PROJECT DESCRIPTION

SECURE INTER-DOMAIN ROUTING

Part 1: Route Hijacks

William Haag, Jr.
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Doug Montgomery
National Institute of Standards and Technology

William C. Barker
Dakota Consulting Inc.

Allen Tan
The MITRE Corporation

July 6, 2017
sidr-nccoe@nist.gov

This revision incorporates comments from the public.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a Community of Interest (COI), including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

Abstract

Since the creation of the internet, the Border Gateway Protocol (BGP) has been the default routing protocol to route traffic among organizations (Internet Service Providers (ISPs) and Autonomous Systems (ASes)). While the BGP protocol performs adequately in identifying viable paths that reflect local routing policies and preferences to destinations, the lack of built-in security allows the protocol to be exploited. As a result, attacks against internet routing functions are a significant and systemic threat to internet based information systems. The consequences of these attacks can: (1) deny access to internet services; (2) detour internet traffic to permit eavesdropping and to facilitate on-path attacks on endpoints (sites); (3) misdeliver internet network traffic to malicious endpoints; (4) undermine IP address-based reputation and filtering systems; and (5) cause routing instability in the internet.

To improve the security of inter-domain routing traffic exchange, NIST has begun development of a Special Publication (SP 800-189 – in preparation) that provides security recommendations for the use of inter-domain protocols and routing technologies. These recommendations aim to protect the integrity of internet traffic exchange. Implementing BGP Route Origin Validation (ROV) based upon the Resource Public Key Infrastructure (RPKI) can mitigate accidental and malicious attacks associated with route hijacking. The NCCoE understands that organizations and individuals have internet performance expectations and requirements to protect against malicious cyber attacks. It is expected that eventual wide-scale deployment of RPKI-based ROV will significantly enhance the overall security and robustness of the internet.

This project will result in a NIST Cybersecurity Practice Guide—a publicly available description of the solution and practical steps needed to implement practices that effectively demonstrate the security and functionality of all components of ROV.

Keywords

Autonomous Systems (AS), Border Gateway Protocol (BGP), Denial-of-Service (DoS) attacks, Internet Service Providers (ISPs), Regional Internet Registry (RIR), Resource Public Key Infrastructure (RPKI), route hijack, Route Origin Authorization (ROA), Route Origin Validation (ROV)

Disclaimer

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology or the National Cybersecurity Center of Excellence, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Table of Contents

1. Executive Summary

Purpose

This document describes an NCCoE project focused on improving inter-domain routing security for which we are seeking public feedback.

The purpose of the project is to demonstrate and explain how to use security protocols to protect the integrity of internet routing functions using Border Gateway Protocol (BGP) information that is used to route information from its source to destination addresses. All organizations and individuals who are dependent on the internet would benefit greatly from implementing these protocols. If widely implemented, these enhancements would significantly improve the security and stability of the global internet.

The proposed project focuses on a proof-of-concept implementation of Internet Engineering Task Force (IETF) security protocols and National Institute of Standards and Technology (NIST) implementation guidance in order to protect ISPs and Autonomous Systems (ASes) against wide spread and localized attacks. One example of such attacks is route hijacking, in which an AS originates a prefix (either maliciously or accidentally) that is assigned by its legitimate owner to be originated by another AS. Subsequently, this fraudulent announcement is received by other ASes throughout the internet. ASes see multiple routes and will use their local policies to choose one of the routes. Since both routes seem legitimate, some ASes will choose the fraudulent route.

This project will demonstrate BGP Route Origin Validation (ROV), using Resource Public Key Infrastructure (RPKI), to address and resolve route hijacking issues. Using ROV, an AS can protect routes that it originates and discard bogus routes that do not come from legitimate originating ASes. While commercial implementations of BGP origin validation are available, the adoption rate in the United States has, to date, been slow. The goal of the project is to pilot RPKI-ROV in realistic deployment scenarios, develop detailed deployment guidance, identify implementation and use issues, and generate best practices and lessons learned. This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps required to implement a cybersecurity reference design that addresses this challenge.

Scope

The scope of this project covers the roles of both address owners (e.g., enterprises, providers of Internet services) and network operators that provide BGP-based routing services to clients and their peer networks in other autonomous systems.

For address owners, the scope of this project includes two implementation models of RPKI: hosted RPKI and delegated RPKI. For hosted RPKI, a Regional Internet Registry (RIR) provides the infrastructure to host the certificate authorities and private keys used to sign the Route Origin Authorizations (ROAs) for address blocks registered in their region. A ROA authorizes one or more prefixes originated from an AS, and is signed with the private key associated with the prefix owner's digital certificate. Address owners who are registered with the RIR can access the tools provided by the RIR to create and publish ROAs. Those ROAs are stored in the RIR's RPKI repositories. Network operators around the world can retrieve the ROAs from the RIR RPKI repositories, validate their integrity and authenticity, and use the information in the ROAs to detect validity of the origin AS in received BGP updates. Any routes (i.e. updates) which fail ROV (i.e. routes that are identified as invalid) may be assigned lower priority in route selection or may be discarded. For delegated RPKI, address owners (e.g. ISPs or large enterprises) operate a delegated RPKI certificate authority, and their own publication point to store associated certificates, keys and ROAs. This implementation model allows an ISP or other entity to offer Hosted or Delegated RPKI resources to its customers. This project will focus on the Hosted RPKI model initially and then the Delegated RPKI model.

