Security of the Internet’s Routing Infrastructure

A BROADBAND INTERNET TECHNICAL ADVISORY GROUP
TECHNICAL WORKING GROUP REPORT

A Uniform Agreement Report

Issued:
11/2/2022
The Security of the Internet’s Routing Infrastructure
A Broadband Internet Technical Advisory Group Technical Working Group Report

Completed: 10/18/2022
# Table of Contents

## Executive Summary
- Observations .......................................................... 3
- Recommendations ...................................................... 4

## 1 Introduction to Internet Routing and Addressing
- 1.1 Internet Addressing ............................................... 5
- 1.2 Internet Routing and the Border Gateway Protocol ........... 6

## 2 Common Routing Security Problems
- 2.1 Route Misorigination ............................................... 7
- 2.2 Path Manipulation Attacks ........................................... 8
- 2.3 Route Leaks ........................................................... 9
- 2.4 Relationship to Higher-Level Attacks ......................... 10

## 3 Routing Security Incidents
- 3.1 Route-Hijacks ...................................................... 11
- 3.2 Route-Leaks ........................................................ 12
- 3.3 IP Squatting ........................................................ 13
- 3.4 Using BGP to Subvert HTTPS .................................... 14

## 4 Routing Security Solutions
- 4.1 BGP Monitoring and Anomaly Detection ....................... 15
- 4.2 Route Filtering Using Internet Routing Registry Data ....... 17
- 4.3 Route Filtering Using Resource Public Key Infrastructure Data ..... 18
- 4.4 BGP Session Security ............................................. 19
- 4.5 Source Address Validation ....................................... 20

## 5 Challenges of Adoption and Future Direction
- 5.1 A Collective-Action Problem .................................... 21
- 5.2 Non-Technological Factors ........................................ 22

## 6 Observations .......................................................... 23

## 7 Recommendations
- 7.1 General Recommendations ...................................... 24
- 7.2 Recommendations to Network Operators ...................... 25
- 7.3 Recommendations to Policy-makers ............................. 26

## 8 Appendices
- 8.1 KLAYSwap Cryptocurrency Attack ............................. 27
- 8.2 RPKI Ecosystem and Operational Considerations ............... 28
- 8.3 BGPsec details ..................................................... 30

## Glossary ................................................................. 31

## References ............................................................. 32

## Report Contributors and Reviewers .................................. 33

## Editors ................................................................. 34
Copyright / Legal Notice

Copyright © Broadband Internet Technical Advisory Group, Inc. 2022. All rights reserved.

This document may be reproduced and distributed to others so long as such reproduction or distribution complies with Broadband Internet Technical Advisory Group, Inc.’s Intellectual Property Rights Policy, available at www.bitag.org, and any such reproduction contains the above copyright notice and the other notices contained in this section. This document may not be modified in any way without the express written consent of the Broadband Internet Technical Advisory Group, Inc.

This document and the information contained herein is provided on an “AS IS” basis and BITAG AND THE CONTRIBUTORS TO THIS REPORT MAKE NO (AND HEREBY EXPRESSLY DISCLAIM ANY) WARRANTIES (EXPRESS, IMPLIED OR OTHERWISE), INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, OR TITLE, RELATED TO THIS REPORT, AND THE ENTIRE RISK OF RELYING UPON THIS REPORT OR IMPLEMENTING OR USING THE TECHNOLOGY DESCRIBED IN THIS REPORT IS ASSUMED BY THE USER OR IMPLEMENTER.

The information contained in this Report was made available from contributions from various sources, including members of Broadband Internet Technical Advisory Group, Inc.’s Technical Working Group and others. Broadband Internet Technical Advisory Group, Inc. takes no position regarding the validity or scope of any intellectual property rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this Report or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.
About the BITAG

The Broadband Internet Technical Advisory Group (BITAG) is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical Working Group (TWG) to develop consensus on how the Internet operates including broadband network management practices and other related technical issues that can affect users’ Internet experience, including the impact to and from applications, content and devices that utilize the Internet.

The BITAG’s mission includes: (a) educating policymakers on such technical issues; (b) addressing specific technical matters in an effort to minimize related policy disputes; and (c) serving as a sounding board for new ideas and network management practices. Specific TWG functions also may include: (i) identifying “best practices” by broadband providers and other entities; (ii) interpreting and applying “safe harbor” practices; (iii) otherwise providing technical guidance to industry and to the public; and/or (iv) issuing advisory opinions on the technical issues germane to the TWG’s mission that may underlie disputes concerning broadband network management practices.

