May 19, 2025

Ms. Marlene Dortch
Secretary
Federal Communications Commission
45 L Street, NE
Washington, DC 20554

Re: *Reporting on Border Gateway Protocol Risk Mitigation Progress (PS Docket No. 24-146); Secure Internet Routing (PS Docket No. 22-90)*

Dear Ms. Dortch:

The Communications Sector Coordinating Council ("CSCC")[1] respectfully submits the attached report—*Deploying Resource Public Key Infrastructure (RPKI): Steps for Prioritization and Implementation*—as a contribution to the public record in the above-referenced proceedings.

This document was developed pursuant to the *Roadmap to Enhancing Internet Routing Security, A Report by the White House Office of the National Cyber Director*, and is intended to help organizations understand the risks posed by internet routing incidents, the benefits of mitigating the risks of such incidents through the use of the RPKI, and steps that can be taken to prioritize these mitigation efforts where needed. The document builds on established best practices in routing security and risk management, including those developed by the National Institute of Science and Technology ("NIST"), as well as the Broadband Internet Technical Advisory Group ("BITAG"), Mutually Agreed Norms for Routing Security ("MANRS"), CableLabs and other key industry-led initiatives.

This product is the result of robust collaboration between members of the Communications and IT Sector Coordinating Councils (for a full list of industry contributors see the acknowledgments below). It was also informed by consultative discussions with partners across the U.S. federal government, including the Office of the National Cyber Director ("ONCD"), the Cybersecurity and Infrastructure Security Agency ("CISA"), NIST, and the National Telecommunications and Information Administration ("NTIA").

[1] The Communications Sector Coordinating Council ("CSCC") (www.comms-scc.org) was established to help coordinate initiatives to improve the physical security and cybersecurity of sector assets; to ease the flow of information within the communications sector, across critical infrastructure sectors, and with designated federal agencies; and to address issues related to response and recovery following an incident or event.

- Section 1 summarizes the role of internet routing and Border Gateway Protocol ("BGP").
- Section 2 introduces the RPKI and discusses the potential benefits of its widespread use.
- Section 3 lays out a three-step process to make use of the RPKI, including the identification of internet resources and assets, their prioritization based on the potential consequences of a BGP attack, and the application of RPKI publication to address these risks.
- Section 4 is a playbook for all network operators, providing them with step-by-step guidance for describing routing intent by publishing RPKI Route Origin Authorization ("ROA") objects.
- Section 5 is a playbook geared toward enterprise networks that provides additional guidance to use in tandem with the general playbook outlined in section 4.
- Section 6 is a playbook of additional actions specific to ISPs to perform Route Origin Validation ("ROV").
- Section 7 concludes the discussion.

The following industry contributors are acknowledged for their work on this effort:

- AT&T
- Amazon Web Services
- CableLabs
- Charter
- Cisco
- Cloudflare
- Comcast
- Cox
- Communications Sector Coordinating Council (CSCC)
- CTIA
- Cybersecurity Coalition
- Google Cloud
- Internet Society
- IT Sector Coordinating Council (ITSCC)
- Juniper Networks
- Lumen
- Microsoft
- NCTA
- NTCA
- T-Mobile
- USTelecom
- Verizon

Respectfully submitted,

/s/ Paul Eisler

Paul Eisler

Vice President, Cybersecurity
USTELECOM – THE BROADBAND ASSOCIATION
601 New Jersey Avenue, N.W., Suite 600
Washington, DC 20001

Chief of Staff
COMMUNICATIONS SECTOR COORDINATING COUNCIL

Deploying Resource Public Key Infrastructure (RPKI): Steps for Prioritization and Implementation

May 18, 2025 – Final Report

Table of Contents

Abstract

Nearly seven Internet routing incidents occur each day.[1] These incidents include both malicious and accidental route hijacking and can lead to data interception, service disruptions, as well as financial losses, underscoring the critical need for widescale adoption of robust routing security technologies like the Resource Public Key Infrastructure (RPKI)—a security framework designed to enhance the security of Internet routing by authenticating and verifying the use of Internet Protocol (IP) address prefixes and Autonomous System Numbers (ASNs).

Every organization (e.g., Internet Service Providers (ISPs), Cloud Service Providers (CSPs), Content Delivery Networks (CDNs), and public and private enterprises (e.g., critical infrastructure of all types, businesses, schools, etc.) that holds Internet resources, such as IPv4 (IP version 4) or IPv6 (IP version 6) addresses should take action to ensure the authorized routing of those resources and protect the important and valuable information that uses those resources. Failure to do so risks severe consequences that threaten not only the operations of their organization, but also that of their customers and end users.

- Section 1 summarizes the role of Internet routing and Border Gateway Protocol (BGP).
- Section 2 introduces the RPKI and discusses the potential benefits of its widespread use.
- Section 3 lays out a three-step process to make use of the RPKI, including the identification of Internet resources and assets, their prioritization based on the potential consequences of a BGP attack, and the application of RPKI publication to address these risks.
- Section 4 is a playbook for all network operators, providing them with step-by-step guidance for describing routing intent by publishing RPKI Route Origin Authorization (ROA) objects.
- Section 5 is a playbook geared toward enterprise networks that provides additional guidance to use in tandem with the general playbook outlined in section 4.
- Section 6 is a playbook of additional actions specific to ISPs to perform Route Origin Validation (ROV).
- Section 7 concludes the discussion.

This document was developed pursuant to the *Roadmap to Enhancing Internet Routing Security, A Report by the White House Office of the National Cyber Director* (ONCD),[2] and is intended to help organizations understand the risks posed by Internet routing incidents, the benefits of mitigating the risks of such incidents through the use of the RPKI, and steps that can be taken to prioritize these mitigation efforts where needed. The document builds on established best practices in routing security and risk management, including those developed by the National Institute of Standards and Technology (NIST), as well as the Broadband Internet Technical Advisory Group (BITAG), Mutually Agreed Norms for Routing Security (MANRS), CableLabs and other key industry-led initiatives**.**

This product is the result of robust collaboration between members of the Communications and IT Sector Coordinating Councils (for a full list of industry contributors see the Acknowledgments). It was also informed by consultative discussions with partners across the U.S. Federal government, including ONCD, NIST, the Cybersecurity and Infrastructure Security Agency (CISA), and the National Telecommunications and Information Administration (NTIA).

[1] Rosenblatt, S. (2024, December 3). 101: Why BGP hijacking just won't die. *Dark Reading*. https://www.darkreading.com/cyber-risk/101-why-bgp-hijacking-just-won-t-die

[2] This document was published in Sep. 2024 and is available at https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/09/03/fact-sheet-biden-harris-administration-releases-roadmap-to-enhance-internet-routing-security/.

1. The Role of Internet Routing

Internet routing forms the foundation of modern global communications, enabling seamless data transfer across systems. From personal email to financial transactions to critical healthcare services, efficient and reliable routing is essential to deliver data to its intended destinations. At the core of this infrastructure lies the **Border Gateway Protocol (BGP)**—a protocol designed to ensure the quick and effective transfer of routing information between networks.[3]

The basic arrangement of the Internet is a "network of networks" each of which is called an "Autonomous System," or "AS." Each AS is a separate administrative domain with its own policies and unique ASN (Autonomous System Number) which identifies it in the global system. Interconnections between ASes happen through bilateral agreements to exchange routing information and deliver packets between the networks and their other directly connected partners. The BGP routing system is said to be "global" in that a given network needs to have routing information to be able to reach all other networks and destinations, even those with which it has no direct relationship. Unfortunately, there is no mechanism inherent to BGP itself to verify routing information's integrity, authentication, authorization, and interconnection agreement compliance – all of which are necessary for secure Internet routing.