For the Hosted RPKI model, NCCoE will create the necessary RPKI certificates and create/sign ROAs within the American Registry for Internet Numbers (ARIN) or other RIRs. The following are the other RIRs: African Network Information Center (AFRINIC), Asia-Pacific Network Information Centre (APNIC), Latin America and Caribbean Network Information Center (LACNIC), and Réseaux IP Européens Network Coordination Centre (RIPE-NCC). The project will produce guidance and document issues encountered in exercising the interfaces and services provided by RIR hosted RPKI services.

For both hosted and delegated RPKI deployment scenarios, the project will test and document issues and best practices for the creation, update, deletion and management of RPKI objects, the accessibility, robustness and responsiveness of RPKI repositories, and the potential issues that arise when ROA creation is integrated in other address management business processes of large enterprises and service providers. The project will seek Community of Interest (COI) partners from various classes of enterprises and service providers that can contribute to the design and conduct of tests in these areas.

For network operators, the scope of the project will focus on deployment and use scenarios for use of RPKI-ROA information for BGP ROV [RFC 6811]. This component of the project will test and document issues and best practices for the operation of RPKI validating caches (RPKI VC) and RPKI-aware BGP routers. It will also focus on the issues of robustness and responsiveness of these components, the range of routing policies that can be configured with them, and the potential issues that arise when RPKI-based ROV is integrated in other business, security and management processes of large network operators. The project will solicit COI and National Cybersecurity Excellence Partnership (NCEP) partners that can provide commercial-off-the-shelf (COTS) and open-source products that implement the components necessary for BGP network operators to acquire, validate, and use RPKI information to implement BGP ROV. The project will also seek COI partners from various classes of network operators (e.g. enterprise, stub ISPs, regional networks, transit ISPs, internet exchange point operators) that can contribute to the design and conduct tests in realistic scenarios (e.g. BGP routing architectures (eBGP and iBGP), route reflectors, ISP architectures, etc.).

For each deployment scenario RPKI origin validation functionality will be validated, including various scenarios for BGP ROV results (valid, invalid, and not-found [RFC 6811]), and vendor / implementation specific options for RPKI-ROV based filtering mechanisms will be examined. This project will result in a freely available NIST Cybersecurity Practice Guide describing steps to test, adopt, deploy, and manage RPKI based ROV for both address owners and network operators, identify implementation and interoperability issues, provide sample deployment architectures, and provide best practices and lessons learned.

The IETF has also developed a new protocol called BGPsec which provides cryptographic protection for the entire AS path in an update. This security extension to BGP would help prevent AS path modification attacks (e.g. maliciously shortening the AS path to redirect traffic or altering an announced prefix to a more specific prefix, etc.). Adoption and deployment of BGPsec is expected to be slower relative to that of ROV, while wide-scale deployment of ROV will mitigate at least a significant component of routing vulnerability that has to do with accidental mis-origination of routes. Hence, this effort initially focuses on BGP ROV, and consideration of the BGPsec protocol is likely to be outside the scope of this project.

Assumptions/Challenges

The vast installed base of legacy systems is a significant factor inhibiting companies from taking advantage of new security innovations. Additionally, there are some usability and technical questions that impede adoption of secure inter-domain routing technology.

To date adoption of RPKI-based ROV has been relatively slow, with less than 10% of the routes in the global Internet covered by ROAs. The ARIN region has the smallest deployment (~1.3%), while LACNIC (~21%) and RIPE (~12%) have more aggressive adoption rates. Impediments to wider adoption in the ARIN region include lack of detailed guidance on the implementation of RPKI-ROV in commercial routers and validating caches, detailed deployment, operation and management guidelines, and lack of experience with the security and robustness associated with the new technologies. Without detailed guidance, lingering concerns and questions about the functionality, performance, availability, scalability, and policy implications will continue to slow the wide scale adoption of BGP ROV.

Background

Most of the routing infrastructure underpinning the internet currently lacks basic security services. In most cases, internet traffic must transit multiple ISPs before reaching its destination. Each network operator implicitly trusts other ISPs to provide (via BGP) accurate information necessary for network traffic to be routed correctly. When that information is inaccurate, traffic will either take inefficient paths through the internet, arrive at malicious sites that masquerade legitimate destinations, or never arrive to its intended destination. The consequences of these attacks can: (1) deny access to internet services, (2) detour internet traffic to permit eavesdropping and to facilitate on-path attacks on endpoints (sites), (3) misdeliver internet network traffic to malicious endpoints, (4) undermine IP address-based reputation and filtering systems, and (5) cause routing instability in the internet. These impacts can be mitigated through widespread adoption of current and emerging internet security protocols.

2. Scenarios

The project will demonstrate two scenarios for ROV. These scenarios may involve different entities completing different tasks. The entities can be categorized into two groups: organizations (or Address Holders) and Network Operators. Address Holders are the entities who have been assigned the IP prefixes. Network Operators are the entities that perform BGP ROV. Below is a list of tasks completed by the different entities.

Note: Network Operators (i.e. someone operating an AS) are also typically Address Holders. Large Network Operators (major ISPs) might be the one who go fordelegated RPKI models and host RPKI services for their many customers.

