NIST SPECIAL PUBLICATION 1800-14A

# Protecting the Integrity of Internet Routing:

## Border Gateway Protocol (BGP) Route Origin Validation

**Volume A:**
**Executive Summary**

**William Haag**
Applied Cybersecurity Division
Information Technology Laboratory

**Doug Montgomery**
Advanced Networks Technology Division
Information Technology Laboratory

**Allen Tan**
The MITRE Corporation
McLean, VA

**William C. Barker**
Dakota Consulting
Silver Spring, MD

August 2018

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/secure-inter-domain-routing

National Institute of
Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

# Executive Summary

- It is difficult to overstate the importance of the internet to modern business and to society in general. The internet is essential to the exchange of all manner of information, including transactional data, marketing and advertising information, remote access to services, entertainment, and much more.
- The internet is not a single network, but rather a complex grid of independent interconnected networks. The design of the internet is based on a trust relationship between these networks and relies on a protocol known as the Border Gateway Protocol (BGP) to route traffic among the various networks worldwide. BGP is the protocol that internet service providers (ISPs) and enterprises use to exchange route information between them.
- Unfortunately, BGP was not designed with security in mind. Traffic typically traverses multiple networks to get from its source to its destination. Networks implicitly trust the BGP information that they receive from each other, making BGP vulnerable to route hijacks.
- A route hijack attack can deny access to internet services, misdeliver traffic to malicious endpoints, and cause routing instability. A technique known as BGP route origin validation (ROV) is designed to protect against route hijacking.
- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) has developed proof-of-concept demonstrations of BGP ROV implementation designed to improve the security of the internet's routing infrastructure.
- This NIST Cybersecurity Practice Guide demonstrates how networks can protect BGP routes from vulnerability to route hijacks by using available security protocols, products, and tools to perform BGP ROV to reduce route hijacking threats. The example implementation described in this guide aims to protect the integrity and improve the resiliency of internet traffic exchange by verifying the source of the route.

## CHALLENGE

Most of the routing infrastructure underpinning the internet currently lacks basic security services. In most cases, internet traffic must transit multiple networks before reaching its destination. Each network implicitly trusts other networks to provide (via BGP) the accurate information necessary to correctly route traffic across the internet. When that information is inaccurate, traffic will take inefficient paths through the internet, arrive at malicious sites that masquerade as legitimate destinations, or never arrive at its intended destination. These impacts can be mitigated through a widespread adoption of BGP ROV.

To date, ISPs and enterprises have been slow to adopt BGP ROV for reasons that include an unavailability of detailed BGP ROV deployment, operation, and management guidelines, as well as lingering concerns and questions about functionality, performance, availability, scalability, and policy implications. These concerns need to be addressed so that potential users of BGP ROV can appreciate the feasibility of using BGP ROV and the increased security that it can provide.

## SOLUTION

The NCCoE Secure Inter-Domain Routing (SIDR) Project is improving internet security by demonstrating how to use ROV to protect against route hijacks. The SIDR Project has produced a proof-of-concept example that demonstrates the use of BGP ROV in realistic deployment scenarios, has developed detailed deployment guidance, has addressed implementation and use issues, and has generated best practices and lessons learned. Project results are presented in this publicly available NIST Cybersecurity Practice Guide. This guide describes the following concepts:

- security objectives that are supported by implementing BGP ROV that uses Resource Public Key Infrastructure (RPKI) mechanisms
- an example solution of methods and tools that demonstrate and enable a practical implementation of BGP ROV
- how to protect your own internet addresses from route hijacking by registering them with trusted sources, thereby gaining assurance that traffic intended for your organization will not be hijacked when it is forwarded by entities that perform BGP ROV
- how to perform BGP ROV on received BGP route updates to validate, if possible, whether the entity that originated the route is in fact authorized to do so
- how to more precisely express your routing security requirements and/or service offerings

While the NCCoE used a suite of available products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and information technology (IT) system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

## BENEFITS

The NCCoE’s practice guide is intended to improve the security and stability of the global internet by allowing networks to verify the validity of BGP routing information and strengthen the security and stability of traffic flowing across the global internet—benefitting all organizations and individuals that use and rely on it. This practice guide can help your organization:

- reduce the number of internet outages due to BGP route hijacks
- ensure that internet traffic reaches its destination
- make informed decisions regarding routes and what actions to take in cases when BGP ROV implementation has not been performed or has indicated that an advertised route is invalid

## SHARE YOUR FEEDBACK

You can view or download the guide at https://nccoe.nist.gov/projects/building-blocks/secure-inter-domain-routing. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at sidr-nccoe@nist.gov.

---

## TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as “Technology Partners/Collaborators” herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

---

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses’ most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

**LEARN MORE**

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200