BGP first came into use in the early 1990s, prioritizing efficiency over security. At that time, the Internet consisted of fewer than 2,000 networks, belonging primarily to academic institutions and governments, operating within a cooperative environment where trust and simple verification processes sufficed to maintain cybersecurity. This design aligned well with the Internet's limited scale and collaborative nature prevalent at that time.[4]

Today's Internet is vastly more complex, encompassing over 82,900 interconnected networks,[5] each with diverse characteristics shaped by differences in scale, locality, and governing laws.[6] These networks include ISPs, Cloud Service Providers (CSPs), Content Delivery Networks (CDNs), and public and private enterprises, among others. (These will collectively be referred to as "Organizations" in this document.) The vast scale of the Internet now necessitates intricate coordination among its stakeholders to ensure the functionality and security of its routing infrastructure. This complexity and the breadth of relevant stakeholders exposes BGP to significant security challenges. Inadequate verification mechanisms can lead to incidents where malicious actors or operational errors reroute traffic to unintended destinations, potentially disrupting critical services. These potential vulnerabilities make securing BGP routing a top priority to maintain uninterrupted global connectivity.[7]

---

[3] BITAG. (2022, November 2). *Security of the Internet's Routing Infrastructure: A BROADBAND INTERNET TECHNICAL ADVISORY GROUP TECHNICAL WORKING GROUP REPORT*. Broadband Internet Technical Advisory Group. https://www.bitag.org/documents/BITAG_Routing_Security.pdf

[4] Ibid.

[5] ipapi.is. (2025, January). IP to ASN Database. Retrieved January 9, 2025, from https://ipapi.is/asn.html

[6] BITAG. (2022, November 2). *Security of the Internet's Routing Infrastructure: A BROADBAND INTERNET TECHNICAL ADVISORY GROUP TECHNICAL WORKING GROUP REPORT*. Broadband Internet Technical Advisory Group. https://www.bitag.org/documents/BITAG_Routing_Security.pdf

[7] Ibid.

Maintaining uninterrupted global connectivity requires action and vigilance by all Organizations. This is because BGP routing faces significant risks from both deliberate and accidental misconfigurations (see **Appendix B** for an overview of BGP threat types), ranging from incorrectly configured access controls and security parameters to improperly maintained route configurations settings. These vulnerabilities are actively exploited by various threat actors, including organized crime groups, malicious insiders, and nation-states. Nation-state actors have repeatedly demonstrated their intent to disrupt critical systems, steal data and intellectual property, and conduct espionage campaigns on communications networks. For instance, in 2010, Chinese state-sponsored hackers used BGP hijacking to redirect traffic from major telecommunications providers to Chinese-controlled networks, allowing them to intercept sensitive data and potentially monitor communications.[8] See **Appendix C** for additional information on threat actors and past BGP incidents.

2. Widespread Routing Validation

One of the most promising approaches to enhance BGP security is the specification and realization of the **Resource Public Key Infrastructure (RPKI).** The RPKI is a cryptographic framework that builds upon the existing delegation and authority pathways for Internet number resources (IP addresses, Autonomous System Numbers). The first use-case called ROV (Route Origin Validation) enables IP address holders to certify legitimate origin ASes for their IP address blocks, thus preventing malicious interception attempts via unauthorized ASes. This is enabled through widespread issuance of Route Origin Authorizations (ROAs) by Organizations that have IP prefixes. Network Operators can then enable ROV on their routers to verify incoming BGP route announcements against ROA records and drop those which are invalid. Note that the IP address holders may or may not be the same as the AS network operators and that ROA publication and ROV enablement for a given Organization can be decoupled; it is not necessary to do in a particular order and indeed some might do one and not the other; depending on the circumstances.

Despite its great potential, adoption of these RPKI technologies has been gradual, partly due to the complexities, and in some cases the expense involved if equipment and software upgrades are necessary, as well as the need for testing and deploying it across diverse networks and regions. As of 2024, just over 50% of IPv4 and IPv6 routes in the global routing table were covered by ROAs.[9] While this significant partial deployment accrues some benefits, more work needs to be done to approach complete RPKI adoption.[10] Stakeholders, including government agencies, must therefore work together to accelerate RPKI implementation, recognizing that improving the integrity of the Internet's routing infrastructure is critical to the security of global communications.

---

[8] Robert McMillan. (2010, April 8). A Chinese ISP momentarily hijacks the Internet (again). *Computerworld*. https://www.computerworld.com/article/1546128/a-chinese-isp-momentarily-hijacks-the-Internet-again.html

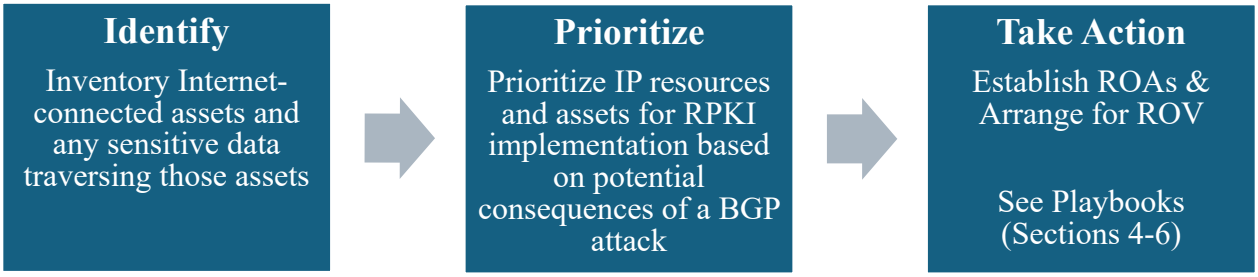
[9] Madory, D and Snijder, J. (2024, December 3). *RPKI-ROV deployment reaches major milestone*. Kentik. https://www.kentik.com/blog/rpki-rov-deployment-reaches-major-milestone/

[10] Doug Madory. (2023, August 31). *A Tale of Two BGP Leaks*. Kentik. https://www.kentik.com/blog/a-tale-of-two-bgp-leaks/

While RPKI enablement is a high priority for most major network service providers, it has been a lesser priority for other Organizations. This is likely due, in part, to the higher visibility and security priorities associated with other hazards, such as ransomware, phishing, insider threats, fraud, network misconfigurations, website attacks, Distributed Denial of Service (DDoS), smishing, and business email compromises, as well as limited financial and employee resources. For many Organizations, their focus is therefore on threats that would cause significant degradation and service disruptions affecting their customers. While these types of incidents necessitate a constant focus, the consequences of BGP incidents also pose a similar risk that must be addressed—and can be through a mature approach with a reasonable return on investment.

3. Three-Step RPKI Planning

Organizations should follow a three-step process to start working with the RPKI. First, Organizations should identify their Internet assets and the data traveling across those assets to understand what is of the greatest value and most needs protection. Next, they should prioritize ROA creation based on the potential consequences from potential loss, misrouting, or disruption of these holdings and data. Finally, Organizations should take action by using the playbooks provided in the following sections to implement and maintain RPKI assets.



Organizations should focus on the creation and ongoing management of ROAs for their IP address assets and ensure ROV is being implemented by network service providers such as ISPs, content providers, and Internet exchanges.

Step #1: Identify

The first step in implementing RPKI technologies is identifying the Internet resources and assets the Organization has that are of value or that deliver mission critical services. These assets often include first-party Domain Name System (DNS) infrastructure, web servers, email servers, cloud services, VPN (Virtual Private Network) infrastructure, and critical routing and network devices. Additionally, Organizations should identify customer and partner networks, CDNs, and public IP address spaces that may be exposed to the Internet. Identifying these assets helps to understand the full scope of an Organization's digital footprint and the potential points of vulnerability.