- Address Holders perform the following:
    - Hosted RPKI
        - Resource certificate maintenance, and ROA creation, maintenance, and revocation (ROA is revoked by the revoking the corresponding end-entity certificate [RFC 6480])
        - Repository accessibility, robustness, responsiveness
    - Delegated RPKI
        - RPKI CA / Repository Deployment
        - Resource certificate maintenance, and ROA creation, maintenance, and revocation
        - Repository accessibility, robustness, responsiveness
        - RPKI management, monitoring, and debugging tools
    - Note: scenarios might vary depending on RIR region. Initially we will focus on the ARIN region.
- Network Operators perform the following:
    - RPKI Validating Cache (RPKI VC) Deployment
        - Repository interoperability: rsync, RPKI Repository Delta Protocol (RRDP) [reference: draft-ietf-sidr-delta-protocol-08]
        - RPKI VC interoperability with routers, route reflectors, route servers: RPKI-Router protocol [RFC 6810]
    - ROV-enabled BGP Routers (Create ROV Policy configuration options)
        - Stub AS ROV Configurations
            - RPKI robustness, responsiveness, and security
        - Transit AS ROV Configurations
            - RPKI robustness, responsiveness, and security

        - Intra-AS Configurations
            - iBGP ROV signaling [ref: RFC 8097], Route-reflectors, monitoring and management
        - Internet Exchange Point (IXP) Configurations
            - eBGP ROV signaling [ref: draft-ietf-sidr-route-server-rpki-light], Route-servers, monitoring and management
        - Other scenarios
            - BGP-based DDoS mitigation services

Scenario 1: Hosted RPKI for ROV

In this scenario, the RIR hosts a Certificate Authority (CA) and signs ROAs for resources within the region the RIR oversees. An organization that owns resources (IP subnets, ASes) gets digital certificates from its RIR, and signs ROAs for all prefixes that it owns. Once an organization (address holder) signs its ROA, other ASes can pull this information from the RIR repositories and validate the origin of the route. Using the tasks described above, below are the steps to implement ROV:

1. Address holder registers with the RIR to obtain resource certificate and create ROAs:
    - ROA creation, maintenance, and revocation
    - Repository accessibility, robustness, responsiveness
2. Network Operator performs the following for BGP ROV:
    - Use rsync or RRDP for communication between RIR Validators and local RPKI VC
    - Local RPKI VC receives all ROAs from the RIR Validators (validates information)
    - Local RPKI VC communicates with its eBGP router (sends ROA data to router) using the RPKI-Router protocol
    - eBGP router receives BGP advertisements from its neighbors
    - eBGP router checks advertisement against ROA information received from RPKI VC
    - eBGP router makes routing decision based on ROV Policy configuration options

Scenario 2: Delegated RPKI for ROV

Delegated RPKI does not require the RIR to host the private key of an AS's delegated RPKI key pair. In this scenario, the organization (Address Holder) can host and delegate RPKI services to its customers who participate in BGP. To participate, the organization must have IPv4 or IPv6 prefixes that are obtained from an RIR. It also needs to have signed a Registration Services Agreement (RSA) to cover all resources (or ROAs) it needs to certify. The organization must have an account with its RIR to manage the resources it plans to certify. Once these items are met, the organization must set up its RPKI system to: perform work maintaining the CA, exchange public keys of the key pairs it created with its RIR, and create a RPKI repository to host the resource certificates and ROAs. Steps for implementation are similar to the Hosted RPKI for ROV:

1. Address holder performs the following:
    - Create an online account with RIR, which is used to manage the resources (ASes, prefixes) for certification
    - Create and manage its own CA or use a third party to manage CA for resources
    - Create an RPKI repository to publish resource certificates and ROAs
    - Have customers create and sign ROAs for their IP prefixes (Address holder can create a ROA for an AS that does not belong to them; ASes may allow their transit provider to originate their prefix.)
        - ROA creation, maintenance, and revocation
    - Exchange public key associated with Delegated RPKI private key with RIR
2. Network operators perform the following for BGP ROV:
    - Create local RPKI VC to gather ROAs and certificates from the RPKI repositories (validates information)
    - Local RPKI VC communicates with its eBGP router (sends ROA data to router)
    - Large network operators may provide RPKI VC services to their customer ASes (i.e. customer AS may outsource RPKI VC function to a third party)
    - Router receives BGP advertisements from its neighbors
    - Router checks advertisement against ROA information received from RPKI VC
    - Router makes decision based on ROV policy configuration options

3. High-Level Architecture

This diagram identifies a high-level architecture of the areas of the internet technologies that are required for an organization to perform ROV for the scenarios above. During the development of the laboratory environment implementing the use case, the diagram will be refined to describe detailed components and mapped to a physical architecture in the lab environment for the specific scenario being implemented.

