

Global Routing Operations
Internet-Draft
Intended status: Informational
Expires: April 14, 2016

K. Sriram
D. Montgomery
US NIST
D. McPherson
E. Osterweil
Verisign, Inc.
B. Dickson
Twitter, Inc.
October 12, 2015

Problem Definition and Classification of BGP Route Leaks
draft-ietf-grow-route-leak-problem-definition-03

Abstract

A systemic vulnerability of the Border Gateway Protocol routing system, known as 'route leaks', has received significant attention in recent years. Frequent incidents that result in significant disruptions to Internet routing are labeled "route leaks", but to date we have lacked a common definition of the term. In this document, we provide a working definition of route leaks, keeping in mind the real occurrences that have received significant attention. Further, we attempt to enumerate (though not exhaustively) different types of route leaks based on observed events on the Internet. We aim to provide a taxonomy that covers several forms of route leaks that have been observed and are of concern to Internet user community as well as the network operator community.

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 April 14, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Working Definition of Route Leaks	3
3.	Classification of Route Leaks Based on Documented Events . .	3
3.1.	Type 1: U-Shaped Turn with Full Prefix	4
3.2.	Type 2: Lateral ISP-ISP-ISP Leak	5
3.3.	Type 3: Leak of Transit-Provider Prefixes to Peer	5
3.4.	Type 4: Leak of Peer Prefixes to Transit Provider	5
3.5.	Type 5: U-Shaped Turn with More Specific Prefix	6
3.6.	Type 6: Prefix Re-Origination with Data Path to Legitimate Origin	6
3.7.	Type 7: Accidental Leak of Internal Prefixes and More Specifics	6
4.	Additional Comments about the Classification	7
5.	Summary	7
6.	Security Considerations	7
7.	IANA Considerations	8
8.	Acknowledgements	8
9.	Informative References	8
	Authors' Addresses	11

[1.](#) Introduction

Frequent incidents [[Huston2012](#)][[Cowie2013](#)][[Toonk2015-A](#)][[Toonk2015-B](#)][[Cowie2010](#)][[Madory](#)][[Zmijewski](#)][[Paseka](#)][[LRL](#)][[Khare](#)] that result in significant disruptions to Internet routing are commonly called "route leaks". Examination of the details of some of these incidents reveals that they vary in their form and technical details. Before we can discuss solutions to "the route leak problem" we need a clear, technical definition of the problem and its most common forms. In [Section 2](#), we provide a working definition of route leaks, keeping in view many recent incidents that have received significant attention.

Further, in [Section 3](#), we attempt to enumerate (though not exhaustively) different types of route leaks based on observed events on the Internet. We aim to provide a taxonomy that covers several forms of route leaks that have been observed and are of concern to Internet user community as well as the network operator community. This document builds on and extends earlier work in the IETF by Dickson [[draft-dickson-sidr-route-leak-def](#)][[draft-dickson-sidr-route-leak-regts](#)].

2. Working Definition of Route Leaks

A proposed working definition of route leak is as follows:

A "route leak" is the propagation of routing announcement(s) beyond their intended scope. That is, an AS's announcement of a learned BGP route to another AS is in violation of the intended policies of the receiver, the sender and/or one of the ASes along the preceding AS path. The intended scope is usually defined by a set of local redistribution/filtering policies distributed among the ASes involved. Often, these intended policies are defined in terms of the pair-wise peering business relationship between ASes (e.g., customer, transit provider, peer). For literature related to AS relationships and routing policies, see [[Gao](#)] [[Luckie](#)] [[Gill](#)]. For measurements of valley-free violations in Internet routing, see [[Anwar](#)] [[Giotsas](#)] [[Wijchers](#)].

The result of a route leak can be redirection of traffic through an unintended path which may enable eavesdropping or traffic analysis, and may or may not result in an overload or black-hole. Route leaks can be accidental or malicious, but most often arise from accidental misconfigurations.

The above definition is not intended to be all encompassing. Perceptions vary widely about what constitutes a route leak. Our aim here is to have a working definition that fits enough observed incidents so that the IETF community has a basis for developing solutions for route leak detection and mitigation.

3. Classification of Route Leaks Based on Documented Events

As illustrated in Figure 1, a common form of route leak occurs when a multi-homed customer AS (such as AS3 in Figure 1) learns a prefix update from one transit provider (ISP1) and leaks the update to another transit provider (ISP2) in violation of intended routing policies, and further the second transit provider does not detect the leak and propagates the leaked update to its customers, peers, and transit ISPs.