Organizations also need to identify the types of sensitive data that travel across these Internet assets. This includes customer data like personally identifiable information (PII), financial transaction details, and health records. Employee data, credentials, and business-critical information such as intellectual property, financial records, and operational data should also be considered. Furthermore, Organizations should recognize the flow of confidential communications, security logs, and compliance data, all of which could be at risk during a BGP incident. Identifying both the assets and the data that require protection is essential.

Step #2: Prioritize

In the second step, Organizations should prioritize the critical resources for which ROAs should be created based on the potential **consequences** that could arise from BGP incidents, such as data interception and theft, service disruption, or financial losses. By evaluating the severity of potential impacts on critical systems, customer trust, and regulatory compliance, Organizations can allocate resources effectively and prioritize the deployment of RPKI technologies where it will provide protection for high value assets and data. Ideally, Organizations can create ROAs for all their assets, but this prioritization process will help those with limited budgets or resources target their efforts more strategically. See **Appendix A** for a worksheet to help walk through the prioritization process.

Organizations should also carefully consider the **severity** of different consequences when making their decisions. To determine the severity of various consequences, Organizations must make a judgment, considering their specific needs and the potential impacts. The consequences with the most severe impact, such as those that could result in significant financial loss, operational disruption, intellectual property loss, reputational damage, or legal penalties, should be prioritized for ROA creation. Ultimately, this process allows Organizations to make risk-informed decisions that align with their unique operational and security requirements.

On the following page is a comprehensive (but non-exhaustive) list of considerations of impact and potential consequences that can occur from deliberate or non-deliberate BGP misconfigurations. These consequences span multiple dimensions, including human, economic, operational, strategic, and national critical functions,[11] that Organizations must consider in their risk-informed considerations. Consequences are categorized for ease of use, serving as a helpful guide for Organizations; however, this categorization is flexible and can be adjusted as needed.

Step #3: Take Action

The third step to deployment is to take action by referring to the playbooks in **Sections 4 – 6** of this document for detailed guidance on how to create and manage ROAs across an Organization's assets, and options to arrange for ROV filtering. It's important to note that RPKI publication requires periodic maintenance to remain effective, as the landscape of threats and routing configurations can change over time. Regular updates, monitoring, and adjustments are essential to ensure continued protection against BGP attacks and to keep an Organization's network secure.

[11] Cybersecurity and Infrastructure Security Agency CISA. (n.d.). National Critical Functions: CISA. https://www.cisa.gov/topics/risk-management/national-critical-functions

Considerations of Impact and Potential Consequences of BGP Attacks

Human

- Loss of public trust
- Customer service interruption
- Compromised employee, customer, vendor data

Economic

- Revenue loss
- Reputational damage
- Legal penalities and compliance costs
- Incident response and recovery costs
- Service level agreement compliance

Operational

- Disruption of core business functions
- Compromise of sensitive/confidential data
- Degradation of critical functions
- Loss of intellectual property

Strategic

- Loss of competitive advantage
- Damage to partnerships and customer relationships
- Privacy breaches
- Impact on decision-making

National Critical Functions

- Impact of critical infrastructure
- Risk to national security
- Risk to economic stability
- Risk to public safety and health

Consider the ***severity*** of different consequences taking into account the specific needs and vulnerabilities of your organization.

4. Overarching Playbook Guidance: Using the RPKI

This playbook offers step-by-step guidance for network operators – from ISPs to private entities, government agencies, universities, and more – to make use of the RPKI, including two major aspects: authorization using ROAs and validation using ROV. It also provides guidance on filtering and monitoring to ensure continuous robust and resilient routing infrastructure. While it is recommended that all organizations that hold Internet resources (i.e., IP address space) create ROAs, organizations should consider taking additional actions, depending on how they receive Internet and cloud-based services. This playbook is not exhaustive and a list of additional resources and references that provide more detailed information and guidance, as well as applicable standards, is included in **Appendix D**.

Routing security infrastructure involves multiple interconnected pieces. Making use of RPKI technologies within your organization's networks requires significant, detailed planning that must be undertaken by technologists in your own organization.

When setting up a production environment for business services, cloud integrations, applications, web tooling, or even email, misconfigurations during the process have the potential to impact the hosting organization, but often the risk stops at the organizational boundary. However, in the context of routing security infrastructure, misconfiguration of an AS could not only negatively impact the hosting organization, but it could also have a potentially harmful cascading effect on a large number of routes across the Internet. Misconfiguration could disable entire regions, businesses, and disrupt communications impacting safety-critical, life-critical, and potentially national defense activities. Therefore, extreme care must be taken during advertising, signing, and verification of routes.

This section is not intended as a teaching tool; it is intended to help guide practitioners in the field as to each of the critical steps that must be understood and undertaken to improve the security of Internet routing. If you are not experienced in this function, if you do not have a staging environment to test your changes, or if you do not have a way to easily roll back updates, please consider working with those who do have this expertise and tooling. Your Regional Internet Registry (RIR) can help. The RIR for North America is the American Registry for Internet Numbers (ARIN) (www.arin.net). Other regions have their own RIR, including the Latin American and Caribbean Internet Addresses Registry (LACNIC), Réseaux IP Européens Network Coordination Centre (RIPE NCC), African Network Coordination Centre (AFRINIC), and the Asia-Pacific Network Coordination Centre (APNIC). In some cases, though not typical, an operator in North America can use IP addresses by other RIRs.

4.1 Preparation

After identifying your assets and the relevant staff in your organization with the authorization and capability to access and make changes to network configurations (as described in Section 3 above), the following must be in place before IP address holders can issue RPKI ROAs:

- IPv4 or IPv6 number resources directly allocated to your organization by the RIR.

- If your organization has resources assigned by precursors to the current RIRs or prior to the establishment of ARIN circa 1997, your organization will need an executed ("Legacy") Registration Services Agreement covering those IPv4/IPv6 resources.

- A user account (in ARIN, for the U.S.) linked to your organization as the Admin, Tech, or Routing Point of Contact to use the ARIN Online member portal.

- The ASN that is currently (or, in the case of pending changes, may soon be) originating BGP announcements covering your IP address space. Note that some DDoS mitigation products may require that ROAs be pre-provisioned to allow for a (sub-)prefix origination from a different AS to enable their "scrubbing" service. Consult with the particular provider in cases where you have contracted for such.

Next, you must determine which RPKI model is appropriate for your organization:

Hosted RPKI

In this model, the RIR (e.g., ARIN) runs the Certificate Authority (CA), the publication server, and the repository. This model is suggested for all organizations, but recommended in particular for organiztion that do not have expert technical staff able to devote significant amounts of time to monitoring and maintaining the RPKI.

Delegated RPKI

In this model, the ISP runs everything, including the CA, the publication server, and the repository. This model is suggested for organizations that want to retain cryptographic control of RPKI certificates and that have a deeper understanding of the RPKI and routing security, along with technical staff capable of running and maintaining the high-availability Internet-facing publication server with sufficient computational and network capacity to keep pace with growing demand.

Hybrid RPKI

In this model, the ISP runs the CA, but the RIR runs the publication server and the repository. This is an option for organizations that want cryptographic control but do not want to maintain the high availability repository and publication requirements.

If you are new to RPKI publication, it is recommended to select the "Hosted" model, as it is the most straightforward to use.

