From Policy to Practice: A Research Agenda for Measurement-based BGP Risk Assessment

Savvas Kastanakis
University of Twente
s.kastanakis@utwente.nl

Cristian Hesselman
SIDN Labs and University of Twente
cristian.hesselman@sidn.nl

ABSTRACT

In this work, we outline a research agenda to develop and evaluate tools that help network operators take a risk-based approach to routing security, as suggested by recent policy recommendations by the US government. Our research efforts set the stage for a systematic risk assessment model that enhances BGP security across diverse network settings.

1 BACKGROUND

The Border Gateway Protocol (BGP) [3] is the foundation of the global Internet, enabling its 75,000 different Autonomous Systems (ASes) to route data from source to destination through multiple intermediate ASes. As a result, the security of BGP's routing announcements is paramount for the integrity and the resilience of the communication service that the Internet provides.

Despite its criticality, BGP remains susceptible to several major and widely exploited vulnerabilities [1]. Some of the most common attacks include *prefix hijacks*, where a malicious AS falsely claims ownership of an IP prefix assigned to another AS and *route leaks*, where an AS improperly advertises a learned route, leading to traffic misrouting. These attacks can have serious consequences, including service outages, data interception, and service impersonation.

In response to these risks, the White House Office of the National Cyber Director (ONCD) released recommendations in September 2024 aimed at enhancing the security and resilience of Internet routing [2]. The ONCD's policy underscores a *risk-based approach* to improve routing security, urging network operators to implement risk management strategies and BGP route validation measures, as well as promote best practices in routing security.

However, we hypothesize that operationalizing such a risk-based approach is a major challenge because it requires (1) additional BGP measurement and analysis methods to assess, prioritize, and secure the routing assets of network operators, and (2) practical and easy to use tools for operators to deploy these methods. For example, developing methods to identify critical prefixes is essential to prioritize security measures for high-risk routes, alongside impact estimation tools to quantify the effects of prefix hijacks and route leaks. However, distinguishing critical prefixes requires continuous, data-driven analysis of complex network dependencies, while robust impact estimation demands rich topological and incident impact-data which is often sparse and challenging to obtain.

2 RESEARCH AGENDA

To address this challenge, we propose a 6-point research agenda, which we outline below. We envision that it will result in what we call the *BGP Risk Assessment Toolbox (BRAT)*, which consists of a collection of tools based on new and existing BGP measurement and analysis methods. The 6-point research agenda is as follows:

1. Critical Asset Identification: Enables operators to identify and categorize their critical BGP prefixes and paths, which are essential to network operations. While operators may have a general understanding of critical prefixes and paths, these can be overlooked or misunderstood in complex network environments. Unlike traditional methods that rely on intuition or static configurations. *BRAT* enhances this process with a systematic, data-driven approach using passive and active BGP measurements to critical domains.

2. Vulnerability Assessment: Enables operators to identify potential BGP attack vectors targeting their critical network assets. To assess vulnerabilities, operators may passively monitor BGP update feeds to detect historical weaknesses and misconfigurations, or actively conduct controlled penetration tests on actual BGP paths.

3. Impact Quantification: Enables operators to understand the potential consequences of BGP attacks on their networks. By modeling the operational, financial, and reputational impacts of outages or routing integrity breaches, operators can prioritize their resilience efforts towards critical paths and prefixes.

4. Path Prioritization: Not all AS paths are equal in terms of risk exposure or criticality. Developing criteria and tools for prioritizing paths based on their importance and threat level allows network operators to strengthen the most vulnerable segments of their routing infrastructure. Operators may prioritize paths by passively observing route stability metrics to detect frequently disrupted paths or actively conducting Route Origin Validation (ROV) checks to focus resources on paths with insufficient protection.

5. Dynamic Risk Assessment: By implementing continuous monitoring systems, network operators can respond to emerging BGP threats, maintaining network integrity even as new challenges arise. Continuous BGP monitoring allows for swift detection of real-time routing anomalies, while probing on critical paths offers an active approach to validate route integrity and detect emerging risks.

6. Implementation Feasibility: Finally, practical deployment of the *BRAT* across different network types and scales requires conducting feasibility studies and pilots in varied network environments. To that end, we plan to make our code and data publicly available to support further research.

ACKNOWLEDGEMENTS

This research received funding from the Dutch Research Council (NWO) under the projects UPIN and CATRIN.

REFERENCES

[1] Sandra Murphy. 2006. RFC 4272: BGP Security Vulnerabilities Analysis. (2006).
[2] White House Office of the National Cyber Director (ONCD). 2024. Roadmap to Enhancing Internet Routing Security. (2024).
[3] Yakov Rekhter, Tony Li, and Susan Hares. 2006. RFC 4271: A Border Gateway Protocol 4 (BGP-4). (2006).