Figure 1: Notional Architecture – Hosted RPKI for ROV

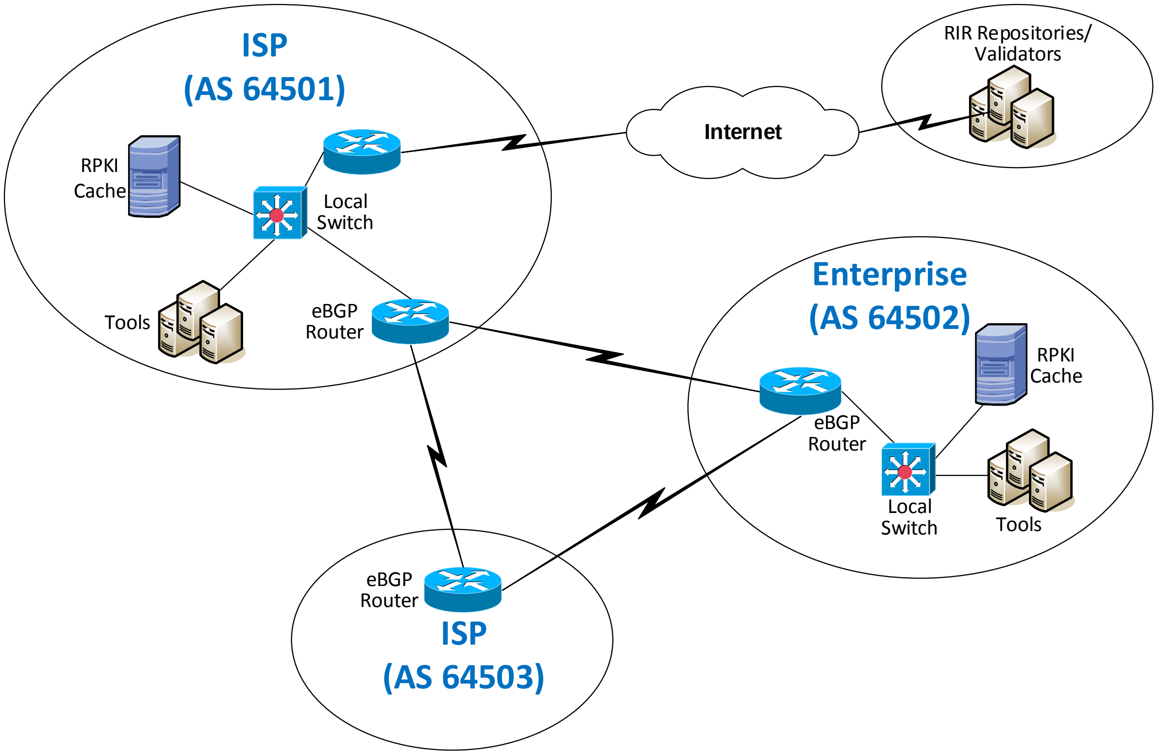
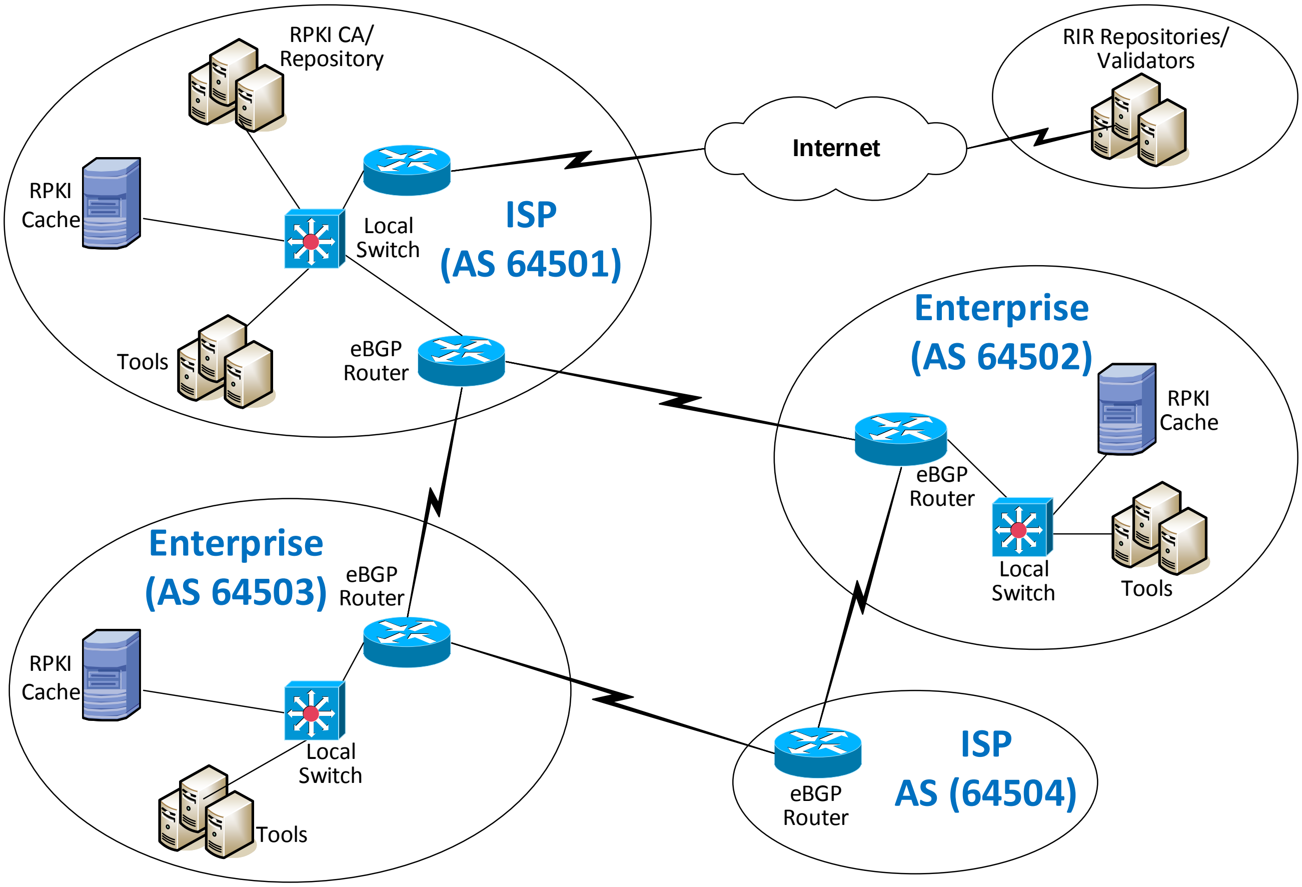


