April 11, 2022

Via ECFS
Before the Federal Communications Commission
Washington, D.C. 20554

In the Matter of Secure Internet Routing, P.S. Docket No. 22-90

Thank you for the opportunity to respond to the Federal Communication Commission's inquiry into internet routing vulnerabilities. We are academic researchers associated with the Center for Information Technology Policy (CITP) at Princeton University,[1] and the University of Chicago, who have extensive expertise in information security, networking, and internet policy. We write to offer our perspective on how the Commission might strengthen the security and integrity of the Border Gateway Protocol (BGP) and other critical points in the internet routing infrastructure.

At the outset we commend the Commission for focusing on the critical nature of the security vulnerabilities in the routing infrastructure and why we must address them. Our research detects and proposes solutions to such vulnerabilities, and we are grateful to not have to repeat the parade of horribles that justify why this issue has significant national security and economic implications.[2]

[1] In keeping with Princeton's tradition of service, CITP's Technology Policy Clinic provides nonpartisan research, analysis, and commentary to policy makers, industry participants, journalists, and the public. This response is a product of that Clinic and reflects the independent views of the undersigned scholars.
[2] *See* Sun et al., *Securing Internet Applications From Routing Attacks*, Communications of the ACM, June 2021, Vol. 64 No. 6, Pages 86-96, available at

Our comment focuses on the challenges of securing the routing infrastructure and proposes steps the government can take to advance our security interests.

1. The strength of BGP security measures depend on whether they are widely adopted. The FCC needs to develop a package of incentives and mandates to motivate participation across the industry.

The core challenge for securing the internet routing infrastructure is that the original design of the network did not prioritize security against adversarial attacks.[3] Instead, the original design focused on how to route traffic through decentralized networks with the goal of delivering information packets efficiently while not dropping traffic.

At the heart of this routing system is BGP, which allows independently-administered networks (Autonomous Systems or ASes) to announce reachability to IP address blocks (called prefixes) to neighboring networks.[4] But BGP has no built-in mechanism to distinguish legitimate routes from bogus routes. Bogus routing information can redirect internet traffic to a strategic adversary, who can use it to launch a variety of attacks, or it can lead to accidental outages or performance issues. Network operators and researchers have been actively developing measures to counteract this problem.

---

https://cacm.acm.org/magazines/2021/6/252822-securing-internet-applications-from-routing-attacks/fulltext.

[3] *See* Government Accounting Office Report, *Internet Architecture Is Considered Resilient, but Federal Agencies Continue to Address Risks*, March 2022, available at https://www.gao.gov/assets/720/719340.pdf

[4] *See* The Communications Security, Reliability and Interoperability Council III Working Group 6 Final Report, March 2013, available at https://www.cs.princeton.edu/~jrex/papers/CSRIC_III_WG6_Report_March_2013.pdf.

At a high level, the current suite of BGP security measures depend on building systems to validate routes. But for these technologies to work, most participants have to adopt them or the security improvements will not be realized. For example, RPKI relies on networks to produce Resource Origin Authorizations (ROAs) to cryptographically attest to the owner of IP prefixes and implement Route Origin Verification (ROV) to filter BGP announcements based on ROAs. In a low deployment environment, incentives on both sides of this are weak. In the absence of ROV, networks are not incentivized to publish ROAs because they will not lead to significant security improvements. Similarly, networks are not incentivized to implement ROV when the vast majority of the route table is not covered by ROAs because such filtering is unlikely to catch an attack.

We see that a number of larger providers have adopted both the ROA and ROV components of RPKI, but these are mainly modest steps that protect against accidental misconfiguration and only offer incremental benefits against a strategic adversary. This is in large part because RPKI only secures the origin, which leaves open the possibility of an attack that advertises a false route with a correct origin. For a full defense, the entire route must be secured. Moreover, small and medium size ASes have not participated in such systems because the incentives for them to invest in these security measures are unclear.

As we outline below, the Commission, along with other agencies, should develop and promote a strategy to address the internet routing vulnerabilities through technologies at various layers in the network architecture.

2. The Commission needs to develop a cross-layer strategy to build routing security.

There is no single magic bullet to address routing security. Instead, the government needs a cross-layer strategy that embraces pushing different elements of the infrastructure to adopt security measures that protect legitimate traffic flows. The industry's Mutually Agreed Norms for Routing Security (MANRS) initiative goes some distance in promoting voluntary practices, but the MANRS initiative, standing alone, will not deliver the security properties that are needed. We identify some of the key players and provide a non-exhaustive list of what they might do to secure the routes below:

a. Internet Service Providers
    1. Participate in MANRS
    2. Run both ROV and deploy ROAs
    3. Monitor BGP routes to their prefixes
b. Content Delivery Networks and Cloud Providers
    1. Participate in MANRS
    2. Run both ROV and ROA
    3. Participate in BGP monitoring
    4. Use the Domain Name System Security Extensions (DNSSEC), which authenticates responses to domain name lookups[5]
    5. Encourage the use of subresource integrity, which is a security feature that lets browsers cryptographically verify that content they

[5] *See* https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en.