4.2 Generating ROAs

4.2.1 ROA Coverage

Since ROAs follow the chain of authority descending from the 5 RIRs (and implicitly from IANA (the Internet Assigned Numbers Authority)), a ROA can *only* be issued by the rightful holder of the block of addresses in question. Keep in mind that the goal is that BGP announcements match at least one ROA as described in RFC6811 Sec. 2. Note that a Validated

ROA Payload (VRP) is the information contained in the ROA, absent the signature and other information used in the process of validating the legitimacy of the ROA itself:

Covered

A Route Prefix is said to be Covered by a VRP when the VRP prefix length is less than or equal to the Route prefix length, and the VRP prefix address and the Route prefix address are identical for all bits specified by the VRP prefix length.*

Matched

A Route Prefix is said to be Matched by a VRP when the Route Prefix is Covered by that VRP, the Route prefix length is less than or equal to the VRP maximum length, and the Route Origin ASN is equal to the VRP ASN.

**That is, the Route prefix is either identical to the VRP prefix or more specific than the VRP prefix.*

Network operators should establish ROAs for their existing BGP announcements indicating the correct origin AS, but also for alternative origin AS values in certain instances. The most common instances where creating ROAs in advance might be useful include provisioning or change activities and where a DDoS mitigation service may episodically originate BGP announcements for some portion of the address space in question. Furthermore, ROAs should also be generated for any prefixes that are not yet advertised to prevent prefix squatting.

4.2.2 Maximum-Length Field

The optional field in the ROA called maxLength can be used to reduce the number of ROAs that need to be created. This is typically set to the longest prefix length you expect to advertise. For instance, if you're assigned a /20 but only advertise /24s, you might set the max length to /24. RFC9319 generally recommends against using the Maximum-Length field at all (which is functionally equivalent to setting it to the same value as the prefix length in the ROA). The Forged-Origin Sub-Prefix Hijack section in that RFC describes some risks associated with this practice.

4.2.3 ROA Generation with Hosted Model

If a hosted RPKI model is chosen, ROAs can be generated from within the RIR's portal (e.g., ARIN portal) using your organization's ARIN account.

4.2.4 Internet Routing Registry (IRR) Data Publication Aligned with ROA Publication

IRR route objects should be kept accurate and synchronized with your RPKI ROAs to avoid confusion and ensure consistent route filtering by third parties. Note that ARIN's IRR Auto-Manager provides an automated function to realize this practice using ARIN's hosted RPKI and IRR. Also, some operators who rely on the IRR will prefer IRR repositories which only allow updates from authorized address holders, and some will not accept entries that are contrary to published ROA data.

4.2.5 Change Management Integration

Since it is critical that published ROA information match intended BGP announcements exactly, it is likewise imperative that processes related to this information (e.g., additions, deletions) be appropriately integrated with change procedures related to the organization's BGP configurations.

Note: If a BGP announcement becomes dropped through a mismatched ROA, the quickest path to resolution is to issue a new ROA that matches the intended announcement rather than deleting the problematic ROA. As long as there is one ROA that matches the prefix, length, and origin AS, the BGP route will be considered "Valid."

4.3 Maintaining, Optimizing, Securing

Maintaining RPKI Information

RPKI maintenance needs to be part of your normal operational processes for provisioning. Customer additions may require new ROAs and filter updates. Departing customers may require ROA and filter deletions. It is strongly recommended that these processes be automated as part of the ISP's Operational Support System. The results of these changes should be periodically reviewed, to ensure that processes are operating correctly.

Optimizing ROA Data

Since one ROA may map multiple prefixes to a given Origin AS, by packing in this way, the overall load of ROA processing, storage, and data transfer is lessened. In the RIPE Hosted RPKI implementation, this optimization is carried out automatically. In the ARIN implementation, to this date, such automation is not in place. However, it is possible to execute an atomic API transaction which deletes and then (re-)issues ROA information to serve this objective.

RPKI Security

The key principles of information security have often been described using the "CIA triad" which is composed of the following:

- Confidentiality: Ensure the information is accessible only to authorized parties. Encryption regimes and access control are typical means to meet this objective.

  The RPKI makes extensive use of digital signatures deriving from its roots in X.509. Aside from the private key material, which is used in this signature process, the data used in the RPKI is, by definition, public. Hence, confidentiality, other than that of private key material, is moot for the RPKI.

- Integrity: Ensure the information cannot be tampered with and/or that such tampering is evident. Cryptographic signatures can be deployed to achieve such.

  The RPKI is designed to have "object" integrity meaning that the data itself is verifiable regardless of which server(s) it was transmitted from.

- Availability: Ensure that the information is and remains available to legitimate users. Besides resiliency of the infrastructure, countermeasures to DoS (Denial of Service) attacks can aid in this cause.

    RPKI availability has several facets. All publication points must remain available at all times and with up-to-date information. In cases where the "Delegated" or "Hybrid" model is used, care must be taken to ensure timely publishing and availability as well as sufficient capacity of both the server(s) and the network(s) involved. Detailed advice in these areas is beyond the scope of this document. Please see the list of technical resources at the end of this document (**Appendix D**).

4.4 Monitoring

There are several reasons to monitor both BGP announcements and RPKI information. First, monitoring BGP announcements allows the ground truth of prefix ownership to be established, which is the first step to the successful deployment of ROAs. Second, such monitoring can also identify discrepancies between published ROAs and announced prefixes, facilitating the correction of potential human errors and misconfiguration. ISPs should monitor ROV in addition to ROAs, which may allow for the discovery of other issues that may go otherwise undetected.

Monitoring involves both internal and external views. Internal monitoring includes checking internal routing tables for impacts from dropping invalids by ROV. In external monitoring, BGP-related resources are monitored from outside the AS. More specifically, BGP announcements can be monitored from public route collecting systems, and ROAs can be monitored from public validators.[12,13,14]

4.5 Governance and Risk Management

The following are best practices and community recommendations to aid in governance and risk management:

- **Integrate Routing Security into Your Organization's Overall Risk Management Strategy:** Establish a strategy focused on enhancing routing security and communicate your organization's expectations, risk tolerances, accountability measures, resources, and routing security policies to internal and external stakeholders.

- **Adapt to an Evolving Threat Landscape:** Cybersecurity is not static – keep up to date on relevant best practices, technological advances, and community recommendations to address emerging threat vectors and routing security risks.

- **Maintain Proper Contacts:** Ensure that contacts for RIR interaction are kept up to date. Not only should RPKI changes be limited to properly trained and authorized employees but verify that your organization's administrative and billing contacts are up to date and

[12] https://bgp.he.net/
[13] https://stat.ripe.net/app/launchpad/
[14] https://rpki-validator.ripe.net/ui/

your registration and associated financial obligations are kept current, including through staffing changes.

- **Document Your Policies:** Publish your RPKI adoption status and route filtering policies to maintain transparency, ensuring your peers know how you handle invalid routes.

4.6 Subsequent Actions

If you are an enterprise network operator that obtains your Internet connectivity from one or more ISPs, continue to Section 5 for additional actions to take.

If you are an ISP, jump to Section 6 for additional actions to take to enable filtering services (i.e., ROV).

5. Enterprise Network Playbook: Specific Actions to Use the RPKI

This supplemental playbook only applies to enterprise networks, and outlines actions that should be taken in addition to those listed in Section 4. For purposes of this section, an "enterprise" network is most typically one which serves a single public or private sector organization. Examples may include private companies, universities, government entities, critical infrastructure entities, non-profit organizations, etc. Such networks generally obtain Internet connectivity from one or more ISPs and may also make use of cloud-based services for hosting of applications, virtual machines, or other software-based functions. All of these capabilities can benefit from the use of various routing security measures, including the use of the RPKI.

