SIDR Working Group
Internet Draft
Expires: March 2007

Dai GuangMing
Z. Ye
Huawei Technologies
FEKI Ines
France Telecom
September 25, 2006

BGP UPDATE Advertisement Restriction
draft-dai-sidr-bgp-advertisement-00.txt

Status of this Memo

Copyright Notice

Abstract

SIDR working group is working on an extended architecture for interdomain routing security framework. One of the functions that this architecture should provide is origin authentication of prefixes for BGP, i.e. a BGP speaker must be able to determine whether an AS (autonomous system) is authorized to originate certain prefixes. This draft documents some ideas from the perspective of internal control in order to alleviate this problem.

Conventions used in this document

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 [RFC-2119]

Table of Contents

1. Introduction

1.1. Problem Description

It has been observed that BGP is vulnerable to several types of attacks (refer to [VULN]). Because of lacking inherent security mechanisms, a UPDATE message receiver can not tell whether the origin AS listed in AS_PATH is authorized to originate the prefixes. Because of misconfiguration or deliberate attacks, wrong prefixes may be propagated through UPDATE messages which may cause traffic redirection, black hole and some other problems.

1.2. Existing solutions

[SBGP] proposes an autonomous system numbers and prefix allocation based PKI to provide an authentication infrastructure to solve this problem.

[SoBGP] solves it in a similar ways except that it uses web-of-trust model for AS identity authentication.

[IRR] is a global distributed database where routing information is stored . The purpose is to ensure stability and consistency of the Internet-wide routing. One can consult the database to obtain the origin AS of a prefix.

1.3. Internal control ideas

Some research projects have focused on internal control of an AS. [RCC] is a configuration analysis tool. Network operators can use it to verify whether network configurations satisfy a prior anticipation.

[RCP] offers a proposal which introduces a routing control plane and mainly focuses on internal problems within an AS, such as protocol oscillation, forwarding loops, blackholes and so on.

1.4. Proposed solution

This draft proposes a solution to alleviate the problem. Since the root cause of the problem is mistake on advertisements, it is necessary to check the outbound advertisements besides of validating received UPDATE. This draft proposes methods to make sure that origin of routes is consistent with the anticipated configuration.

This solution is not brand-new, but it is low cost and incrementally deployable. The solution can be applied alone or be part of a future total solution about BGP security. When an AS has too limited resource to support an expensive security mechanism, this proposal may also be beneficial.

2. Threat Model

Basically, the threat will occur in following two situations.

1 In a deliberate attack situation

An attacker may intercept BGP protocol traffic and modify the information of the traffic. Authentication mechanism can counter the

attack of this type, and [IPsec], [TLS] or [TCPMD5] can be applied to provide such authentication.

An attacker may also compromise a BGP border router and advertises vicious prefixes through it.

2 In a misconfiguration situation

BGP provides no inherent measure to control or monitor route advertisements. Misconfigurations will not be checked or trigger any alarm either. With the size of the AS growing, manual configuration may increase the probability of configuration error. In many known problems, the wrong prefixes have been advertised were mainly caused by misconfiguration. Deliberate attacks are similar to misconfiguration and attacks were reported relatively rarely.

A number of reasons (for example, the complexity of network and its configuration, manual configuration and absence of unified bound to apply AS-level strategy) leads to the fact that the actual network operation is not consistent with the anticipation.

3. Solution

The proposal suggests mechanisms to avoid advertising a wrong message from the inside of an AS and to avoid the mistake in the first place.

The main obstacles [IRR] faces are how to keep the database up-to-date and complete, which limit its use. Conversely, for an AS the range of prefixes that originate from it is a prior knowledge. Therefore, it is possible to validate and restrict the advertisement behavior of the AS. Technically, attacks caused by compromised device are similar to those by misconfiguration, so the solution is also effective to mitigate such attacks.

This solution can be incrementally deployed. Prefixes originating from AS are filtered inside of the AS and EBGP sessions between ASes will not be affected. Besides, received advertisements are also filtered on the basis of a legitimacy level associated with an AS. It is considered as its legitimacy to originate prefixes. This level is inferred from IRR and received advertisements.

This solution is compatible with [SBGP] and [SoBGP]. Introduced infrastructure in these proposals, such as PKI, can be used to provide trust, when restricting advertised prefixes.

3.1. Framework

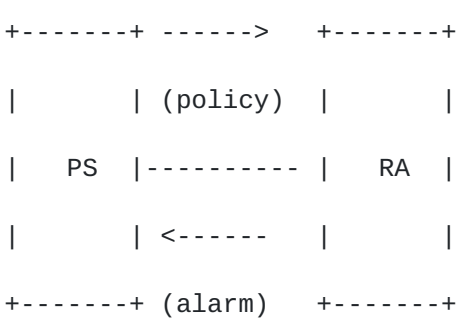

Figure 1: System Architecture

Figure 1 is the framework of the system. RA is a border router in a single AS and PS is a policy station in that AS.

One task of PS is to maintain a uniform advertising policy and to deploy the policy inside the whole AS. Another task is to collect alarms of inconsistent behavior from border routers inside the AS.

