SIDROPS
Internet-Draft
Intended status: Informational
Expires: 20 November 2025

S. Jiang
Zhongguancun Laboratory
K. Xu
Q. Li
Tsinghua University
X. Shi
Tsinghua University & Zhongguancun Laboratory
Z. Liu
Tsinghua University

19 May 2025

Route Origin Registry Problem Statement
draft-jiang-sidrops-psvro-02

Abstract

Prefix hijacking, i.e., unauthorized announcement of a prefix, has emerged as a major security threat in the Border Gateway Protocol (BGP), garnering widespread attention. To migrate such attacks while supporting legitimate Multiple Origin ASes (MOAS), higher requirements are placed on the route origin registry. This document serves to outline the problem statement for current route origin registry.

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 https://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 20 November 2025.

Copyright Notice

Table of Contents

1. Introduction

The Border Gateway Protocol (BGP) is ubiquitously used for inter-domain routing. However, it lacks built-in security validation on whether its UPDATE information is legitimate [RFC4272]. This poses concerns regarding prefix hijacking, where unauthorized announcements of prefixes can occur, simulating legitimate Multiple Origin ASes (MOAS).

Unfortunately, the current route origin registry, such as Internet Routing Registry (IRR) [RFC1786] and Resource Public Key Infrastructure (RPKI) [RFC6480], are not effective in distinguishing between legitimate MOAS and prefix hijacking. There is a pressing need for an verifiable route origin registry that can support registration and protection of legitimate MOAS, thereby mitigating the threats posed by prefix hijacking to the routing system.

This document will primarily analyze the various scenarios of MOAS and highlight the limitations of the current route origin registry. By examining these issues, our primary objective is to offer valuable insights to network operators, researchers, and policymakers for improving the security and robustness of the global routing system.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Working Definition of Route Origin Registry

Route origin registry refers to a system that records the mapping of IP prefixes to the ASes authorised to announce them. Resource holders can register route origin mapping relationships in route origin registry by themselves or delegate to others.

IRR and RPKI currently offer functionalities related to route origin registry. IRRs, which have been in operation since 1995, serve as a globally distributed database for routing information. They record the binding relationship between IPs and Autonomous Systems (ASes) via Route(6) objects, which are defined by the Routing Policy Specification Language (RPSL).

On the other hand, the RPKI, which was developed starting in 2008, provides a formally verifiable framework. The RPKI is based on resource certificates that extend the X.509 standard. It records the mapping between IP prefixes and their authorised ASes via Route Origin Authorization (ROA) objects. These ROA objects contain essential information such as the prefix, origin ASN, and MaxLength.

4. Prefix Hijacking and Legitimate MOAS

[RFC1930] suggests that a prefix should typically have a single Autonomous System (AS) as its origin, with a few exceptions. However, CAIDA's analysis on BGP routing data [CAIDA] reveals that MOAS has always been a common phenomenon. There are various reasons that contribute to the emergence of MOAS prefixes:

* *_Aggregation_*. According to [RFC1930], aggregation could result in prefix originated from multiple possible ASes. For example, if the "Prefix 0/24" originates from ASx and the "Prefix 1/24" originates from ASy, aggregating them into "Prefix 0/23" with the originates from [ASx, ASy] may result in the loss of the specific origin AS information if the ATOMIC_AGGREGATE attributes of the aggregation announcements are not specific.

* *_Business consideration_*. Companies often choose providers that offer high-speed and reliable data services to host their servers. For efficient resource allocation, a parent organization that owns a large chunk of IP addresses may divide its address space among one or more child organizations, which choose different providers and ask them to announce the same prefix. For example, a multi-national company may advertise its prefix from multiple locations where it has offices.

* *_Multi-homing_*. When multi-homing occur without the use of BGP, it can result in MOAS conflicts. Assuming ASx is connected to two providers, ISP1 and ISP2. ISP1 is connected to ASx using BGP, while ISP2 is connected to ASx through static routes or Interior Gateway Protocol (IGP). Both ISP1 and ISP2 advertise prefixes that belong to ASx.

* *_Internet eXchanges_*. When a prefix is associated with an exchange point, it becomes directly accessible from all the ASes connected to that exchange point. Each AS at the exchange point has the capability to advertise the prefix as if it originates directly from their own AS.

* *_Anycast_*. Anycast is often employed by content distribution networks (CDNs) to direct the requests of their customers to the nearest servers, ensuring speedy data delivery to their customers.

* *_Prefix hijacking and misconfigurations_*. A malicious AS may advertise prefixes belonging to another organization to attract its traffic. An AS may also make such annoucements unintentionally due to misconfiguration.

Distinguishing between prefix hijacking, misconfiguration, and legitimate MOAS is a complex task. The challenge arises from the resemblance of these behaviors, as they often display similar characteristics. Moreover, accurately identifying and classifying these situations necessitates a route origin registry with high coverage and accuracy.

5. Problems in Current Route Origin Registry

This section outlines several challenges faced by the current route origin registries in distinguishing legitimate MOAS events from malicious MOAS incidents, such as route hijacking.

