providers use the awareness they have regarding the location of IP addresses to reduce the latency of provision and to selectively provide content to particular locations. If a network provider publishes geographic information in they will allow content providers to more easily direct users traffic to their closest provision point.

2.3. Security Providers

Computer emergency response teams (CERTs) and law enforcement agencies (LEAs) are often concerned with where a network exists as this often predicates the efforts required to address concerns of a security nature given jurisdictional borders. For CERTs, this knowledge is helpful for identifying an appropriate regional contact for assistance when investigating computer system compromise, as well as for statistical analysis purposes (for example, to geographically map the incidence of occurrence over time). For law enforcement purposes, attribution of network activity will likely have a high priority. Correctness in published information will improve the likelihood of successful resolution of security events.

2.4. Geo-Location (GEO) IP services

At present GEO IP service providers glean IP location information from many sources. Its accuracy is always subject to the authoritativeness of the source in addition to the specificity of the provided information. GEOIP providers often have content providers and Security Providers as users of their information, therefore correctness of information is far reaching.

2.5. Research

There is a constant and ongoing effort to investigate and analyse the global internet routing system from many different perspectives. One perspective is related to the geographical position of BGP [RFC4271] speakers and the terrestrial location of the route propagation. Recording of such information by passive BGP listeners in MRT format is described in the MRT BGP routing information export format with geo-location extensions [I-D.ietf-grow-geomrt]. If this information is provided in the RPKI, close approximation of location can be used to model anomalous and unintended routing events in geospatial terms.

3. Required Reading

The assumption is made that the reader comprehends the RPKI, the RPKI Repository Structure, and the various RPKI objects described in the following: [I-D.ietf-sidr-arch], [I-D.ietf-sidr-res-certs], [I-D.ietf-sidr-signed-object].

4. RPKI-GEO Structure

The structure of the RPKI-GEO object follows the description and the generic RPKI validation as described in Signed Object Template for the Resource Public Key Infrastructure [I-D.ietf-sidr-signed-object]

4.1. CMS Packaging

The eContentType of the RPKI-GEO object in the encapContentInfo (signed content) section of object is defined as rRPKIGEO with the numerical value of [TO BE ASSIGNED].

4.2. eContent

The content of a RPKI-GEO object identifies a set of Internet Number Resources and the HELD Identity [RFC6155] or HELD Dereference [I-D.ietf-geopriv-deref-protocol] URI pertaining to the INRs.

The ASN.1 for the RPKI-GEO object is as follows:

```
   rPKIGEO ::= SEQUENCE {
           Version      [0] INTEGER DEFAULT 0,
           geoLocs      SEQUENCE (SIZE(1..MAX)) OF geoObjects
           }

   geoObjects ::= SEQUENCE {
       inrSET           SEQUENCE (SIZE(1..MAX)) OF inrObjects,
       heldURI      UTF8String,
       heldTYPE     BOOLEAN DEFAULT 0,
       }


   inrObjects ::= SEQUENCE {
      asIDs         SEQUENCE (SIZE(0..MAX)) OF ASID,
      ipAddrBlocks  SEQUENCE (SIZE(0..MAX)) OF IPAddressFam
      }

   IPAddressFam ::= SEQUENCE {
      addressFam    OCTET STRING (SIZE (2..3)),
      addresses     SEQUENCE (SIZE (1..MAX)) OF IPAddress
      }

   IPAddress ::= SEQUENCE {
      address       IPAddress,
      length        INTEGER
      }

   ASID ::= INTEGER

   IPAddress ::= BIT STRING

   }
```

4.3. rPKIGEO data elements

4.3.1. Version

The version number of this version of the rPKIGEO object MUST be 0.

4.3.2. geoLocs

This field is a sequence of geoObjects.

4.3.3. geoObjects

Each geoObject contains a sequence (inrSET) of inrObjects, a heldURI, and a heldTYPE. The heldURI is a URI to either a HELD identity or

HELD dereference. The boolean heldTYPE specifies the HELD service choice, 0 for identity and 1 for dereference.

4.3.4. inrObjects

Each inrObjects contains a sequence (asIDs) of ASID, and a sequence (ipAddrBlocks) of IPAddressfam. the minimum number of both sequences is zero (0) to allow the maintainer of the object to specify only AS numbers or only IP address blocks, or both.

4.3.5. IPAddressFam

The IPAddressFam contains the Address Family Identifier (AFI) of an IP address family in addressFam as 0001 for IPv4 and 0002 for IPv6. Only IPv4 and IPv6 is supported. The sequence 'addresses' contains the IP prefixes.

5. RPKI-GEO Validation

After the generic signed objects validation [I-D.ietf-sidr-signed-object] has been performed, the Version number field within the payload is checked. The payload data is checked against the profile defined in this document. All of these checks MUST pass for the RPKI-GEO payload to be considered valid and made available for use.

6. IANA Considerations

This document requests IANA to add the .geo extension to the RPKI file extension namespace.

7. Security Considerations

The RPKI object described here is used in a descriptive nature and provides information that is useful in the analysis and design of routing systems. As such, the authors believe that it does not constitute an additional security risk. It is recommended that the issuers of the RPKI-GEO objects consider their own privacy and physical securiy concerns before supplying geographical coordinates through the RPKI.

8. Acknowledgments

The authors would like to thank a number of people who have reviewed this document and have provided helpful input or guidance. They are Jason Smith (CERT Australia), Joel Hatton (AusCERT), Jason Ketola (Maxmind), Matthew Moyle-Croft (Internode), Ernest Foo (QUT ISI), George Mohay (QUT ISI), and David Graham (QLD Police). Some folks who put effort into reviewing this document chose to remain anonymous. Our thanks and appreciation goes to those people.

9. References

9.1. Normative References

[I-D.ietf-geopriv-deref-protocol]
Winterbottom, J., Tschofenig, H., Schulzrinne, H., Thomson, M., and M. Dawson, "A Location Dereferencing Protocol Using HELD", draft-ietf-geopriv-deref-protocol-02 (work in progress), December 2010.

[I-D.ietf-sidr-arch]
Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", draft-ietf-sidr-arch-13 (work in progress), May 2011.

[I-D.ietf-sidr-res-certs]
Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", draft-ietf-sidr-res-certs-22 (work in progress), May 2011.

[I-D.ietf-sidr-signed-object]
Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure", draft-ietf-sidr-signed-object-04 (work in progress), May 2011.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC5139] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", RFC 5139, February 2008.

[RFC5491] Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", RFC 5491, March 2009.

[RFC6155] Winterbottom, J., Thomson, M., Tschofenig, H., and R. Barnes, "Use of Device Identity in HTTP-Enabled Location Delivery (HELD)", RFC 6155, March 2011.

9.2. Informative References

[I-D.ietf-grow-geomrt]
Manderson, T., "MRT BGP routing information export format with geo-location extensions", draft-ietf-grow-geomrt-02 (work in progress), May 2011.

[RFC4786] Abley, J. and K. Lindqvist, "Operation of Anycast Services", BCP 126, RFC 4786, December 2006.

Authors' Addresses

Terry Manderson
ICANN

Email: terry.manderson@icann.org

Richard L. Barnes
BBN

Email: rbarnes@bbn.com

Matt Lepinski
BBN

Email: mlepinski@bbn.com