A Survey of ROV++: We May Need Another Napkin

Neal Ziring, affiliated with NSA
Berk Gulmezoglu (Faculty), Nathan Ferrell, Bryan Chan, Arrianna Szymczak, Henry Schmidt

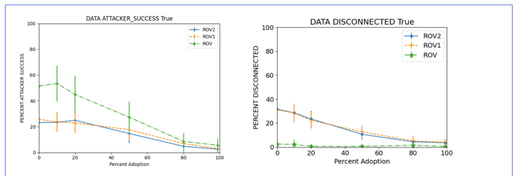
This work was supported by grant H98230-21-1-0317.

Project Statement

- ***Motivation:*** BGP is vital for internet operations but is vulnerable to path manipulation and hijacking attacks. Despite current security measures, BGP needs more robust protections, even in the hypothetical era where Route Origin Validation is fully adopted (Post-ROV era).
- ***Current State:*** RPKI with ROV is partially adopted but lacks protection against various attack types, leading to vulnerabilities.
- ***Goal:*** This project explores the effectiveness of BGP-iSec and ROV++ as potential security enhancements to BGP and assesses its real-world feasibility.
- ***Impact:*** Implementing ROV++ could offer improved security for BGP, though adoption incentives and operational overhead remain significant challenges.

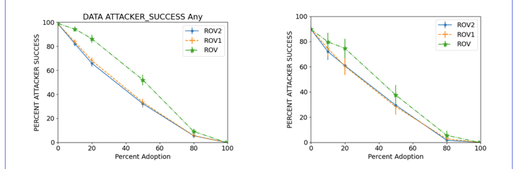
Methodology

- ***Simulation Tool:*** BGPy using the 2020 CAIDA serial-2 AS dataset.
- ***Protocols Evaluated:*** BGP-iSEC, ROV++, ROV++ V1 Lite, ROV++ V2 Lite, and standard ROV.
- ***Simulation Types:*** Baseline (no security), real-world (50% ROV adoption), tier 1 (clique ASes with ROV), custom metrics for edge ASes.
- ***Attack Types Simulated:*** Sub-Prefix Hijacking, Super-prefix Prefix hijacking, Non-Routed Super-Prefix Prefix Hijacking, and Non-Routed Prefix Hijacking.
- ***Metrics Recorded:*** Attacker success rate, victim success rate, disconnection rate for 250 trials per attack type (6000 total trials).



(a) Attacker Success rates on adopted ASes (b) Disconnect rates on adopted ASes

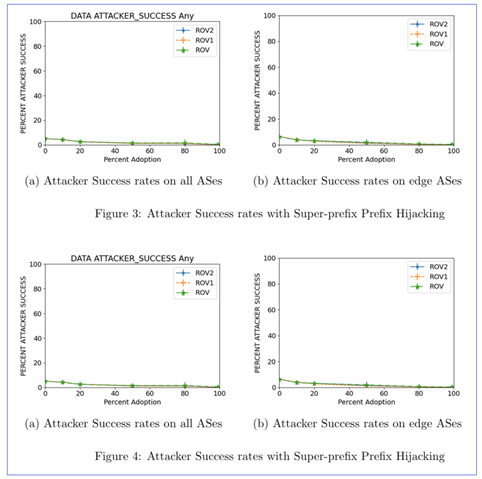
Figure 1: Attacker Success and Disconnect Rates for Sub-Prefix Hijacking (adopted ASes only)



(a) Attacker Success rates (Baseline Simulation) (b) Attacker Success rates (Tier 1 Simulation)

Figure 2: Attacker Success and Disconnect Rates for Sub-Prefix Hijacking (all ASes)

Low adoption rates of ROV++ have higher disconnection rates as well as lower attacker success rates due to the blackholing that the policy utilizes.



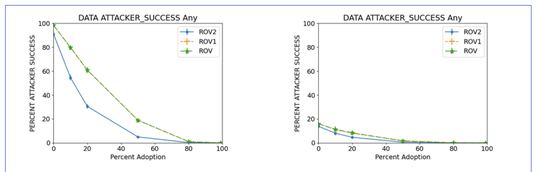
(a) Attacker Success rates on all ASes (b) Attacker Success rates on edge ASes

Figure 3: Attacker Success rates with Super-prefix Prefix Hijacking

(a) Attacker Success rates on all ASes (b) Attacker Success rates on edge ASes

Figure 4: Attacker Success rates with Super-prefix Prefix Hijacking

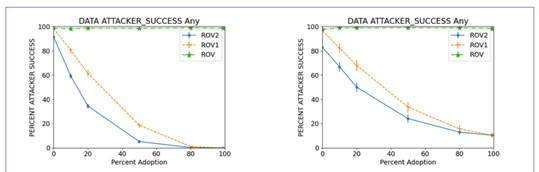
Attacks such as Super-prefix Prefix hijacking are completely mitigated in real world scenarios.



(a) Attacker Success rates (Baseline Simulation) (b) Attacker Success rates (Real-World Simulation)

Figure 5: Attacker Success rates with Non-Routed Prefix Hijacking

Non-Routed Prefix Hijacks were deployed to test the attacker success rates of ROV, ROV++ V1 Lite and ROV++ V2 Lite.



(a) Attacker Success rates (Baseline Simulation) (b) Attacker Success rates (Real-World Simulation)

Figure 6: Attacker Success rates with Non-Routed Super-Prefix Prefix Hijacking

This attack is especially effective against base ROV, but ROV++ V1 Lite and ROV++ V2 Lite produced the same results as the non-routing prefix hijack.

Conclusion

- ***BGP-iSec:***

  Through discussion with the creators of BGP-iSEC and BGPy the following was determined:

  - This protocol will never work in the real world
  - This protocol cannot be properly simulated at this time.
- ***ROV++:***

We simulated this protocol properly and it provided some conflicting conclusions:

- ***Sub-prefix Hijacks:***
  - Early adopters would experience minimal benefit from using ROV++
  - Rate of attacker success does not decrease fast enough to make this financially viable to adopters at any adoption rate.
- ***Super-prefix Prefix Hijacks:***
  - Completely mitigated by ROV++ in present day, real-world simulations due to its blackholing announcements.
  - The mitigation occurs regardless of adoption percentage
- ***Non-Routed Prefix Hijacks:***
  - Almost completely mitigated by blackholing announcements.
  - In this case complete mitigation requires majority adoption.
- ***Non-Routed Super-Prefix Prefix Hijacks:***
  - This attack shows the most significant decrease in success rate between ROV++ and ROV.
  - It is important to consider the possibility of misconfigured blackholing announcements.

References

[1] CameronMorris. "BGP-iSec: Improved Security of Internet Routing Against Post-ROV Attacks". In: (2024). doi: https://dx.doi.org/10.14722/ndss.2024.241035. url: https://www. ndss-symposium.org/ndss-paper/bgp-isec-improved-security-of-internet-routing against-post-rov-attacks/.
[2] Justin Furuness et al. "BGPy: The BGP Python Security Simulator". In: Proceedings of the 16th Cyber Security Experimentation and Test Workshop. CSET '23. Marina del Rey, CA, USA: Association for Computing Machinery, 2023. doi: 10.1145/3607505.3607509. url: https: //doi.org/10.1145/3607505.3607509.
[3] Reynaldo Morillo et al. "ROV++: Improved Deployable Defense against BGP Hijacking". In: Proceedings 2021 Network and Distributed System Security Symposium (2021). url: https: //api.semanticscholar.org/CorpusID:231879110.