- o Example incidents: Examples of Type 1 route-leak incidents are (1) the Dodo-Telstra incident in March 2012 [[Huston2012](#)], (2) the Moratel-PCCW route leak of Google prefixes in November 2012 [[Paseka](#)], (3) the VolumeDrive-Atrato incident in September 2014 [[Madory](#)], (4) the Hathway-Airtel route leak of 336 Google prefixes causing widespread interruption of Google services in Europe and Asia [[Toonk2015-A](#)], and (5) the massive Telekom Malaysia route-

leaks of about 179,000 prefixes, which in turn Level3 accepted and propagated [[Toonk2015-B](#)].

3.2. Type 2: Lateral ISP-ISP-ISP Leak

Description: The term "lateral" here is synonymous with "non-transit" or "peer-to-peer". This type of route leak typically occurs when, for example, three sequential ISP peers (e.g. ISP-A, ISP-B, and ISP-C) are involved, and ISP-B receives a route from ISP-A and in turn leaks it to ISP-C. The typical routing policy between laterally (i.e. non-transit) peering ISPs is that they should only propagate to each other their respective customer prefixes.

- o Example incidents: In [[Mauch-nanog](#)][Mauch], route leaks of this type are reported by monitoring updates in the global BGP system and finding three or more very large ISP ASNs in a sequence in a BGP update's AS path. Mauch [[Mauch](#)] observes that these are anomalies and potentially route leaks because very large ISPs such as ATT, Sprint, Verizon, and Globalcrossing do not in general buy transit services from each other. However, he also notes that there are exceptions when one very large ISP does indeed buy transit from another very large ISP, and accordingly exceptions are made in his detection algorithm for known cases.

3.3. Type 3: Leak of Transit-Provider Prefixes to Peer

Description: This type of route leak occurs when an offending AS leaks routes learned from its transit provider to a lateral (i.e. non-transit) peer.

- o Example incidents: The incidents reported in [[Mauch](#)] include the Type 3 leaks.

3.4. Type 4: Leak of Peer Prefixes to Transit Provider

Description: This type of route leak occurs when an offending AS leaks routes learned from a lateral (i.e. non-transit) peer to its (the AS's) own transit provider. These leaked routes typically originate from the customer cone of the lateral peer.

- o Example incidents: Some of the example incidents cited for Type 1 route leaks above are also inclusive of Type 4 route leaks. For instance, in the Dodo-Telstra incident [[Huston2012](#)], the leaked routes from Dodo to Telstra included routes that Dodo learned from its transit providers as well as lateral peers.

3.5. Type 5: U-Shaped Turn with More Specific Prefix

Description: A multi-homed AS learns a route from one upstream ISP and announces a subprefix (subsumed in the prefix) to another upstream ISP. The AS path in the update is not altered. Update is crafted by the offending AS to have a subprefix to maximize the success of the attack while reverse path is kept open by the path poisoning techniques as in [\[Kapela-Pilosov\]](#). Data packets reach the legitimate destination albeit via the offending AS.

- o Example incidents: One example is the demo performed at DEFCON-16 in August 2008 [\[Kapela-Pilosov\]](#). Another example is the earlier-mentioned incident of route leaks from Telekom Malaysia via Level3, in which out of about 179,000 total route-leaked prefixes, about 10,000 were more specifics of previously announced less specific prefixes [\[Toonk2015-B\]](#). [Note: An attacker who deliberately performs a Type 1 route leak (with full prefix) can just as easily perform a Type 5 route leak (with subprefix) to achieve a greater impact.]

3.6. Type 6: Prefix Re-Origination with Data Path to Legitimate Origin

Description: A multi-homed AS learns a route from one upstream ISP and announces the prefix to another upstream ISP as if it is being originated by it (i.e. strips the received AS path, and re-originate the prefix). This can be called re-origination or mis-origination. However, somehow (not attributable to the use of path poisoning trick by the offending AS) a reverse path is present, and data packets reach the legitimate destination albeit via the offending AS. But sometimes the reverse path may not be there, and data packets get dropped following receipt by the offending AS.

- o Example incidents: Examples of Type 6 route leak include (1) the China Telecom incident in April 2010 [\[Hiran\]](#)[\[Cowie2010\]](#)[\[Labovitz\]](#), (2) the Belarusian GlobalOneBel route leak incidents in February-March 2013 and May 2013 [\[Cowie2013\]](#), (3) the Icelandic Opin Kerfi-Simmin route leak incidents in July-August 2013 [\[Cowie2013\]](#), and (4) the Indosat route leak incident in April 2014 [\[Zmijewski\]](#).