Figure 2: Notional Architecture – Delegated RPKI for ROV



Component List

A ROV solution includes but is not limited to the following components:

- Routers with software that supports BGP, RPKI-ROV, and RPKI-Router protocol
- RPKI Validator Cache (or RPKI VC)
- ROA data
- Operations monitoring and validation tools
- RIR RPKI repository
- Data storage for operations monitoring and validation
- BGP updates (minimum routes received by lab routers)

Desired Architecture Characteristics

This section expands on the component list. Supporting infrastructure components as well as specific requirements and characteristics of critical components are provided below.

1. Network
    - Enterprise-grade network supporting servers and security tools
    - Router
        - eBGP enabled
        - Support for RPKI-Router protocol to communicate with RPKI VC
        - Minimum commercial grade router requirements
        - Support for IPv4/IPv6 routes
        - Internet feed to ISP router
    - Switches
    - Servers
    - Internet link from ISP
    - Government related requirements (Managed Trusted Internet Protocol Services (MTIPS) required or Trusted Internet Connection (TIC))
    - Firewalls
2. RPKI
    - Design supports RPKI specifications described in RFCs 6480-6492
    - RPKI VC
        - System requirements: Refer to the document of the specific RPKI VC
        - Rsync, RRDP and RPKI-Router protocol capabilities
        - Minimal performance requirements (as specified by RPKI VC application vendor)
    - Hosted RPKI support from RIR
3. Tools
    - Monitoring and management tools for RPKI-ROV
        - Functionality monitoring of routers and RPKI VC
        - Performance of BGP ROV capable routers
        - Additional tools for securing ROV

4. Relevant Standards and Guidance

The references, standards, and guidelines that are applicable to the secure inter-domain routing project include Federal policies and standards, NIST guidelines and recommendations, and IETF standards (published as *requests for comments*, or RFCs). Relevant documents include: OMB Circular A-130; FIPS 140-2; SP 800-37 Rev. 1; SP 800-53 Rev. 4; SP 800-54; SP 800-57 Part 1; SP 800-130; SP 800-152; SP 800-160; NIST *Framework for Improving Critical Infrastructure Cybersecurity*; and RFCs 793, 3882, 4012 5280, 5575, 6092, 6472, 6480, 6481-6495, 6810, 6811, 6907, 7115, 7318, 7454, 7674, 7908, 7909, and 8097. The project will also be informed by an in-progress draft 800-series NIST Special Publication (*Secure Interdomain Traffic Exchange)* and two internet draft BGP RFCs (*BGPsec Protocol Specification* and *BGPsec Operational Considerations*). These documents will directly influence the development of the project, as well as the architecture and design. Some documents provide security guidelines by which this project will abide. Some documents describe issues and potential solutions to the issues. Some documents provide specific standards to solutions that this project will use. Brief descriptions of relevant document content for completed references are included below.

- Managing Federal Information as a Strategic Resource, OMB Circular A-130, Executive Office of the President, Office of Management and Budget, July 28, 2016. https://obamawhitehouse.archives.gov/omb/circulars_a130_a130trans4/
- *Security Requirements for Cryptographic Modules*, FIPS 140-2 (including change notices as of 12-03-2002), National Institute of Standards and Technology, May 2001. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
- Guide for Applying the Risk Management Framework to Federal Information Systems a Security Life Cycle Approach, SP 800-37 Revision 1, National Institute of Standards and Technology, February 2010. http://dx.doi.org/10.6028/NIST.SP.800-37r1
- Security and Privacy Controls for Federal Information Systems and Organizations, SP 800-53 Revision 4, National Institute of Standards and Technology, April 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- Border Gateway Protocol Security, NIST Special Publication 800-54, July 2007. http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf
- Recommendation for Key Management - Part 1: General, SP 800-57 Part 1, Revision 3 and Draft Revision 4, National Institute of Standards and Technology, January 2016. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf. http://csrc.nist.gov/publications/drafts/800-57/sp800-57p1r4_draft.pdf
- A Framework for Designing Cryptographic Key Management Systems, SP 800-130, National Institute of Standards and Technology, August 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf
- A profile for U.S. Federal Cryptographic Key Management Systems, SP 800-152, National Institute of Standards and Technology, October 2015. http://dx.doi.org/10.6028/NIST.SP.800-152