The BITAG Technical Working Group and its individual Committees make decisions through a consensus process, with the corresponding levels of agreement represented on the cover of each report. Each TWG Representative works towards achieving consensus around recommendations their respective organizations support, although even at the highest level of agreement, BITAG consensus does not require that all TWG member organizations agree with each and every sentence of a document. The Chair of each TWG Committee determines if consensus has been reached. In the case there is disagreement within a Committee as to whether there is consensus, BITAG has a voting process with which various levels of agreement may be more formally achieved and indicated. For more information please see the BITAG Technical Working Group Manual, available on the BITAG website at www.bitag.org.

BITAG TWG reports focus primarily on technical issues, especially those with the potential to be construed as anti-competitive, discriminatory, or otherwise motivated by non-technical factors. While the reports may touch on a broad range of questions associated with a particular network management practice, the reports are not intended to address or analyze in a comprehensive fashion the economic, legal, regulatory or public policy issues that the practice may raise. BITAG welcomes public comment. Please feel free to submit comments in writing via email at comments@bitag.org.
Executive Summary

The Internet is critical to the global economy, and Internet security incidents regularly make headlines. Though much attention has been paid to the security of applications, data, and users, this report focuses on the security of the system by which the Internet routes our traffic around the world.

The Internet consists of the set of networks that utilize the same standard Internet protocols to interconnect and exchange data. These networks belong to Internet service providers, content and application providers, government agencies, universities, businesses, and others. The Internet’s globally-distributed nature requires the cooperation of the tens of thousands of entities collectively responsible for the planning, maintenance, and operation of its routing infrastructure.

Because no single network is directly connected to everything on the Internet, each network exchanges routing information with its neighbors to indicate which destinations it can reach—either because it is connected to those destinations directly, or because it can reach them via another neighbor. With this information, each of those networks’ routers constructs its own map (called a “routing table”) of the Internet, which it uses to direct traffic. The protocol used to communicate routing information is called “Border Gateway Protocol,” or BGP[1]. BGP was first standardized in June 1990 and, like many parts of the early Internet, functionality was prioritized over security. Though many other Internet protocols have seen subsequent security improvements, integrating encryption and authentication, BGP is more complex so changes require many incremental, iterative development and deployment efforts. Because this routing infrastructure forms the most basic underpinning of the Internet, attacks against it can subvert or deny access to the applications and services that rely on the Internet. Both malicious attacks and simple operational errors can, and often do, result in such disruption.

Routing security incidents have severe consequences: large-scale service outages, compromises of data security and privacy, and subversion of other critical Internet infrastructure like domain name service and cryptographic key management. Yet it can be difficult to recognize incorrect routing information: it propagates far from its point of origin and from any context that could be used to evaluate its veracity.

When BGP was introduced, the Internet consisted of fewer than 2,000 networks[2]. Trust, identity, and verification of routing information were relatively simple, and the Internet’s practitioners were generally both well informed and willing to collaborate toward the success of their shared endeavor. Today, the Internet consists of more than 71,000 interconnected networks with disparate business models, scale, locality, and governing law[3] [4]. Today’s risks are vastly different than those at the time BGP was designed, due to the subsequent increase in the Internet’s complexity and scale, and the rise of cybercrime, government cyber-conflict and other threats.

For these reasons, the Internet community continues to improve the security of the global routing system to protect the applications and services that rely on it. From the IETF (Internet Engineering Task Force) and network operator forums, to MANRS (Mutually Agreed Norms for Routing Security)[5], network operators have found many venues in which to collaboratively address this need.

In this report, we review the current state of Internet routing technology, discuss its weaknesses, and present a few illustrative real-world examples of the resulting connectivity disruptions and criminal activity. We review existing technologies that can mitigate some of these problems and introduce emerging technologies that may provide more comprehensive solutions in the future.

Broadly speaking, we discuss misrouting which is intentional or unintentional, and misrouting which is characterized by a false origin or an unauthorized path. We also touch on the related topic of forged IP packets.
These categories are often conflated in popular accounts, and variously termed “hijacks,” “route leaks,” or “address spoofing.” Among the remedies we discuss are route monitoring, route filtering using publicly available routing policy data, and source-address validation.

None of these techniques address the full spectrum of BGP vulnerabilities and threats[6], and indeed a comprehensive solution to routing weaknesses may continue to elude us. For example, RPKI ROV can protect some aspects, but leaves residual vulnerabilities. Other techniques to address those weaknesses are still under development, their effectiveness has not been fully tested or proven, and may themselves introduce new vulnerabilities or complexity. Furthermore, the adoption of even those practices that do exist is incomplete, and many networks thus lack even protections that are currently available. Nonetheless, the current techniques are largely complementary and the Internet engineering and operations community continues to develop and refine routing security practices.