5.1. Security Risks from Partial Adoption

As the adoption of RPKI continues to grow, the number of address prefixes registered within RPKI is gradually increasing. However, recent reports from the Number Resource Organization (NRO) [NRO] indicate that the coverage of IP prefixes within ROAs is still relatively low, and the adoption rate of route origin validation (ROV), as measured by Mutually Agreed Norms for Routing Security (MANRS) [MANRS], is even significantly lower than the coverage of ROAs. Similarly, [IRRegularities] also notes a decreasing trend in IP Prefix coverage in certain IRRs. When focusing on MOAS, their coverage is significantly lower and insufficient to distinguish between legitimate MOAS and route hijacking.

Limited IP prefix coverage within the current route origin registry, especially for MOAS prefixes, hinders the complete validation of route announcements, significantly limiting the motivation for network operators to utilize route origin registry.

5.2. Inconsistency between Different Route Origin Registries

Based on the analysis presented in the previous sections, it is evident that relying solely on a single source of route origin registry is insufficient in route origin validation. To address this issue effectively, it is recommended to integrate the RPKI and multiple active IRRs.

However, it is important to note that this fusion approach may encounter several limitations. As highlighted in [IRRegularities], inconsistencies exist among the Route(6) objects across different IRRs. This inconsistency can be attributed to the chronic neglect by IRR customers. For instance, some companies may register Route(6) objects in some IRRs but fail to update them in all the route origin registries, resulting in outdated and stale Route(6) objects. Furthermore, it is observed that a higher number of IRRs exhibit

lower consistency with RPKI. In practice, different networks often use different data and methodologies to perform route validation and filtering, resulting in disparate outcome, especially when ROA and IRR data conflict with each other.

As a result, while integrating the RPKI and multiple active IRRs can improve the effectiveness of route origin validation, it is essential to address the issues of inconsistencies between different route origin registries.

5.3. Insufficiency of Resource Certification

As mentioned in [RFC7682], the lack of certification and incentives for maintaining up-to-date data within IRRs leads to low accuracy of the information. Recent measurement [IRRegularities] reveals that IRRs with low update activity exhibit lower overlap with BGP announcements than those with high update activity. This indicates that IRRs with lower activity may contain a higher proportion of outdated and stale Route(6) objects, thereby impacting the reliability of the route origin registry.

RPKI is a hierarchical Public Key Infrastructure (PKI) that binds Internet Number Resources (INRs) such as Autonomous System Numbers (ASNs) and IP addresses to public keys via certificates. However, there is a risk of conflicts in INRs ownership when misconfiguration or malicious operations occur at the upper tier, resulting in multiple lower tiers being allocated the same INRs. Additionally, the existence of legitimate MOAS necessitates the authorization of binding between a prefix with multiple ASes, further complicating the issue. Balancing the protection of legitimate MOAS while minimizing risks in INRs certificates presents a challenging problem that requires innovative solutions. Furthermore, it is worth noting that RPKI Relying Parties (RPs) [RFC8897] have not yet standardized the process of constructing certificate chains and handling exceptions such as Certificate Revocation Lists (CRLs) and Manifests. This lack of standardization has resulted in different views on the RPKI records by RPs who adopt different implementations. Consequently, ASes served by different RPs may have varying validation results for the same route announcement.

Consequently, the absence of data validation and standardization in operations within the IRR or RPKI framework means that there is no guarantee of the accuracy of the data registered in any route origin registry.

5.4. Synchronization and Management

The current practice in IRRs involves the use of the Near-Real-Time Mirroring (NRTM) protocol [NRTMv4] to replicate and synchronize Route(6) object from other IRRs. Similarly, the RPKI relies on the RPKI Repository Delta Protocol (RRDP) [RFC8182] to synchronize and update data. However, these network protocols exhibit several weaknesses that need to be addressed.

* The absence of a mechanism to notify other mirrors when updates occur results in synchronization delays and data inconsistency issues. This can be problematic when timeliness and accuracy are crucial.

* The absence of validation for replicated data from mirrored sources in both IRRs and RPKI is a legitimate concern. This situation creates a considerable risk for inconsistencies and conflicts with the current data.

* The absence of application security mechanisms within these protocols is another area of vulnerability. This lack of security measures exposes the system to unauthorized access and compromise on data integrity.

Although some approaches attempt to optimise the quality of the route origin registry, e.g. RIPE NCC, IRRdv4 using RPKI to validate/filter IRR Route(6) objects, and [RFC8416] proposing that RPs can customise route origin with local data, the problem of inconsistency persists due to the limited coverage of RPKI and the lack of effective mechanisms to resolve conflicting data between IRRs. It is crucial to establish a effective communication mechanism among multiple route origin registry, enabling negotiation and cross-validation of conflicting or special-purpose route origin information.

5.5. Summary

The current route origin registry systems, namely IRRs and RPKI, are facing challenges as the increased occurrence of MOAS prefixes. These challenges mainly include low adoption rates, global inconsistency, insufficient resource certification, and incomplete multi-source collaboration mechanisms.