3.7. Type 7: Accidental Leak of Internal Prefixes and More Specifics

Description: An offending AS simply leaks its internal prefixes to one or more of its transit-provider ASes and/or ISP peers. The leaked internal prefixes are often more specifics subsumed by an already announced less specific prefix. The more specifics were not intended to be routed in eBGP. Further, the AS receiving those leaks fails to filter them. Typically these leaked announcements are due to some transient failures within the AS; they are short-lived, and

typically withdrawn quickly following the announcements. However, these more specifics may momentarily cause the routes to be preferred over other aggregate route announcements, thus redirecting traffic from its normal best path.

- o Example incidents: Leaks of internal routes occur frequently (e.g. multiple times in a week), and the number of prefixes leaked range from hundreds to thousands per incident. One highly conspicuous and widely disruptive leak of internal routes happened recently in August 2014 when AS701 and AS705 leaked about 22,000 more specifics of already announced aggregates [[Huston2014](#)][[Toonk2014](#)].

4. Additional Comments about the Classification

It is worth noting that Types 1 through 4 are similar in that a route is leaked in violation of policy in each case, but what varies is the context of the leaked-route source AS and destination AS roles.

It is also worth noting that Type 5 route leak involves a subprefix and is a special case of Type 1, which involves a full prefix. Similarly, subprefix versions of other types of route leaks may also be considered, for example, for Types 2, 3, and 4. Similarly, Type 6 (i.e. prefix mis-origination with data path to legitimate origin) can be also conceived to happen in conjunction with Types 2, 3, and 4. While these possibilities are acknowledged, simply enumerating more types to consider all such special cases does not add value as far as solution development for route leaks is concerned. Hence, the special cases mentioned here are not included in enumerating route leak types.

5. Summary

We attempted to provide a working definition of route leak. We also presented a taxonomy for categorizing route leaks. It covers not all but at least several forms of route leaks that have been observed and are of concern to Internet user and network operator communities. We hope that this work provides the IETF community a basis for pursuing possible BGP enhancements for route leak detection and mitigation.

6. Security Considerations

No security considerations apply since this is a problem definition document.

7. IANA Considerations

No updates to the registries are suggested by this document.

8. Acknowledgements

The authors wish to thank Jared Mauch, Jeff Haas, Warren Kumari, Amogh Dhamdhere, Jakob Heitz, Geoff Huston, Randy Bush, Ruediger Volk, Andrei Robachevsky, Charles van Niman, Chris Morrow, and Sandy Murphy for comments, suggestions, and critique. The authors are also thankful to Padma Krishnaswamy, Oliver Borchert, and Okhee Kim for their comments and review.

9. Informative References

- [Anwar] Anwar, R., Niaz, H., Choffnes, D., Cunha, I., Gill, P., and N. Katz-Bassett, "Investigating Interdomain Routing Policies in the Wild", ACM Internet Measurement Conference (IMC), October 2015, <<http://www.cs.usc.edu/assets/007/94928.pdf>>.
- [Cowie2010] Cowie, J., "China's 18 Minute Mystery", Dyn Research/Renesys Blog, November 2010, <<http://research.dyn.com/2010/11/chinas-18-minute-mystery/>>.
- [Cowie2013] Cowie, J., "The New Threat: Targeted Internet Traffic Misdirection", Dyn Research/Renesys Blog, November 2013, <<http://research.dyn.com/2013/11/mitm-internet-hijacking/>>.
- [[draft-dickson-sidr-route-leak-def](#)] Dickson, B., "Route Leaks -- Definitions", IETF Internet Draft (expired), October 2012, <<https://tools.ietf.org/html/draft-dickson-sidr-route-leak-def-03>>.
- [[draft-dickson-sidr-route-leak-reqts](#)] Dickson, B., "Route Leaks -- Requirements for Detection and Prevention thereof", IETF Internet Draft (expired), March 2012, <<http://tools.ietf.org/html/draft-dickson-sidr-route-leak-reqts-02>>.

