

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

Savvas Kastanakis¹ and Cristian Hesselman^{1, 2}

¹ UNIVERSITY
OF TWENTE.

²  SDN LABS

Motivation

The **Border Gateway Protocol (BGP)** is the glue that holds the Internet together by enabling 75.000 networks to route data from a source to a destination.

Despite its criticality, **BGP is vulnerable** to several major and widely exploited vulnerabilities, i.e., *prefix hijacks* and *route leaks*.

The White House published a **list of recommendations** aimed to enhance the global Internet Routing Security.

To operationalize these recommendations, we propose a 6-point research agenda:

Research Agenda

Critical Asset Identification:

How can organizations systematically identify and categorize critical prefixes and critical paths within their networks?

Vulnerability Assessment:

How can organizations assess the potential attack vectors that could target their critical assets?

Impact Quantification:

How can the impact of be quantified in terms of operational disruption, financial loss, and reputational damage?

Path Prioritization:

What criteria should be used to prioritize AS paths?

Dynamic Risk Assessment:

How can the toolbox be adapted to incorporate real-time risk assessment capabilities?

Implementation Feasibility:

What are the practical challenges in deploying the proposed BRAT across diverse network types and scales?

We'd Love Your Feedback! Scan Here to Share Your Thoughts!

CSNG'24, November 22, 2024, Utrecht, Netherlands

Contact us at: s.kastanakis@utwente.nl, cristian.hesselman@sidn.nl



SCAN ME