fetch (for example, from a CDN) is delivered without being compromised.[6]

c. Internet Exchange Points
    1. Participate in MANRS
    2. Run ROV on route server
d. Certificate Authorities
    1. Improve domain verification methods with techniques like multi-vantage-point domain validation to prevent the issuance of certificates during BGP attacks.[7] Ensure the prefixes used for their operations are covered by ROAs and their ISP (if they are not an ISP themselves) performs ROV.
    2. BGP monitoring
e. Equipment manufacturers
    1. Work towards BGPSec support
f. DNS providers
    1. Use DNSSEC
    2. Run authoritative nameservers on /24 IPv4 prefixes to reduce vulnerability to "subprefix" BGP attacks
    3. Make sure nameservers are covered by ROAs and providers are performing ROV

[6] *See* https://www.w3.org/TR/SRI/
[7] *See* Birge-Lee et al., *Bamboozling Certificate Authorities with BGP*, Proceedings of the 27th USENIX Security Symposium, Aug. 2018, available at: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-birge-lee.pdf.

4. BGP monitoring

g. Browsers

1. Continue with advancements to DNS security technologies like DoH and DoT
2. Continue to push security warnings on non-HTTPS content to encourage larger HTTPS adoption.
3. Encourage developers to cryptographically verify the content of web resources with subresource integrity.

h. Independent Traffic Observatory

There is an opportunity for the government to fund academic research centers that collect real-time data from a variety of sources that measure traffic and how it is routed across the internet. Such an independent observatory would build on the work of CAIDA[8] and the data collected and analyzed by MANRS Observatory.[9] And it would use data from sources like Google, whose release of coarse, high-level data about internet traffic still gives some valuable insights about potential anomalies.[10] But there are important questions about what are the right number of vantage points to understand how data is being routed and how to make sense of the data using machine-learning techniques. There are also questions about how to get the different players to cooperate and to ensure that the data is

[8] *See* CAIDA's Measurement and Data Infrastructure, Jan. 2022, https://www.caida.orxg/catalog/media/2022_caida_measurement_data_infrastructure_overview/caida_measurement_data_infrastructure_overview.pdf.
[9] https://observatory.manrs.org/#/about
[10] https://transparencyreport.google.com/traffic/overview?hl=en.

used responsibly for its intended purpose of detecting bogus routing patterns.

3. There are significant challenges to adopting the cross-layer strategy that need to be anticipated and addressed proactively.

There are four challenges to the cross-layer strategy we outline:

First, to mandate the cross-layer security measures, the Commission has to have regulatory authority over the relevant players. Section 1 of the Communications Act of 1934 explains that the Congress centralized authority within the Commission "for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communications." Former Chairman Wheeler argues that this grant of authority is sufficient to regulate cybersecurity in the internet routing infrastructure.[11] Other commentators disagree.[12] We do not take a position on this legal issue in this comment, but note that it would be helpful for the Commission to bring clarity to this question.

That said, some of the key players, such as certificate authorities, browser developers, and equipment manufacturers, would likely not fall under the purview of a more expansive view of the FCC's authority. This points to the need for the

[11] *See* Wheeler, Cybersecurity is not something; it is everything, Brookings Blog, Feb. 2018, https://www.brookings.edu/blog/techtank/2018/02/15/cybersecurity-is-not-something-it-is-everything/.
[12] *See* Statement by Commissioner O'Reilly, Feb. 2018, https://www.fcc.gov/news-events/blog/2018/02/21/abusing-section-1.

Commission to promote a whole-of-government approach to secure the routing infrastructure.

Second, large portions of the internet routing infrastructure lie outside the jurisdiction of the United States. As such, there are international coordination issues that the Commission will have to navigate to achieve the security properties needed. That said, if there is a sufficient critical mass of providers who participate in the security measures that could create a tipping point for a larger global adoption.

Third, the package of incentives and mandates that the Commission develops has to account for the risk that there will be recalcitrant small and medium sized firms who might undermine the comprehensive approach that is necessary to truly secure the infrastructure.

Fourth, while it is important to develop authenticated routes for traffic to counteract adversaries, there is an underappreciated risk from a flipped threat model – the risk that an adversary takes control of an authenticated node and uses that privileged position to disrupt routing.[13] There are no easy fixes to this threat – but an awareness of this risk can allow for developing systems to detect such actions, especially in international contexts.

* * *

[13] *See* Cooper et al., On the Risk of Misbehaving RPKI Authorities, HotNets-XII: Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks, Nov. 2013, available at https://www.cs.bu.edu/~goldbe/papers/hotRPKI_full.pdf.

We appreciate the opportunity to provide these comments and welcome the opportunity to discuss any questions.

Respectfully submitted,

Henry Birge-Lee
Research Software Engineer, Computer Science and Electrical Engineering Departments, Princeton University

Nick Feamster
Neubauer Professor of Computer Science, University of Chicago

Mihir Kshirsagar
Technology Policy Clinic Lead, Center for Information Technology Policy, Princeton University

Prateek Mittal
Associate Professor of Electrical and Computer Engineering, Princeton University

Jennifer Rexford
Gordon Y.S. Wu Professor of Engineering, and Chair of Computer Science, Princeton University

Contact: 609-258-5306; mihir@princeton.edu