- [Gao] Gao, L. and J. Rexford, "Stable Internet routing without global coordination", IEEE/ACM Transactions on Networking, December 2001, <<http://www.cs.princeton.edu/~jrex/papers/sigmetrics00.long.pdf>>.
- [Gill] Gill, P., Schapira, M., and S. Goldberg, "A Survey of Interdomain Routing Policies", ACM SIGCOMM Computer Communication Review, January 2014, <<http://www.cs.bu.edu/~goldbe/papers/survey.pdf>>.
- [Giotsas] Giotsas, V. and S. Zhou, "Valley-free violation in Internet routing - Analysis based on BGP Community data", IEEE ICC 2012, June 2012.
- [Hiran] Hiran, R., Carlsson, N., and P. Gill, "Characterizing Large-scale Routing Anomalies: A Case Study of the China Telecom Incident", PAM 2013, March 2013, <<http://www3.cs.stonybrook.edu/~phillipa/papers/CTelecom.html>>.
- [Huston2012] Huston, G., "Leaking Routes", March 2012, <<http://labs.apnic.net/blabs/?p=139/>>.
- [Huston2014] Huston, G., "What's so special about 512?", September 2014, <<http://labs.apnic.net/blabs/?p=520/>>.
- [Kapela-Pilosov] Pilosov, A. and T. Kapela, "Stealing the Internet: An Internet-Scale Man in the Middle Attack", DEFCON-16 Las Vegas, NV, USA, August 2008, <<https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf>>.
- [Khare] Khare, V., Ju, Q., and B. Zhang, "Concurrent Prefix Hijacks: Occurrence and Impacts", IMC 2012, Boston, MA, November 2012, <<http://www.cs.arizona.edu/~bzhang/paper/12-imc-hijack.pdf>>.
- [Labovitz] Labovitz, C., "Additional Discussion of the April China BGP Hijack Incident", Arbor Networks IT Security Blog, November 2010, <<http://www.arbornetworks.com/asert/2010/11/additional-discussion-of-the-april-china-bgp-hijack-incident/>>.

- [LRL] Khare, V., Ju, Q., and B. Zhang, "Large Route Leaks", Project web page, 2012, <<http://nrl.cs.arizona.edu/projects/lrsl-events-from-2003-to-2009/>>.
- [Luckie] Luckie, M., Huffaker, B., Dhamdhere, A., Giotsas, V., and kc. claffy, "AS Relationships, Customer Cones, and Validation", IMC 2013, October 2013, <<http://www.caida.org/~amogh/papers/asrank-IMC13.pdf>>.
- [Madory] Madory, D., "Why Far-Flung Parts of the Internet Broke Today", Dyn Research/Renesys Blog, September 2014, <<http://research.dyn.com/2014/09/why-the-internet-broke-today/>>.
- [Mauch] Mauch, J., "BGP Routing Leak Detection System", Project web page, 2014, <<http://puck.nether.net/bgp/leakinfo.cgi/>>.
- [Mauch-nanog] Mauch, J., "Detecting Routing Leaks by Counting", NANOG-41 Albuquerque, NM, USA, October 2007, <<https://www.nanog.org/meetings/nanog41/presentations/mauch-lightning.pdf>>.
- [Paseka] Paseka, T., "Why Google Went Offline Today and a Bit about How the Internet Works", CloudFare Blog, November 2012, <<http://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about/>>.
- [Toonk2014] Toonk, A., "What caused today's Internet hiccup", August 2014, <<http://www.bgpmon.net/what-caused-todays-internet-hiccup/>>.
- [Toonk2015-A] Toonk, A., "What caused the Google service interruption", March 2015, <<http://www.bgpmon.net/what-caused-the-google-service-interruption/>>.
- [Toonk2015-B] Toonk, A., "Massive route leak causes Internet slowdown", June 2015, <<http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/>>.

[Wijchers]

Wijchers, B. and B. Overeinder, "Quantitative Analysis of BGP Route Leaks", RIPE-69, November 2014, <<http://ripe69.ripe.net/presentations/157-RIPE-69-Routing-WG.pdf>>.

[Zmijewski]

Zmijewski, E., "Indonesia Hijacks the World", Dyn Research/Renesys Blog, April 2014, <<http://research.dyn.com/2014/04/indonesia-hijacks-world/>>.

Authors' Addresses

Kotikalapudi Sriram
US NIST

Email: ksriram@nist.gov

Doug Montgomery
US NIST

Email: dougmont@nist.gov

Danny McPherson
Verisign, Inc.

Email: dmcpherson@verisign.com

Eric Osterweil
Verisign, Inc.

Email: eosterweil@verisign.com

Brian Dickson
Twitter, Inc.

Email: bdickson@twitter.com