- DRAFT Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems (Second Draft), SP 800-160, National Institute of Standards and Technology, May 4, 2016. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf
- Cybersecurity Framework, National Institute of Standards and Technology. http://www.nist.gov/cyberframework/
- Postel, Transmission Control Protocol, IETF RFC 793, September 1981. https://tools.ietf.org/rfc/rfc793.txt
- Turk, Configuring BGP to Block Denial-of-Service Attacks, IETF RFC 3882, September 2004. https://tools.ietf.org/rfc/rfc3882.txt
- Blunk, Damas, Parent, and Robachevsky, Routing Policy Specification Language next generation (RPSLng), IETF RFC 4012, March 2005. https://tools.ietf.org/html/rfc4012
- Cooper, Santesson, Farrell, Boeyen, Housley, and Polk, Internet X.509 Public Key Infrastructure Certification and Certificate Revocation List (CRL) Profile, IETF RFC 5280, May 2008. http://www.ietf.org/rfc/rfc5280.txt.
- Marques et al., Dissemination of Flow Specification Rules, IETF RFC 5575, August 2009. https://tools.ietf.org/html/rfc5575
- Woodyatt, Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service, IETF RFC 6092, January 2011. https://tools.ietf.org/html/rfc6092
- Kumari and Sriram, Recommendation for Not Using AS_SET and AS_CONFED_SET in BGP, IETF RFC 6472, December 2011. https://tools.ietf.org/html/rfc6472
- Lepinski and Kent, An Infrastructure to Support Secure Internet Routing, IETF RFC6480, February 2012. https://tools.ietf.org/html/rfc6480
- Huston, Loomans, and Michaelson, A Profile for Resource Certificate Repository Structure, IETF RFC 6481, February 2012. https://tools.ietf.org/html/rfc6481
- Lepinski, Kent, and Kong, A Profile for Route Origin Authorizations (ROAs), IETF RFC 6482, February 2012. https://tools.ietf.org/html/rfc6482
- Huston and Michaelson, Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs), IETF RFC 6483, February 2012. https://tools.ietf.org/html/rfc6483
- Kent, Kong, Seo, and Watro; Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI); IETF RFC 6484; February 2012. http://tools.ietf.org/html/rfc6484
- Huston, The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI), IETF RFC 6485, February 2012. https://tools.ietf.org/html/rfc6485
- Austein, Huston, Kent, and Lepinski; Manifests for the Resource Public Key Infrastructure (RPKI); IETF RFC 6486; February 2012. https://tools.ietf.org/html/rfc6486
- Huston, Michaelson, and Loomans, A Profile for X.509 PKIX Resource Certificates, IETF RFC 6487, February 2012. https://tools.ietf.org/html/rfc6487

- Lepinski, Chi, Kent; Signed Object Template for the Resource Public Key Infrastructure (RPKI); IETF RFC 6488; February 2012. https://tools.ietf.org/html/rfc6488
- Huston, Michaelson, Kent; Certificate Authority (CA) Rollover in the Resource Public Key Infrastructure (RPKI); IETF RFC 6489; February 2012. https://tools.ietf.org/html/rfc6489
- Huston, Weiler, Michaelson, and Kent; Resource Public Key Infrastructure Trust Anchor Locator; IETF RFC 6490; February 2012. https://tools.ietf.org/html/rfc6490
- Manderson, Vegoda, and Kent; Resource Public Key Infrastructure (RPKI Objects Issued by IANA; RFC 6491; February 2012. https://tools.ietf.org/html/rfc6491
- Huston, Loomans, Ellacott, and Austein, A Protocol for Provisioning Resource Certificates, IETF RFC 6492, February 2012. https://tools.ietf.org/html/rfc6492
- Bush, The Resource Public Key Infrastructure (RPKI) Ghostbusters Record, IETF RFC 6493, February 2012. https://tools.ietf.org/html/rfc6493
- Gagliano, Krishnan, and Kukec, Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND), IETF RFC 6494, February 2012. https://tools.ietf.org/html/rfc6494
- Gagliano, Krishnan, and Kukec, Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields, IETF RFC 6495, February 2012. https://tools.ietf.org/html/rfc6495
- Bush and Austein; The Resource Public Key Infrastructure (RPKI) to Router Protocol, IETF RFC 6810, January 2013. https://tools.ietf.org/html/rfc6810
- Mohapatra, Scudder, Ward, Bush, and Austein; BGP Prefix Origin Validation; IETF RFC 6811; January 2013. https://tools.ietf.org/html/rfc6811
- Manderson, Sriram, White, Use Cases and Interpretations of Resource Public Key Infrastructure (RPKI) Objects for Issuers and Relying Parties; IETF RFC6907; March 2013. https://tools.ietf.org/html/rfc6907
- Bush, Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI), IETF RFC 7115, January 2014. https://tools.ietf.org/html/rfc7115
- Newton and Huston, Policy Qualifiers in Resource Public Key Infrastructure (RPKI) Certificates, IETF RFC 7318, July 2014. https://tools.ietf.org/html/rfc7318
- Durand, Pepelnjak, and Doering, BGP Operations and Security, IETF RFC 7454, February 2015. https://tools.ietf.org/html/rfc7454
- Haas, Clarification of the Flowspec Redirect Extended Community, IETF RFC 7674, October 2015. https://tools.ietf.org/html/rfc7674
- Sriram, Montgomery, McPherson, Osterweil, and Dickson, Problem Definition and Classification of BGP Route Leaks, IETF RFC 7908, June 2016. https://tools.ietf.org/html/rfc7908
- Kisteleki and Haberman, Securing Routing Policy Specification Language (RPSL) Objects with Resource Public Key Infrastructure (RPKI) Signatures, IETF RFC 7909, June 2016. https://tools.ietf.org/html/rfc7909

- Mohapatra, Patel, Scudder, Ward, and Bush, BGP Prefix Origin Validation State Extended Community, IETF RFC 8097, March 2017. https://tools.ietf.org/html/rfc8097

5. Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to the relevant standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF), and other NIST standards. This exercise is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Table 1: Security Control Map

