CableLabs

Driving More Secure Internet Routing

Introducing a "Cybersecurity Framework Profile for Internet Routing"

NCSL Task Force on Artificial Intelligence, Cybersecurity and Privacy Meeting

May 17, 2024

Priya Shrinivasan

Director, Technology Policy

p.shrinivasan@cablelabs.com

Summary

- The cable industry has long recognized the threats to internet routing and consumer routers and has proactively sought to address those threats both internally and through broader industry technical fora.
- CableLabs, its members, and NCTA – the Internet and Television Association developed a Cybersecurity Framework (CSF) Profile for Internet Routing (RSP).
- The RSP, released on January 23, 2024, is a compilation of the cable industry's expertise, aligned with the National Institute for Standards & Technology (NIST) CSF v1.1, that provides a roadmap for any organization to drive more secure internet routing.
- In 2021, CableLabs issued a Best Common Practices document regarding cybersecurity for consumer routers that is widely used and referenced by NIST.

WHO WE ARE

CableLabs is the global broadband industry's leading R&D lab for next-generation network technologies

CABLELABS: OUR TECHNOLOGIES

Advanced Optics & Fiber

AI & Machine Learning

Cloud Native

Convergence

Hybrid Fiber Coax

Immersive Media

Mobile

Security & Privacy

Quantum Networks

Wi-Fi

The Road to the Routing Security Profile

Background – Increased Governmental Interest and Focus

- US Federal Communications Commission (FCC) Secure Internet Routing NOI (Feb 2022) and FCC Public Border Gateway Protocol (BGP) Security Workshop (July 31, 2023)

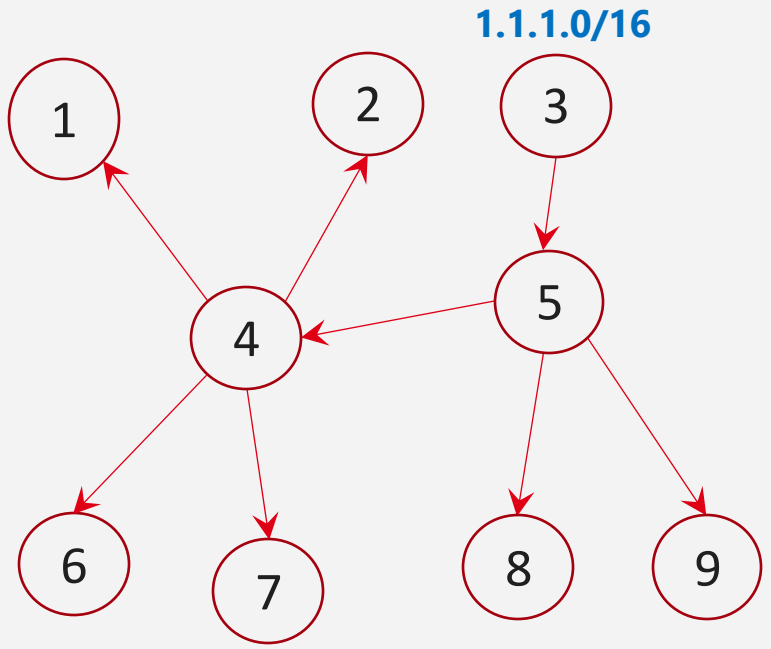
- US National Cybersecurity Strategy (March 2023): *"We must take steps to mitigate the most urgent of these pervasive concerns such as Border Gateway Protocol vulnerabilities…"* and National Cybersecurity Strategy Implementation Plan (July 2023/May 2024 (v2))

- US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): *call to action to submit examples of "profiles" mapped to the CSF aimed at addressing cybersecurity risks associated with a particular business activity of operation*

Background on Cybersecurity, Internet Routing & Associated Threats

What is Internet Routing?

- The Internet consists of many independent and separate networks, namely "Autonomous Systems" (ASes).
- Each AS is assigned an AS Number (ASN).
- The Border Gateway Protocol (BGP) enables routing between and across ASes.
- BGP was first developed in 1989 and continues to be the foundation of the Internet today.



