GROW
Internet-Draft
Intended status: Informational
Expires: November 1, 2014

D. McPherson
Verisign, Inc.
S. Amante
Level 3 Communications, Inc.
E. Osterweil
Verisign, Inc.
D. Mitchell
Twitter, Inc.
April 30, 2014

Route-Leaks & MITM Attacks Against BGPSEC
draft-ietf-grow-simple-leak-attack-bgpsec-no-help-04

Abstract

This document describes a very simple attack vector that illustrates how RPKI-enabled BGPSEC machinery as currently defined can be easily circumvented in order to launch a Man In The Middle (MITM) attack via BGP. It is meant to serve as input to the IETF's Global Routing Operations Working group (GROW) during routing security requirements discussions and subsequent specification.

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 November 1, 2014.

Table of Contents

1. Introduction

This document describes a very simple attack vector that illustrates how RPKI-enabled BGPSEC [I-D.ietf-sidr-bgpsec-protocol] machinery, as currently defined, can be easily circumvented in order to launch a Man In The Middle (MITM) attack via BGP [RFC4271]. It is meant to serve as input to the IETF's Global Routing Operations Working Group (GROW) during routing security requirements discussions and subsequent specification.

This draft shows evidence that the attack vector described herein is extremely common, with over 9.6 million candidate instances being recorded since 2007. As a result of this evidence and additional contextual knowledge, the authors believe the capability to prevent leaks and MITM leak-attacks should be a primary engineering objective in any secure routing architecture.

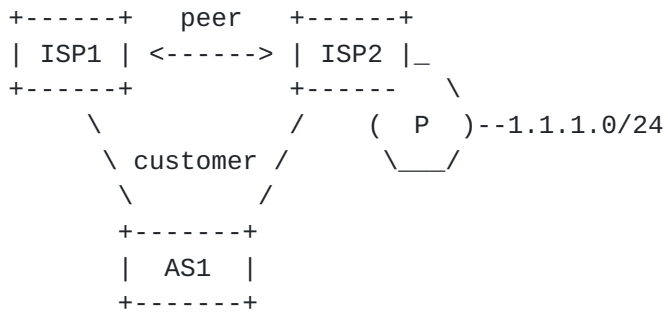
While the formal definition of a 'route-leak' has proven elusive in literature, the rampant occurrence and persistent operational threats have proven to be anything but uncommon. This document is intended to serve as a proof of existence for the referenced attack vector and any supplementary formal models are left for future work.

2. Discussion

In order to understand how a Man In the Middle (MITM) Attack can be conducted using this attack vector, refer to the below example.

Assume a multi-homed Autonomous System (AS), AS1, connects to two ISPs (ISP1 and ISP2) and wishes to insert themselves in the data-path between target network (prefix P) connected to ISP2 and systems in ISP1's network in order to proceed with an MITM attack.

Assume that an RPKI-enabled BGPSEC deployment [I-D.ietf-sidr-bgpsec-protocol] is currently operational by all parties in the scenario and functioning as designed.



This figure depicts a multi-homed AS, AS1, that is a customer connected to two upstream ISPs (ISP1 and ISP2). ISP2 has a second customer, P, that is assigned prefix 1.1.1.0/24.

Network operators on the Internet today typically prefer customer routes over routes learned from bi-lateral or settlement free peers. Network operators commonly accomplish this via application of one or more BGP [RFC4271] Path Attributes, most commonly, LOCAL_PREF as illustrated in [RFC1998], that are evaluated earlier in the BGP Path Selection process than AS_PATH length.

As currently defined, [I-D.ietf-sidr-bgpsec-protocol] only provides two methods for validating an announced NLRI:

1. Is the Autonomous System authorized to originate an IP prefix?
2. Is the AS_PATH (or any similarly derived attribute such as BGPSEC_Path) in the route the same as the list of ASes through which the NLRI traveled?

In order for an attacker (AS1) to divert traffic from ISP1 toward prefix P through their AS, AS1 must simply fail to scope the propagation of the target prefix P (1.1.1.0/24), received from ISP2. This is completed by announcing a syntactically correct BGPSEC update for prefix P to ISP1.

This vulnerability is what authors refer to as a 'route-leak' or 'leak-attack', respectively, when intent aligns with actions. It is important to note that the default behavior in BGP [RFC4271] is to announce all best paths to external BGP peers, unless explicitly configured otherwise by a BGP speaker. Because ISP1 prefers prefixes learned from customers (AS1) over prefixes learned from peers (ISP2), ISP1 begins forwarding traffic for prefix P through the attacker (AS1), thus successfully completing the route hijack.

It is important to note that the route-leaks described herein are not illegal NLRI origins. These are cases in which routes are propagated with an authentic origin AS, as per [RFC6480]. Furthermore, the BGPSEC route for prefix P is propagated through intermediate ASN's, in this case AS1, that each applies a valid BGPSEC_Path attribute to the route. Ultimately, ISP1 receives two, valid BGPSEC routes for prefix P, (one directly from ISP2 and one directly from AS1); however, due to the local policy implemented within ISP1, it prefers the customer route, due to higher LOCAL_PREF, received from customer AS1. This will cause ISP1 to misdirect packets through a invalid intermediate ASN, AS1, to reach prefix P.