Example Characteristic		Cybersecurity Standards & Best Practices			
Security Characteristics	Example Capability	Function	Category	Subcategory	Informative References
Integrity and Authenticity	Ensure BGP routes are sourced from the owner of the IP prefixes	PROTECT (PR)	Data Security (PR.DS)	PR.DS-1, PR.DS2, PR.DS-6	ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 SC-28 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8
		DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-2, DE.CM-4, DE.CM-7	NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE20 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3 NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
			Detection Processes (DE.DP)	DE.DP-3	ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
Anomalous Route Detection	Ensure the detection anomalous routes to block misrouting or to report the anomalous events	DETECT (DE)	Detection Processes (DE.DP)	DE.DP-4	ISO/IEC 27001:2013 A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4

Example Characteristic		Cybersecurity Standards & Best Practices			
Security Characteristics	Example Capability	Function	Category	Subcategory	Informative References
System and Application Hardening	Adjust security controls on the server and/or software applications such that security is maximized ("hardened") while maintaining INTENDED USE.	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-1, PR.IP-2	ISO/IEC 27001:2013 A.6.1.5, A.12.1.2, A.12.5.1, A.12.6.2 A.14.1.1, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4 A.14.2.5 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8
Device Protection	Ensure the protection of devices, communications, and control networks	PROTECT (PR)	Access Control (PR.AC)	PR.AC-3, PR.AC-5	ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.1.3, A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-19, AC-20, SC-7
		PROTECT (PR)	Protective Technology (PR.PT)	PR.PT-4	ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
Incident Response	Ensure the integrity of network connections in the case of incidents that result in a compromise, the effects of the compromise can be limited by exclusion of systems and devices that have not implemented the integrity mechanisms	RESPOND (RS)	Communications (RS.CO)	RS.CO-2, RS.CO-3	ISO/IEC 27001:2013 A.6.1.3, A.16.1.2, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8, CA-2, CA-7, CP-2, IR4, IR-8, PE-6, RA-5, SI-4
		RESPOND (RS)	Mitigation (RS.MI)	RS.MI-1	ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 IR-4

Example Characteristic		Cybersecurity Standards & Best Practices			
Security Characteristics	Example Capability	Function	Category	Subcategory	Informative References
COOP and Disaster Recovery	Ensure that ROV has recovery capabilities or fails to baseline routing without interruption after damage or destruction of data, hardware, or software	IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-5	ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
				ID.AM-6	ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Appendix A – References

“Worldwide Infrastructure Security Report,” Vol. XI, Arbor Networks report (2016). https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf.

M. Lepinski (Ed.) and K. Sriram (Ed.), “BGPsec Protocol Specification,” IETF work-in-progress. https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-protocol/

M. Adalier, K. Sriram, O. Borchert, K. Lee, and D. Montgomery, “High Performance BGP Security: Algorithms and Architectures”, North American Network Operators Group (NANOG69), Washington D.C, February 2017. https://nanog.org/meetings/abstract?id=3043

M. Lepinski and S. Turner, “An Overview of BGPsec,” IETF work-in-progress. https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-overview/

S. Turner, “BGPsec Algorithms, Key Formats, & Signature Formats,” IETF work-in-progress. https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-algs/

C. Morrow and A. Retana, “BGPsec Operational Considerations,” IETF work-in-progress. https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-ops/

A. Pilosov, A. and T. Kapela, "Stealing the Internet: An Internet-Scale Man in the Middle Attack", 16th Defcon Conference, August 2008, https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf

Cybersecurity Framework, National Institute of Standards and Technology [Web site], http://www.nist.gov/cyberframework/ [accessed 2/25/14].

“RPKI Deployment Monitor,” NIST’s online monitor with Global and Regional views. https://rpki-monitor.antd.nist.gov/

NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013 (including updates as of January 15, 2014), 460pp. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

D.R. Kuhn, K. Sriram, and D. Montgomery, “Border Gateway Protocol Security,” NIST Special Publication 800-54, July 2007. http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf

“Heightened DDoS Threat Posed by Mirai and Other Botnets,” US-CERT alert TA16-288A, October 14, 2016. https://www.us-cert.gov/ncas/alerts/TA16-288A

Toonk, A., "What caused the Google service interruption", BGPMON Blog, March 2015, http://www.bgpmon.net/what-caused-the-google-service-interruption/.

Toonk, A., "Massive route leak causes Internet slowdown", BGPMON Blog, June 2015, http://www.bgpmon.net/massive-route-leak-cause-Internet-slowdown/.

Toonk, A., BGPstream and The Curious Case of AS12389, [Website], https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/ [accessed 5/2/17]

Resource Public Key Infrastructure (RPKI), American Registry for Internet Numbers, [website], https://www.arin.net/resources/rpki/index.html [accessed 5/9/17]

Tools and Resources (for RPKI service), RIPE Network Coordination Centre, [website], https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources [access 5/9/17]

K. Sriram, and D. Montgomery, “Secure Inter-Domain Traffic Exchange,” NIST Special Publication 800-189, draft (in preparation).