6. Requirements for New Route Origin Registry Mechanisms

This section lists the requirements designed to guide the improvement of route origin registry mechanisms. These enhancements should prioritize multi-party collaboration to safeguard legitimate MOAS events while effectively filtering out malicious MOAS incidents.

6.1. Allowlist Mechanism

To ensure robust protection for legitimate MOAS events, prefix users should implement an allowlist mechanism as a complementary to the current resource-owner-centric systems. This mechanism permits multiple users to be authorized to announce the same prefix concurrently. Moreover, users should be able to dynamically join or leave the allowlist based on practical business consideration.

6.2. Blocklist Mechanism

One of the primary objectives of route origin validation is to suppress the propagation of malicious MOAS incidents and mitigate their impact. To enhance the efficiency and precision of anomaly detection, network participants should employ real-time anomaly monitoring and rapid consensus mechanisms to construct a blocklist. This blocklist enables the timely de-prioritization of anomalous routes, thereby reducing their disruptive effects on the routing system.

6.3. Multi-party Governance

Multi-party governance plays a pivotal role in the development of new route origin mechanisms. By integrating and cross-verifying data from multiple sources, this approach facilitates effective negotiation and resolution of data duplication and conflicts. It ensures the full utilization of the strengths of each data source, thereby enhancing the reliability and functionality of the system.

7. Security Considerations

There is no security consideration in this draft.

8. IANA Considerations

There is no IANA consideration in this draft.

9. References

9.1. Normative References

[RFC1786] Bates, T., Gerich, E., Joncheray, L., Jouanigot, J., Karrenberg, D., Terpstra, M., and J. Yu, "Representation of IP Routing Policies in a Routing Registry (ripe-81++)", RFC 1786, DOI 10.17487/RFC1786, March 1995, <https://www.rfc-editor.org/rfc/rfc1786>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/rfc/rfc6480>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8182] Bruijnzeels, T., Muravskiy, O., Weber, B., and R. Austein, "The RPKI Repository Delta Protocol (RRDP)", RFC 8182, DOI 10.17487/RFC8182, July 2017, <https://www.rfc-editor.org/rfc/rfc8182>.

[RFC8416] Ma, D., Mandelberg, D., and T. Bruijnzeels, "Simplified Local Internet Number Resource Management with the RPKI (SLURM)", RFC 8416, DOI 10.17487/RFC8416, August 2018, <https://www.rfc-editor.org/rfc/rfc8416>.

9.2. Informative References

[CAIDA] "RouteViews Prefix to AS mappings", 2024, <https://catalog.caida.org/dataset/routeviews_prefix2as>.

[IRRegularities] Du, B., Izhikevich, K., Rao, S., Akiwate, G., Testart, C., AC Snoeren, and K. Claffy, "IRRegularities in the internet routing registry", Proceedings of the 2023 ACM on internet measurement conference , 2023.

[MANRS] "MANRS Observatory", 2024, <https://observatory.manrs.org/>.

[NRO] "RIR Statistics", 2024, <https://www.nro.net/about/rirs/statistics/>.

[NRTMv4] Romijn, S., Snijders, J., Shryane, E., and S. Konstantaras, "Near Real Time Mirroring (NRTM) version 4", Work in Progress, Internet-Draft, draft-ietf-grow-nrtm-v4-07, 14 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-nrtm-v4-07>.

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, DOI 10.17487/RFC1930, March 1996, <https://www.rfc-editor.org/rfc/rfc1930>.

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <https://www.rfc-editor.org/rfc/rfc4272>.

[RFC7682] McPherson, D., Amante, S., Osterweil, E., Blunk, L., and D. Mitchell, "Considerations for Internet Routing Registries (IRRs) and Routing Policy Configuration", RFC 7682, DOI 10.17487/RFC7682, December 2015, <https://www.rfc-editor.org/rfc/rfc7682>.

[RFC8897] Ma, D. and S. Kent, "Requirements for Resource Public Key Infrastructure (RPKI) Relying Parties", RFC 8897, DOI 10.17487/RFC8897, September 2020, <https://www.rfc-editor.org/rfc/rfc8897>.

Acknowledgments

The authors would like to thank Yangfei Guo, Di Ma, Qi Li, Shuhe Wang, Xiaoliang Wang, Hui Wang, etc. for their valuable comments on this document.

Authors' Addresses

Shenglin Jiang
Zhongguancun Laboratory
Beijing
China
Email: jiangshl@zgclab.edu.cn

Ke Xu
Tsinghua University
Beijing
China
Email: xuke@tsinghua.edu.cn

Qi Li
Tsinghua University
Beijing
China
Email: qli01@tsinghua.edu.cn

Xingang Shi
Tsinghua University & Zhongguancun Laboratory
Beijing
China
Email: shixg@cernet.edu.cn

Zhuotao Liu
Tsinghua University
Beijing
China
Email: zhuotaoliu@tsinghua.edu.cn