The intended audience for this section is the managers and technicians who are responsible for the planning and operation of the IT infrastructure and services used by the organization. This section is primarily applicable to organizations that are either receiving specific routing information from their ISP(s) via BGP and/or are advertising prefixes into BGP, perhaps with the aid of their ISPs. For organizations that point a static default route to their ISP and use address space that is part of their ISP's allocation and advertisement, this section can provide some background information, but generally those networks do not need to take specific action with regard to the RPKI.

5.1 Background on IP Address Resource Assignments

IP address space comes in two varieties, IPv4 and IPv6. In most ways they are similar if not the same, but this distinction can be important in some cases. IPv4 was, as the designation suggests, developed earlier and is in the most widespread use. Also, because it was developed and used first, the practices for assigning it may differ somewhat. Some of these differences also stem from the fact that the size (number) of possible addresses is much, much less and is significantly smaller than the human population of planet Earth. For this reason, the IPv4 space is considered a scarce and precious resource and techniques such as NAT (Network Address Translation) and private addressing (e.g., RFC1918, RFC6598) are in widespread use to enable sharing of a single IP address by many users. Hence, the IP address assigned to a given user/device may not be the one that is relevant in the context of the global routing table. Instead, it is the "public"-facing IP address that is relevant for this discussion.

For most networks, IP addresses will typically be assigned as part of a larger block of addresses which are assigned by an RIR or some intermediate LIR (Local Internet Registry). Examples of LIRs include country-level registries such as exist in China, India, Brazil, and possibly other places, but LIRs may also refer to the IP-address-assignment capability of an ISP toward its customers, or to an IP leasing company.

In cases where the organization is using IP address resources provided by their connectivity or cloud providers, the organization should inquire with those providers as to their use of RPKI technologies and general routing security posture.

In cases where the organization is using IP address resources obtained directly from an RIR such as ARIN in North America, the organization can straightforwardly make use of the RPKI to publish ROA objects to match their routing intent.

If the IP addresses in use by an organization are obtained from an IP broker or leasing organization, the recommendation would be to ensure ROAs can and will be put in place to reflect the routing intent.

5.2 Autonomous System Number and Running BGP

If an enterprise is using its own IP address assignment, it is generally advisable to also run BGP to originate routes from the customer's own unique ASN. Doing so gives the following advantages:

- Network sovereignty: If you decide you want to switch providers permanently, there is less work to do.
- Upgrade flexibility: You have laid the groundwork for being multihomed in the future should the business case present itself.
- DR (Disaster Recovery) capabilities: You will have ROAs in place for announcing the netblock(s) from an AS that you control, should you want to do temporary DR with another entity who can support a BGP customer.

Obtaining a single ASN as an existing ARIN customer, bears no extra cost.[15] Acquiring an ASN from ARIN by itself costs well under $500/year (as of this writing).

5.3 IP Address Leasing

In the case where Enterprises work with IP address leasing companies to obtain use of IP address space without permanent transfer, the Enterprises should ensure that the leasing company can and will provide timely ROA publication to reflect the desired routing intent.

5.4 Working with ISPs and CSPs for ROV Filtering

Enterprises are recommended to indicate their requirement that the ISPs, CSPs, and other IT service providers perform ROV filtering. Adding such requirements to their RFI/RFP (Request for Information/Proposal) processes is suggested.

5.5 Current Best Practices

While it should be apparent that keeping BGP announcements and published ROAs aligned, some clarification may be helpful:

- Multiple ROA/VRPs may exist for the same or overlapping prefixes and more than one origin AS. A primary use for this practice includes transitions or migrations from one origin AS to another where continuity of reachability can be facilitated by the "new"

[15] https://www.arin.net/participate/policy/nrpm/#5-as-numbers

mapping coexisting with the “old” one. Another case where multiple possible origins may be reflected in the RPKI is where a “scrubbing” or “mitigation” service to address DDoS (Distributed Denial of Service) attacks may need to be activated in short order.

- A common traffic engineering practice may involve originating more specific routes for a given IP prefix. Depending on the particulars of this use, it may or may not be necessary to issue matching ROA mappings. For instance, the more-specific routes may be intended to only propagate to one or more direct neighbor networks in which case the details of the agreements between those networks would be appropriate to take into account.

- Some care should be taken to ensure that published ROA information stays reasonably aligned with current or possible routing intent. If a use-case described above no longer applies, the relevant ROA data should be updated or removed.

Enterprises should consult their various network services providers including cloud, connectivity (via an ISP), hosting, software, DDoS mitigation, etc. to understand how each makes use of the RPKI.

6. Internet Service Provider (ISP) Playbook: Specific Actions to Use the RPKI

This section outlines additional relevant actions to be taken by ISPs, which play an integral role in the filtering of invalid routes.

6.1 Implementing ROV

Implementing ROV is recommended on all external BGP (eBGP) sessions, particularly where those sessions are with networks that connect to and carry BGP updates from further downstream networks.

6.1.1 Investigate ROV Support

Ensure support for ROV on routing platforms where inter-provider BGP sessions are terminated. A non-exhaustive reference for router support of ROV is available (RPKI Router Support), but operators should check with their own vendors and ask said vendors to keep them abreast of any software bugs related to the ROV feature set.

6.1.2 Set Up and Operate a Relying Party (RP) System

Deploy RP software running on a server or, preferably, multiple servers. If multiple servers are deployed, they may run different RP software packages and may be placed in different geographic locations to achieve software diversity and location redundancy. Independent implementations of RP software are available. The RP system needs to implement two functions, which can be in the same package/server or separate ones:

- Collect and validate ROAs to produce a list of validated ROA payloads.
- Feed the results to routers using the RPKI to Router (RTR) Protocol.

6.1.3 Configure Routers to Ingest Verified ROA Payload (VRP) Data

The routers performing ROV need the information from the RP software. If using, for instance, two different RP codebases running in two different geographically diverse data centers, it may be possible and advisable to configure each router performing ROV to intake data from all four instances. The router generally considers the union of all received VRP information in validating incoming BGP information.

6.1.4 Design Modified Routing Policies to Properly Include a "Drop-Invalid" Posture

Consider, for instance, how the "drop-invalid" logic might interact with features such as RTBH (Remotely Triggered Black-Hole) as these routes are by definition more specific and will likely not match published RPKI information. To ensure that a customer can only trigger black-hole drop behavior for prefixes within their domain, incoming BGP updates must first match a route filter containing the customer's prefixes. Only then is the update examined for the BGP community value which is used to trigger the black-hole behavior. This evaluation should occur before checking the RPKI status. Some background on RTBH can be seen here.

6.1.5 Perform Staged ROV Enablement

Since validation can be configured on a per-neighbor basis, it is possible and advisable to enable it on a neighbor-by-neighbor, router-by-router, or partner-by-partner basis. Through a gradual, staged deployment, it is possible to observe the outcome and roll-back if necessary while gaining confidence with the featureset.

6.1.6 Do Not Use ROV on Internal BGP (iBGP) Sessions

Performing ROV on iBGP sessions is almost never advised as it is normal to carry many more-specific routes internally which aren't seen beyond the local operator's perimeter.

6.2 Filtering

Route filtering on eBGP sessions is a long-standing and recommended practice that should be maintained in conjunction with ROV enablement. Not only does it provide types of protection that ROV does not, but it can also provide a backstop to prevent unintentional route propagation should ROV fail in some way. ROV itself does not replace route filtering. Instead, it provides complementary protection. There are two main aspects of route filtering:

- **Prefix Filters:** This type of filtering uses a defined list of filters to compare against incoming BGP updates. It is typical to deny "private use" IP address space as defined in RFC1918 so that routes for addresses in these blocks do not leak beyond the borders of a network operator's domain of control. Such filters should be applied to both inbound and outbound BGP updates. Additionally, on "customer" eBGP sessions it is necessary to explicitly match a list of feasible prefixes that might be advertised by that neighbor. Traditionally, the contents of the filter list have come by self-reporting during the customer provisioning process or by automated means using data published in the IRR.