As a border router, such as RA in figure 1, before prefixes being advertised out of the AS, they should check them against the policy to determine whether the prefixes are consistent with the policy.

3.2. Operation

3.2.1. Policy maintaining

A policy station in an AS is responsible for maintaining a prefixes advertisement policy. A policy station could be a dedicated host or a router who has implemented additional functions of policy maintaining.

Conceptually a policy defines the range of prefixes which originate from the AS. The policy may be established by manual configuration or introduced into an AS through some external mechanism. For example, for the address PKI proposed by [SBGP], the policy may be introduced by utilizing Address Attestation (AA). In any case, the most important thing is to ensure the accuracy of the range of prefixes, i.e. to ensure the advertised prefixes originating from some AS is properly authorized.

3.2.2. Policy deployment

There are two types of deployment model according to participation of a router.

o Distributed deployment model

In this scenario, the advertisement policy should be deployed in every BGP speaker in an AS. A policy station could use a BGP-based mechanism to distribute the policy, such as a new type of BGP message or some technology similar to [ORF]. The policy could also be distributed in an "out-of-band" channel.

In this model, border routers are responsible for the policy execution. The policy may be implemented with some filtering mechanisms. Before distributing static or IGP routes into RIB of BGP, the routes should be checked.

Since the policy is deployed inside an AS, transport security of the policy may not be a serious problem. It is important to keep policy deployment reliable and on time.

o Centralized deployment model

In this model, border routers need not execute security policies. A policy station can make use of IBGP, as mentioned in [RCP], to obtain advertised routes and check them against the deployed policy. In this way, the policy station is able to determine whether a route is consistent with the policy. If not, it triggers an alarm to a management system.

Because a policy check occurs at a single host, a policy station is supposed to keep online and analyze the alteration of routes in time.

3.2.3. Violation Response

When local routes violate the deployed policy, there are two kind of possible measures to be taken:

o A loose measure

If a router uses a loose measure, violating routes will still be advertised. However, an event should be reported to a management system immediately, so an administrator could perform a proper counter measure in time.

o A strict measure

If a router uses a strict measure, violating routes will be filtered and will not be spread out of the AS. This is an active measure and can prevent false route from being advertised, which may be caused by misconfiguration.

If this security measure is implemented as a mandatory option, attacks made by a compromised router may also be detected.

4. Future Work

This application framework is more fit for BGP stub ASes which do not provide transitive services and for the ASes whose devices are with limited resource.

As to upper ASes, frequent changes of internet route must be considered. In such situation, a policy station is supposed to know these changes, so it should be [s|so|ps]BGP-aware and could get credible routing and authorization information from outside security systems.

Furthermore, the policy station could be enhanced to process more complicated semantic validation, such as AS_PATH validation.

To sum up, in this framework only a few devices in an AS are required to participate in security validation. In this way most BGP router could meet security requirements without update hardware.

5. Security Considerations

This draft focuses on preventing sending and receiving BGP false advertisements incurred by misconfiguration. Since attack may also be a potential cause of the problem, the proposal is a security mechanism for BGP in the same time.

A policy station is the key element of the solution. Since it is located in the domain of an AS, launching an attack toward it may be difficult. If strict security requirements are needed, operators may take more strict access control to the policy station.

6. Acknowledgements

7. References

7.1. Normative References

[RFC1208] Jacobsen, O. and D. Lynch, "Glossary of networking terms", RFC 1208, March 1991.

[RFC1812] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

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

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

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

[IPsec] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[TLS] T. Dierks, C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[TCPMD5] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

7.2. Informative References

[VULN] S. Murphy, "BGP Security Vulnerabilities Analysis", RFC 4272, January 2006.

[SBGP] Charles Lynn, Joanne Mikkelson, Karen Seo, "Secure BGP (S-BGP)", draft-clynn-s-bgp-protocol-01.txt, June 2003.

[SoBGP] R. White, "Architecture and Deployment Considerations for Secure Origin BGP (soBGP)", draft-white-sobgp-architecture-01.txt, May 24, 2005.

[IRR] "Internet Routing Registry", http://www.irr.net.

[RCC] MIT, "Routing Configuration Checker", http://nms.lcs.mit.edu/bgp/rcc/#status.

[RCP] Matthew Caesar, Donald Caldwell, Nick Feamster, Jennifer Rexford, Aman Shaikh, Jacobus van der Merwe, "Design and Implementation of a Routing Control Platform".

[ORF] Enke Chen, Yakov Rekhter, "Cooperative Route Filtering Capability for BGP-4", draft-ietf-idr-route-filter-13.txt.

Author's Addresses

Dai Guangming
Huawei Technologies
No.3, Xinxi Road, Shangdi Information Industry Base
Haidian District, Beijing City 100085
Email: daigm@huawei.com

Zhao Ye
Huawei Technologies
No.3, Xinxi Road, Shangdi Information Industry Base
Haidian District, Beijing City 100085
Email: yezhao@huawei.com

Intellectual Property Statement

Disclaimer of Validity

INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

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