It should be understood that any multi-homed AS can potentially launch such an attack, even if through simple misconfiguration, which

is a common occurrence on the Internet. As a matter of fact, advertising these prefixes is the default behavior of many BGP implementations and explicit action must be taken to not advertise all prefixes learned in BGP.

Such occurrences have been historically archived and presented to the operational community since 2007 [NANOG_LEAK_TALK]. To date, over 9.6 million such events have been recorded within the [ROUTE_LEAK_DETECTION_TOOL].

Said dataset serves as a basis for analysis and likely contains a degree of false positives. Even while some may debate how many of the incidents were malicious route-leaks versus accidental misconfiguration that resulted in leaked routes, the size of the dataset provides evidence of the magnitude of the issue.

Determination of intent in these situations is difficult to ascertain and requires preventative controls be put in place to mitigate occurrences of route-leaks. In order to illustrate the difficulty in determining intent, consider the events that transpired on November 6th, 2012 [LEAK_ATTACK_ON_GOOGLE].

Google is the largest Internet site and processes billions of end-user transactions per day. It became unreachable for approximately 27 minutes. At their scale, an outage of 27 minutes is extremely visible and, most likely, a financially measurable event. In this example, its services became unreachable because a BGP peer improperly propagated the company's prefixes. Because this was a highly visible outage, there exists a public acknowledgment of improper intent executed by one of Google's peers, proving that [RFC6480] and [I-D.ietf-sidr-bgpsec-protocol] would be unable to detect or prevent this type of attack.

In an environment where [I-D.ietf-sidr-bgpsec-protocol] is fully deployed, it is expected that there would be substantial assurances as to the semantic integrity of the AS_PATH or BGPSEC_Path attribute. An operator would expect that such an attribute would accurately reflect the attacker's ASN in the appropriate location of the BGPSEC_Path. Unfortunately, as currently designed, [I-D.ietf-sidr-bgpsec-protocol] is unable to distinguish whether an ASN is allowed, by policy, to add their ASN within the BGPSEC_Path attribute before the BGP update is propagated to downstream ASNs. This proves that mechanisms defined in [I-D.ietf-sidr-bgpsec-protocol] would not stop an attacker from completing this type of attack.

It should be noted that the attack scenario described in this document can be mitigated by performing proper route filtering

techniques.

Discussion of out of band methods to mitigate this attack are important; albeit beyond the scope of this document. This document is meant to provide input into routing protocol design choices being considered within the IETF, and to foster discussion of the practical implications of "policy" and "intent" in operational routing system security.

3. Acknowledgements

The authors gratefully acknowledge the contributions of John Curran.

4. IANA Considerations

There are no actions for IANA in the document.

5. Security Considerations

This document describes an attack on an RPKI-enabled BGPSEC and is meant to inform the IETF community that this vulnerability exists as a result of route-leaks and attacks that conform to this type of behavior, and that operators should not assume that that work items and designs address these operational security issues.

The authors believe the capability to prevent route-leaks and leak-attacks should be a primary engineering objective in any secure routing architecture.

6. Informative References

[I-D.ietf-sidr-bgpsec-protocol]
Lepinski, M., "BGPSEC Protocol Specification", November 2013.

[LEAK_ATTACK_ON_GOOGLE]
CloudFlare, CF., "Why Google Went Offline Today and a Bit about How the Internet Works", November 2012, <http://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about>.

[NANOG_LEAK_TALK]
Mauch, J., "Detecting Routing Leaks by Counting", October 2007, <http://www.nanog.org/meetings/nanog41/

presentations/mauch-lightning.pdf>.

[RFC1998] Chen, E. and T. Bates, "An Application of the BGP Community Attribute in Multi-home Routing", RFC 1998, August 1996.

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

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, February 2012.

[ROUTE_LEAK_DETECTION_TOOL]
Mauch, J., "BGP Routing Leak Detection System Routing Leak Detection System", September 2007, <http://puck.nether.net/bgp/leakinfo.cgi>.

Authors' Addresses

Danny McPherson
Verisign, Inc.
12061 Bluemont Way
Reston, VA 20190
USA

Phone: +1 703.948.3200
Email: dmcpherson@verisign.com

Shane Amante
Level 3 Communications, Inc.
1025 Eldorado Boulevard
Broomfield, CO 80021
US

Phone: +1 720.888.1000
Email: shane@level3.net

Eric Osterweil
Verisign, Inc.
12061 Bluemont Way
Reston, VA 20190
USA

Phone: +1 703.948.3200
Email: eosterweil@verisign.com

Dave Mitchell
Twitter, Inc.
1355 Market Street, Suite 900
San Francisco, CA 94103
USA

Email: dave@twitter.com