- **AS-Path Filters:** As the name suggests, the logic of such a filter uses data in the AS-path portion of the BGP update instead of the prefix. These filters can and should be used to limit the propagation of a particular type of "route leak" in which a given AS becomes transit for AS(es) which are not intended. For instance, ensuring any non-transit a/k/a "peer" partner AS cannot become transit for any other non-transit partner is one use case. It is common ISP practice to use these in some conjunction with prefix-filters.

The exact scope of configuring route filters is beyond the scope of this document.
For further information, please consult a MANRS route filtering tutorial and also vendor-specific documentation for the relevant equipment.

6.3 Interconnection (Peering)

Interconnection agreements usually include details about the prefixes to be exchanged between ISPs, as well as communication about operational practices on both sides. ISPs implementing ROV are advised to communicate with their peers well in advance of actual deployment to ensure that there are no surprises. Unexpected service interruptions due to errors in ROV deployment are in no one's best interests.

6.4 Other Considerations

Operators who use freely available open-source software may consider obtaining a support contract with the software maintainers or otherwise materially or financially contributing to the upkeep of the software to mitigate the well-known risks associated with open-source software.[16] Accountable, committed maintainers are critical for continuity and for patching security vulnerabilities and bugs, refactoring and reoptimization and implementing new features. This level of support matches the operator's expectation of other suppliers of critical network infrastructure components such as routers, switches, and servers.

[16] https://www.cisa.gov/sites/default/files/2023-10/Fact_Sheet_Improving_OSS_in_OT_ICS_508c.pdf CISA, Improving Security of Open Source Software in Operational Technology and Industrial Control Systems.

7. Conclusion

Organizations must prioritize the use of RPKI technologies to effectively mitigate risks from misconfigurations and malicious rerouting and ensure the continued reliability and security of the Internet's routing infrastructure.

Securing Internet routing requires taking a multi-layered approach to RPKI implementation. By following the playbooks provided in this document, Organizations will be able to:

- Publish ROAs to indicate routing intent.
- Enable ROV to help mitigate the spread of mis-originated BGP routes.
- Implement BGP filtering strategies that provide complementary protection.
- Improve the level of assurance of BGP routing by developing structured incident response plans to mitigate risks.
- Continuously improve security controls to address evolving threats.

By adopting a proactive, collaborative, and standards-driven approach, Organizations can significantly enhance Internet routing security and resilience, safeguarding critical data and services from potential threats.

Appendix

Appendix A: RPKI Prioritization Worksheet

For each identified asset, fill out the following chart. Repeat the process for each asset. Assess the severity of consequences that could result from a BGP incident on a 1 (very low) to 5 (very high) scale.

Asset	Consequences	Severity
Critical Network/ IP Addresses: _____	Loss of public trust	
	Customer service disruption	
	Revenue loss	
	Compromised employee, customer, vendor data	
	Degradation of critical functions	
	Other:	
	Other:	
	Other:	
		Average:

After calculating the average severity for each of your identified assets, rank them to prioritize RPKI deployment.

RPKI Deployment Prioritization	
Asset Name	**Average Severity Score**

High Priority

Low Priority

Now that you have prioritized deployment, use the playbooks to take action by identifying how to make use of RPKI technologies in order of highest average severity score to lowest average severity score.

Appendix B: BGP Threat Types

Widespread adoption of RPKI technologies, which include ROA registration of IP addresses combined with arranging for ROV, helps enterprises defend against the following threat and risk scenarios:

BGP Misconfiguration/Hijacking

Route Misorigination/Hijack: Route misorigination occurs when a network advertises an IP prefix without authorization and contrary to the intentions of the address holder, leading to traffic misdirection and potential security breaches. This can be caused by accidental configuration errors or malicious intent, and its effects can range from data interception to service disruption. Misorigination often impacts the integrity of routing systems, reducing trust among network operators. The term “Route Hijack” has been used, sometimes interchangeably, though it presumes some proof or indication of intent and consequence such as traffic interception, eavesdropping, and blackholing.

More-Specific Prefix Attacks: Internet routes typically follow the shortest route between two ASes absent a routing agreement to the contrary. As a result, attackers can exploit this method by advertising more-specific IP prefixes than those intended by the legitimate owner, thereby exploiting the "longest prefix match" rule to redirect traffic to their own network. Attackers can use this method to intercept data, disrupt services, or conduct man-in-the-middle (MitM) attacks. More-specific prefix advertisements are often difficult to detect quickly, as they appear legitimate in routing announcements.

Path Manipulation Attacks: Path manipulation occurs when attackers alter the AS path in BGP updates, influencing the direction and flow of network traffic. By changing the routing paths, attackers can introduce increased latency, instability, or direct traffic through malicious intermediaries. This manipulation poses risks such as traffic interception, data tampering, and service disruptions.

Route Leaks

Route Leaks: Route leaks happen when route announcements propagate beyond their intended scope, potentially violating routing policies and agreements between networks. This may occur due to configuration errors but can also be exploited for malicious purposes to reroute traffic through insecure or less reputable networks. The effects of route leaks include increased latency, potential traffic monitoring, and degradation of network stability.

Interception and Eavesdropping

Using BGP to Subvert Transport Layer Security (TLS): By manipulating BGP to reroute traffic, attackers can subvert TLS-encrypted communications (notably HTTPS web traffic), potentially downgrading or intercepting encrypted traffic. This threat undermines the security guarantees of TLS, exposing sensitive data to interception and compromise. Subversion can involve MitM attacks, where encrypted data is redirected to malicious servers before reaching its intended destination.

Nearer Origin Attacks: In this attack type, the attacker manipulates routing paths to make their AS appear closer to the target network, influencing routing decisions to favor malicious paths. This can result in traffic being redirected to locations that facilitate interception, tampering, or prolonged latency. Nearer origin attacks can lead to widespread service degradation or data compromise, depending on the attacker's goals.

Relationship to Higher-Level Attacks: Routing threats can act as enablers or gateways to more sophisticated attacks, such as DDoS, MitM attacks, and data breaches. Compromised routing security provides attackers with leverage over broader network operations, undermining the integrity, availability, and confidentiality of data flows. Successful routing exploits often become the first step in complex, multi-stage cyber-attacks.

Additional BGP Exploitation

IP Squatting: Malicious actors exploit unallocated or dormant IP address blocks to carry out illicit activities, such as sending spam, launching attacks, or disguising malicious traffic origins. By using unassigned or under-monitored IP addresses, attackers can evade detection and blacklist measures, complicating defense efforts. IP squatting undermines trust in IP routing systems and can lead to significant security concerns. In 2014, cybercriminals utilized unallocated IP addresses to conduct large-scale spam campaigns and malicious activities, highlighting the vulnerabilities associated with dormant IP blocks.

For more information on BGP threat types see the BITAG Security of the Internet's Routing Infrastructure Report.[17]

[17] BITAG. (2022, November 2). *Security of the Internet's Routing Infrastructure: A BROADBAND INTERNET TECHNICAL ADVISORY GROUP TECHNICAL WORKING GROUP REPORT*. Broadband Internet Technical Advisory Group. https://www.bitag.org/documents/BITAG_Routing_Security.pdf

Appendix C: Threat Actors and Historical Incidents

Listed below are the most significant threat actors with examples of previous BGP attacks they carried out. Note, however, these groups are expansive and additional actors emerge frequently.