Appendix B - Acronyms and Abbreviations

AFRINIC	African Network Information Center
APNIC	Asia-Pacific Network Information Center
ARIN	American Registry for Internet Numbers
AS	Autonomous System
BGP	Border Gateway Protocol
CA	Certificate Authority
COI	Community of Interest
COTS	Commercial-off-the-shelf
DNS	Domain Name System
DoS	Denial of Service
eBGP	Exterior Border Gateway Protocol
iBGP	Interior Border Gateway Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISP	Internet Service Provider
IXP	Internet Exchange Point
LACNIC	Latin America and Caribbean Network Information Center
MTIPS	Managed Trusted Internet Protocol Services
NANOG	North American Network Operators Group
NCCoE	National Cybersecurity Center of Excellence
NCEP	National Cybersecurity Excellence Partnership
NIST	National Institute of Standards and Technology
RFC	Request for Comments
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	Regional Internet Registry
ROA	Route Origin Authorization
ROV	Route Origin Validation
RPKI	Resource Public Key Infrastructure
RPKI VC	RPKI Validating Cache
RSA	Registration Services Agreement

SIDR	Secure Inter-Domain Routing
TIC	Trusted Internet Connection

APPENDIX C – GLOSSARY

Autonomous System (AS)

Within the internet, an autonomous system (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the internet.

AS Path Modification

An adversary AS that receives a BGP update may illegitimately remove some of the preceding ASes in the AS_PATH attribute of the update to make the path length seem shorter. When the update modified in this manner is propagated, the ASes upstream can be deceived to believe that the path to the advertised prefix via the adversary AS is shorter. By doing this, the adversary AS may increase (illegitimately) its revenue from its customers, or may be able to eavesdrop on traffic that would otherwise not transit through their AS [Draft SP 800-189 (in preparation)].

Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the internet. The protocol is often classified as a path vector protocol, but is sometimes also classified as a distance-vector routing protocol.

Border Gateway Protocol Security (BGPsec)

BGPsec is based on a path attribute BGPsec_Path, which is an optional non-transitive attribute of BGP and, when in use, will replace the AS_Path attribute. Along with AS path information, the BGPsec_Path attribute also carries a set of digital signatures (one corresponding to each AS in the path) that provide cryptographic protection against modification of the AS path or prefix.

Certification Authority (CA)

An entity that issues and manages certificates.

Certificate Policy (CP)

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Denial of Service (DoS)

Distributed Denial of Service (DDOS), an attack where multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack.

Domain Name System (DNS)

The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or any resource connected to the internet or a private network. It associates various information with domain names assigned to each of the participating entities.

Forwarding Information Base (FIB)

A forwarding information base (FIB), also known as a forwarding table, is most commonly used in network bridging, routing, and similar functions to find the proper outgoing interface to which the input interface should forward a packet.

Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the internet architecture and the smooth operation of the internet. It is open to any interested individual.

Internet Protocol (IP)

The Internet Protocol (IP) is the principal communications protocol in the internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the internet.

IP Address

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

IP Prefix

IP address prefixes are patterns that match the first *n* binary bits of an IP address. The modern standard form of specification of the network prefix is using CIDR notation, which is used for both IPv4 and IPv6. CIDR notation counts the number of bits in the prefix and appends that number to the address after a slash (/) character separator: 192.168.0.0, net mask 255.255.255.0 is written as 192.168.0.0/24.

IP Prefix List

An IP prefix list specifies a list of networks. When an IP prefix list is applied to a neighbor, the device sends or receives only a route whose destination is in the IP prefix list. The software interprets the prefix lists in order, beginning with the lowest sequence number.

Internet Service Provider (ISP)

An internet service provider (ISP) is an organization that provides services for accessing and using the internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.

Prefix Hijacking
IP hijacking (sometimes referred to as BGP hijacking, prefix hijacking or route hijacking) is the illegitimate takeover of groups of IP addresses by corrupting internet routing tables.

Public Key
A cryptographic key that can be obtained and used by anyone to encrypt messages intended for a recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient.

Public Key Certificate
An electronic document used to prove the ownership of a public key.

Regional Internet Registry (RIR)
A Regional Internet Registry (RIR) is a not-for-profit organization that oversees Internet Protocol (IP) address space (IPv4 and IPv6) and the Autonomous System (AS) numbers within a specific geographical region. There are five regional RIRs across the globe: ARIN, RIPE, APNIC, LACNIC and AfriNIC.

Request for Comments (RFC)
An IETF standard.

Resource Public Key Infrastructure (RPKI)
RPKI provides a way to connect internet number resource information (such as Autonomous System numbers and IP addresses) to a trust anchor. The certificate structure mirrors the way in which internet number resources are distributed. See [RFC 6480], [RFC 6481], [RFC 6482], [RFC 6483], [RFC 6484], [RFC 6485], [RFC 6486], [RFC 6487], [RFC 6488], [RFC 6489], [RFC 6490], [RFC 6491], [RFC 6492], [RFC 6493], [RFC 6494], and [RFC 6495].

Route Leaks
A route leak is the propagation of routing announcement(s) beyond their intended scope. That is, an announcement from an Autonomous System (AS) of a learned BGP route to another AS is in violation of the intended policies of the receiver, the sender, and/or one of the ASes along the preceding AS path. See [RFC 7908].

Route Origin Authorization (ROA)
A Route Origin Authorization (ROA) is an attestation of a BGP route announcement. It attests that the origin AS number is authorized to announce the prefix(es). The attestation can be verified cryptographically using RPKI. See [RFC 6482].

Route Origin Validation (ROV)
Route origin validation is a mechanism by which route advertisements can be authenticated as originating from an expected autonomous system (AS). Origin validation uses one or more RPKI VC servers to perform authentication for specified BGP prefixes. To authenticate a prefix, the router queries the database of validated prefix-to-AS mappings,

which are downloaded from the RPKI VC server, and ensures that the prefix originated from an expected AS. See [RFC 6811] [RFC 7115].