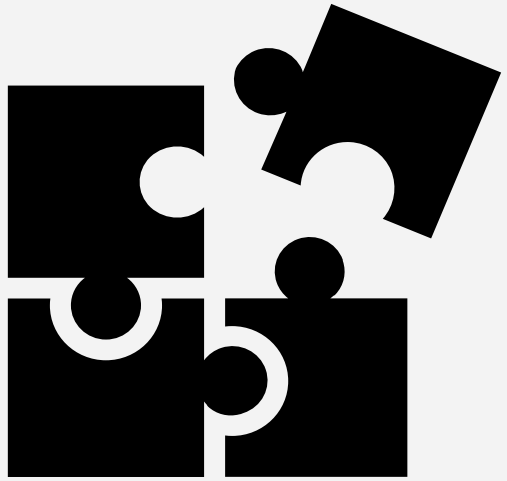
Classic Internet Routing Security Threats

Threat	Description	Potential Consequence
Prefix Hijacking	One AS announces ownership of an IP prefix owned by another AS	• Removes the victim AS from a portion of the Internet, making that AS unreachable • Enables man-in-the-middle attacks
AS Path Manipulation	One AS manipulates an AS_PATH to change the route	Enables prefix hijacking, even though the prefix has a Route Origination Authorization (ROA) record
Route Leaking	One AS announces a large number of routes that it would not be expected to announce	Routing instability and potentially prefix hijacking
BGP Session Attack	Attacks against exchange of BGP information between ASes	Routing instability, denial of services, or traffic hijacking

Cybersecurity Framework Profile for Internet Routing (RSP)

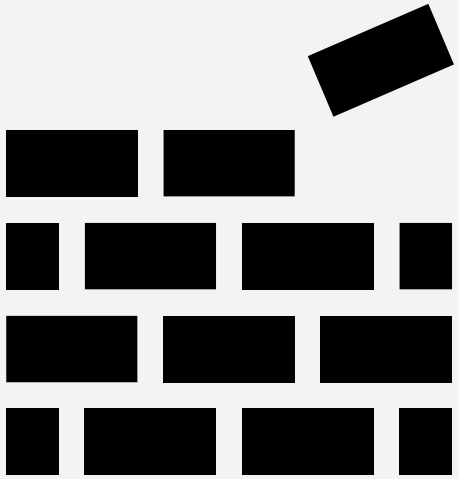
What is the Routing Security Profile (RSP)?

- The RSP is a framework for improving security and managing risks for internet routing, which is *one key piece of a larger critical infrastructure cybersecurity puzzle.*
- It approaches routing security from a holistic, risk management perspective.
- It is applicable for use by any autonomous system (AS) operator – large or small – to enhance routing security.



Goals of the Routing Security Profile

- The RSP serves as a foundational tool for network engineers, IT managers, cybersecurity professionals and decision-makers involved in network security risk management to evaluate, implement, and manage robust routing security policies.
- It aims to be adaptable and scalable to not only aid AS operators as they fortify their own network environments but also contribute to the broader goal of creating a more secure and resilient global internet infrastructure.



Cybersecurity Framework Profile for Internet Routing (Based on NIST CSF 1.1)

Key Takeaways & Next Steps

Key Takeaways:

- Threats to internet routing are diverse, persistent, and changing.
- Current efforts focus on developing and implementing security controls (e.g., RPKI).
- The Routing Security Profile (RSP) approaches routing security from a holistic, risk management perspective and is applicable for use by any Autonomous System (AS) operator to enhance routing security.
- The RSP is a tool for practitioners and network operators to advance routing security of any size organization – large or small.
- The RSP and the underlying technical controls must remain agile and continue to evolve to stay ahead of a constantly changing threat landscape.

Next Steps:

- Engage with broader internet ecosystem stakeholders to drive awareness and to further improve and advance this work for all AS operators, including ISPs, cloud service providers, government agencies, universities, and other organizations.
- Update this first version of the RSP based on feedback received from stakeholders and to reflect changes in the NIST CSF 2.0 (released on February 26, 2024).

Consumer Router Security

Consumer Router Security

- The US government views routers as a popular target for bad actors trying to steal information from consumers or to attack networks. Recent FBI advisories highlight how hackers can secretly install malware and use compromised routers to launch cyberattacks on critical U.S. infrastructure.
- Routers and modems are the pieces of equipment that convert the wired broadband service to Wi-Fi that we rely on every day. Almost every consumer, business, and school has at least one of these devices.
- Routers and modems can be provided by an ISP or purchased by consumers from many retail outlets.
- The cable industry has been focused on security for these devices for decades.
- CableLabs published a Best Common Practices (BCP) document in 2021 to provide guidelines for manufacturers to build secure routers and modems.
- The BCP guidelines are used by many cable operators when they purchase routers and modems to provide to consumers and to verify that consumer-purchased routers are secure and support updates before they are connected to an ISP's network.
- NIST references the CableLabs BCP throughout its *Cybersecurity for Consumer Grade Routers* profile that it intends to publish to provide guidance to the manufacturing community.
- Routers are not currently included in the FCC's Cybersecurity Labeling Program.

Next Steps:

- CableLabs is working to keep the Best Common Practices document up-to-date and coordinating with NIST to ensure routers and modems remain secure and responsive to threats.

Questions?

Priya Shrinivasan

Director, Technology Policy

p.shrinivasan@cablelabs.com

https://www.cablelabs.com/blog/internet-routing-security-framework