Nation-State Actors

Nation-states have been both directly and indirectly responsible for some of the most infamous route leaks and hijacks. These threat actors are highly sophisticated and well resourced. Some nation-states are known for operating through criminal organizations by contracting their services to reach government objectives.

Nation-State Route Leaks

Russian Federation – Rostelecom – 2022: Russia ordered blocks on social media during the invasion of Ukraine in 2022. To carry out this order, Rostelecom used a BGP hijack to black hole Russian IP traffic going to Twitter (now X); however, Rostelecom unintentionally caused propagation of the intentionally hijacked routes, resulting in outages of Twitter outside of Russia.[18]

Union of Myanmar – MPT – 2021: The Myanmar Ministry of Transport and Communications issued a notification to mobile networks and Internet service providers (ISPs) in the country to block Twitter. Local telecom operator Myanmar Posts and Telecommunications (MPT) blocked access to Twitter (now X) within the country through a route hijack, while unintentionally propagating the hijacked route beyond Myanmar, blocking Twitter access in other countries as well.[19]

People's Republic of China – China Telecom Leak – 2010: A small Chinese ISP transmitted misconfigured routing data for over 30,000 networks instead of the ISP's typical 30 routes. The routes were accepted by China's state-owned China Telecommunications, which shared the data with other major ISPs. Although the incident only lasted for approximately 20 minutes, affected networks included major multinational corporations in the U.S., China, Australia and France.[20] It is unclear whether the purpose was to redirect data to malicious computers in China.

Nation-State Route Hijacks

Islamic Republic of Iran – Iranian Government – 2019, 2022: The Iranian government forced a total Internet disconnection which was visible in BGP routing measurements in 2019 during days

---

[18] Goodin, D. (2022, March 29). *Some Twitter traffic briefly funneled through Russian ISP, thanks to BGP mishap*. Ars Technica. https://arstechnica.com/information-technology/2022/03/absence-of-malice-russian-isps-hijacking-of-twitter-ips-appears-to-be-a-goof/

[19] Doug Madory. (2023, September 5). *A Brief History of the Internet's Biggest BGP Incidents*. https://nanog.org/stories/articles/a-brief-history-of-the-Internets-biggest-bgp-incidents/

[20] Robert McMillan. (2010, April 8). A Chinese ISP momentarily hijacks the Internet (again). *Computerworld*. https://www.computerworld.com/article/1546128/a-chinese-isp-momentarily-hijacks-the-Internet-again.html

of demonstrations over gas prices.[21] Iran also restricted mobile Internet use in response to protests against the president to avoid international support.[22]

Republic of Italy – Special Operations Group of the Italian National Military Police and Hacking Team – 2013: Under the direction of Italian spyware provider Hacking Team and Special Operations Group of the Italian National Military Police, an Italian web host announced 256 IP addresses owned by another entity into the BGP routing system. The hijack of the IP addresses lasted six days during which time the Special Operations Group monitored the computers of unidentified targets.[23]

Government of Pakistan – PTCL Pakistan – 2008: State Telecom of Pakistan (PTCL)/YouTube BGP hijack: The Pakistani government ordered ISPs to block access to YouTube due to a video the government deemed anti-Islamic. PTCL responded by announcing more-specific BGP routes for YouTube in order to redirect traffic from YouTube to PTCL. The upstream providers accepted the new routes announced by PTCL and passed them along, resulting not only in blocking access to YouTube in many parts of the world but also overwhelming PTCL due to the significant volume of traffic being redirected to their network block.[24]

Nation-State ISP Misconfigurations

Federation of Malaysia – Telekom Malaysia Leak – 2015: Telekom Malaysia announced nearly 180,000 prefixes to Level 3, a U.S. telecommunications provider, which were then propagated to their peers and customers. This resulted in traffic being redirected to Telekom Malaysia for approximately 2 hours, overwhelming Telekom Malaysia with traffic, creating significant packet loss and slower Internet speed throughout the world due to the longer route many IP packets traveled.[25]

Republic of Türkiye – State owned Turk Telekom Leak – 2004: AS9121 announced over 100,000 bad prefixes to peers including AS6762 (Telecom Italia). AS6762 in turn propagated the prefixes to their peers while the "bad" paths originated by AS9121 replaced those originated by the real prefix owners.[26] This resulted in hijacked routes for several large, multinational organizations.

---

[21] Laurent Gil. (2019, November 19). *Historic Internet Blackout in Iran*. Oracle Cloud Security. https://blogs.oracle.com/cloudsecurity/post/historic-Internet-blackout-in-iran

[22] Dan De Luce. (2022, October 1). *Internet activists scramble to help Iranians evade digital crackdown*. NBC News. https://www.nbcnews.com/news/world/Internet-freedom-activists-scramble-help-iranians-evade-tehrans-digita-rcna50232

[23] Doug Madory. (2023, September 5). *A Brief History of the Internet's Biggest BGP Incidents*. https://nanog.org/stories/articles/a-brief-history-of-the-Internets-biggest-bgp-incidents/

[24] Ibid.

[25] Birruntha, S. (2023, July 12). *Telekom Malaysia confirms customer data breach*. NST Online. https://www.nst.com.my/business/2023/07/930316/telekom-malaysia-confirms-customer-data-breach

[26] Alin C. Popescu, Todd Underwood, and Brian J. Premore. (2005, May 15). *The Anatomy of a Leak: AS9121 or How We Learned to Start Worrying and Hate the Maximum Prefix Limits*. https://archive.nanog.org/meetings/nanog34/presentations/underwood.pdf

Criminal Organizations

Criminal organizations targeting cryptocurrency wallets and exchanges have employed BGP hijacks to reroute traffic or forge BGP announcements in conjunction with other security exploits to misdeliver or redirect traffic to malicious websites, allowing them to steal credentials and send funds to imposter accounts.[27]

Unidentified sophisticated threat actors have attacked cryptocurrency exchanges manipulating multiple layers of system security implemented according to best practices, then leveraging a BGP hijack to deliver a malicious version of code or redirect cryptocurrency funds to an attacker-controlled account.[28]

A threat actor named "Snow" breached Orange Spain's Regional Internet Registry of Europe (RIPE) account, reset the credentials, modified the ASN, and invalidated Orange's RPKI configuration. The threat actor found the RIPE credentials for an Orange employee in a "public leak of stolen data." The account was not using multifactor authentication.[29]

Unknown attackers initiated BGP hijacks 38 times over the course of two months using a man-in-the-middle attack, possibly from Belarus and Iceland, although the exact location is uncertain due to attackers' use of proxy locations. These attackers hijacked traffic from a large bank, the U.S. Government, foreign ministries, and a large U.S. ISP, among others.[30]

Hacktivists

Hacktivist organizations, driven by political ideologies, have demonstrated a range of tactics that could include exploiting BGP vulnerabilities. Some of these organizations include:

Anonymous, a decentralized collective, is well-known for targeting organizations it deems unethical. Historically, the group has used Distributed Denial of Service (DDoS) attacks to overwhelm and disrupt the operations of its opponents. While their primary focus has been on digital activism and disruption, their decentralized structure and ideological motives make them potential adopters of advanced techniques like BGP exploitation.[31]

SiegedSec, a hacktivist organization associated with left-wing political goals, has executed attacks against high-profile entities, including the Heritage Foundation, NATO, and Idaho National Laboratories. Their ability to breach such influential organizations underscores a

---

[27] Doug Madory. (2023, September 5). *A Brief History of the Internet's Biggest BGP Incidents*. https://nanog.org/stories/articles/a-brief-history-of-the-Internets-biggest-bgp-incidents/

[28] BITAG. (2022, November 2). *Security of the Internet's Routing Infrastructure: A BROADBAND INTERNET TECHNICAL ADVISORY GROUP TECHNICAL WORKING GROUP REPORT*. Broadband Internet Technical Advisory Group. https://www.bitag.org/documents/BITAG_Routing_Security.pdf

[29] Lawrence Abrams. (2024, January 3). *Hacker hijacks Orange Spain RIPE account to cause BGP havoc*. BleepingComputer. https://www.bleepingcomputer.com/news/security/hacker-hijacks-orange-spain-ripe-account-to-cause-bgp-havoc/

[30] Zetter, K. (2013, December 5). Someone's Been Siphoning Data Through a Huge Security Hole in the Internet. *Wired*. https://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/

[31] Jr, T. H. (2022, March 25). *What is Anonymous? How the infamous 'hacktivist' group went from 4chan trolling to launching cyberattacks on Russia*. CNBC. https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html

willingness to target politically symbolic and strategically significant institutions. The sophistication of their attacks suggests a capability that could extend to exploiting systemic vulnerabilities like BGP to achieve their political objectives.[32]

WikiLeaks, an anti-war and anti-military hacktivist organization, has been at the forefront of exposing classified information to further transparency and accountability. Notable actions include publishing classified U.S. government documents and releasing private emails from the Clinton campaign in 2016. By leveraging stolen data to shape public discourse, WikiLeaks has shown its capacity to influence political narratives. The organization's history of accessing secure systems points to the potential for employing BGP vulnerabilities as a means of expanding its impact.[33]

Additional Threat Actors and Vectors

Insiders represent a significant and often overlooked category of threat actors. These individuals, who are either employees or contracted workers within an organization, typically act with the intent to undermine company objectives. Their motivations may vary widely—from seeking recognition for leaking sensitive information to retaliatory actions driven by personal grievances or dissatisfaction with corporate decisions. Insiders may also collaborate with external entities such as rival corporations, nation-states, hacktivist groups, or other entities to further their goals.

A compelling example of insider threats in action can be seen in a series of attacks targeting cryptocurrency miners in 2014. These incidents, which leveraged false BGP announcements, were analyzed by SecureWorks and attributed to an attacker associated with an ISP in Canada.[34] The investigation suggested several possibilities for the attacker's identity, including:

- A rogue employee of the ISP,
- A former ISP employee with access due to unchanged router credentials, or
- A malicious external hacker.[35]

Route Origin Validation (ROV) Misconfiguration in BGP poses significant risks to the stability and security of Internet routing. ROV ensures that only authorized ASes can announce specific IP address prefixes; however, a lack of proper training and fundamental routing knowledge in staff can lead to errors, such as incorrect prefix lengths, wrong AS numbers, or neglecting to protect critical prefixes. These mistakes can cause valid routes to be flagged as invalid, resulting in dropped or rerouted traffic, downtime, and financial losses. Furthermore, attackers can exploit these misconfigurations to hijack or spoof IP prefixes, compromising the integrity of the BGP.

---

[32] Threat Actor Profile: SiegedSec. (2023, October 18). *SOCRadar® Cyber Intelligence Inc.* https://socradar.io/threat-actor-profile-siegedsec/
[33] BBC. (2024, February 19). *Who is Wikileaks' Julian Assange and what did he do?* https://www.bbc.com/news/world-us-canada-68282613
[34] Joe Stewart. (2014, August 7). *BGP Hijacking for Cryptocurrency Profit*. Secureworks. https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit
[35] Ibid.

Network Misconfiguration occurs when an AS inadvertently originates or announces routes to IP address blocks that it does not legitimately control. This mis-origination solicits traffic intended for those IP addresses, resulting in traffic misdirection. For example, incidents like the Turk Telekom leak exemplify the disruptive consequences of such errors.[36]

Operator Mismanagement involves mistakes or improper practices by Certificate Authority or Publication Point operators, leading to disruptions in Relying Party (RP) systems. These vulnerabilities have caused instability but are often mitigated by best practices and updates such as the 2024 FORT validator patches addressing CVE-2024-48943.[37] Operator oversight or negligence can exacerbate the risks posed by BGP-related misconfigurations and vulnerabilities.

Software Vulnerabilities in routing equipment can lead to significant incidents, such as the AS7007 event. In this case, a software bug caused a router to erroneously announce a large portion of global routing table IP address ranges as originating from AS7007. This overwhelming influx of traffic overloaded networking infrastructure, leading to widespread data loss and dropped traffic. Such vulnerabilities highlight the critical role of robust software in maintaining BGP stability.[38]

Rogue Networks can also engage in BGP exploitation. Spammers, for instance, exploit ranges of IP addresses that have not been recently routed. By announcing these addresses via BGP, they can use them to send spam, evading detection through this deceptive tactic.[39]

Addressing these risks requires robust tools, frequent audits, and automated validation tools, but also a well-trained team with a solid understanding of routing principles and how RPKI technologies work. Training and experience are essential for correctly interpreting ROA specifications, diagnosing issues, and implementing secure routing practices to maintain a resilient and secure network.

---

[36] Doug Madory. (2023, September 5). *A Brief History of the Internet's Biggest BGP Incidents*. https://nanog.org/stories/articles/a-brief-history-of-the-Internets-biggest-bgp-incidents/

[37] Jacobsen, O., Schulmann, H., Vogel, N., & Waidner, M. (2024). Poster: From Fort to Foe: The Threat of RCE in RPKI. Proceedings of the 2024 on ACM SIGSAC *Conference on Computer and Communications Security*, 5015–5017. https://doi.org/10.1145/3658644.3691387

[38] *The BGP router must be configured to use the maximum prefixes feature to protect against route table flooding and prefix de-aggregation attacks.* (n.d.). STIG Viewer | Unified Compliance Framework®. Retrieved December 3, 2024, from https://www.stigviewer.com/stig/router_security_requirements_guide/2021-03-16/finding/V-207156

[39] Andree Toonk. (2014, September 3). *Using BGP data to find Spammers*. https://www.bgpmon.net/using-bgp-data-to-find-spammers/

Appendix D: Technical Resources

1. MANRS Implementation Guide
2. CableLabs Cybersecurity Framework Profile for Routing Security
3. CableLabs RPKI Best Common Practices
4. One RPKI Deployment Journey
5. NIST RPKI Monitor
6. NIST SP 800-189r1, Border Gateway Protocol Security and Resilience, 2025
7. RFC 7454 - BGP Operations and Security - IETF
8. RFC 6480 - An Infrastructure to Support Secure Internet Routing - IETF
9. RFC 8205 - BGPsec Protocol Specification - IETF
10. RFC 6811 - BGP Prefix Origin Validation - IETF
11. RFC 6482 - A Profile for Route Origin Authorizations (ROAs) - IETF
12. RFC 7908 - Problem Definition and Classification of BGP Route Leaks - IETF
13. RFC 4012 - Routing Policy Specification Language (RPSL) - IETF
14. RFC 3704 - Ingress Filtering for Multihomed Networks - IETF
15. RFC 5082 - The Generalized TTL Security Mechanism (GTSM) - IETF
16. ARIN Delegated RPKI
17. Krill RPKI Daemon

Appendix E: Acknowledgments

Special thanks to the following partners for their work on this effort:

- AT&T
- Amazon Web Services
- CableLabs
- Charter
- Cisco
- Cloudflare
- Comcast
- Cox
- Communications Sector Coordinating Council (CSCC)
- CTIA
- Cybersecurity Coalition
- Google Cloud
- Internet Society
- IT Sector Coordinating Council (ITSCC)
- Juniper Networks
- Lumen
- Microsoft
- NCTA
- NTCA
- T-Mobile
- USTelecom
- Verizon