- Section 1 provides background on Internet addressing and routing including BGP.
- Section 2 describes problems in routing security and introduces common vocabulary and taxonomy.
- Section 3 reviews routing security incidents, discussing impacts and causes.
- Section 4 presents a variety of solutions that can mitigate these risks.
- Section 5 catalogs concerns that transcend investment or prescriptive approaches.
- Section 6 summarizes the findings of the paper.
- Section 7 provides recommendations to network operators and policy-makers.
- Appendices 8 explore some topics in greater technical detail.
- A Glossary provides concise definitions of terms-of-art used in the document.

Observations

This report highlights the following observations:

- The problem of ensuring reliable interdomain routing is complex and doing so on a global scale requires that we rely on information from remote and unknown sources.
- The Internet’s routing table is built in tens of thousands of independent instances by network operators around the world. The result is a globally shared consensus with local variation.
- The Internet routing system’s capacity to respond dynamically to change and its freedom from single points of failure are great strengths, but also pose concomitant risks.
- Most routing anomalies are unintentional, but some are clearly malicious attacks. Security improvements make the Internet more resilient to both intentional and unintentional misrouting.
- Routing security incidents have not constituted an existential threat to the Internet, nor have any rendered the Internet generally unusable; nonetheless, it is important that we pursue continuous improvement.
- While there are a multiplicity of applicable security practices, many are technologically complicated to implement and maintain, and many result in increased fragility of already complex systems.
- There are many parties with roles to play in securing the Internet’s routing system, and not all of the recommendations in this report are applicable to all parties.
- Many methods of improving routing security require many parties to implement together, and most protect others more than they protect the party that implements them. As a consequence, many first-movers realize little immediate benefit, while bearing disproportionate costs and risks.
- BGP is a mature protocol. It has flexibly adapted to more than three decades of changing demands. Changes to BGP proceed at a deliberate pace and this reflects the inherent complexity of making changes to a global system of tens of thousands of independent organizations.
- Future communications protocols include their own routing mechanisms, but BGP is unlikely to be replaced as the routing protocol of the Internet. New routing protocols will emerge in conjunction with a new global network, not within the context of the Internet.
- The Internet’s tens of thousands of constituent networks operate under diverse legal systems and business models. Regulation cannot achieve the degree of global harmonization that the Internet routing community already achieves voluntarily[7].
- The Internet’s multistakeholder governance and standardization processes successfully identify problems and develop diverse and complementary solutions.
• The development and global deployment of new technologies in the operational network may take decades, and this is inherent in the complexity of the process.

Recommendations

In addition, this report provides the following recommendations:

Recommendations to Network Operators

• Explicitly include routing security in operating plans and external contracts, to ensure the security and resilience of information systems and services.
• Enroll IP addresses and ASNs independent monitoring systems and publicly declare routing policy using RPKI and IRR systems.
• Validate routes received and ignore BGP routes determined to be invalid.
• Financially support open-source routing security software to ensure continued development.
• Contribute to open data platforms that enable transparent situational and longitudinal routing information sharing.
• Apply source address validation to prevent source address spoofing[8].

Recommendations to Policy-makers

• Respect the Internet’s multistakeholder standards development process. If regulation is considered, set goals rather than specifying technologies.
• Engage the Internet community to address regional policy incentive issues which slow adoption of standardized routing security technologies.
• Fund the long-term monitoring programs needed to understand Internet routing and effects of changes over time.
1 Introduction to Internet Routing and Addressing

The Internet is a network composed of thousands of interconnected constituent networks. Each of these networks, which might belong to a university, a content distribution network (CDN), or an Internet service provider (ISP), is independently administered. For purposes of routing, each of these networks is referred to as an Autonomous System (AS) and uniquely identified by a numeric Autonomous System Number (ASN).

One of the defining characteristics of the Internet is that it can deliver data packets between networks that are not directly connected to each other. Packets are forwarded through as many intermediary networks as necessary to reach their destination. For this forwarding function to work across the global Internet, each intermediate network needs to know what destinations exist, and which of its neighboring networks is on the best path to each destination. This knowledge resides in Internet routing tables, and it is communicated between networks using the Border Gateway Protocol (BGP). From a routing perspective, the destinations are represented by blocks of Internet Protocol (IP) addresses, and the sequence of networks along the path from a source to destination are identified by ASNs. The individual routers within those networks use BGP to construct the “map” that determines the next router on the path to the destination. Much like a street address in the physical network of roads, an IP address identifies a distinct destination (i.e., resource, service, or connected device) in the global Internet, and BGP is like a navigation application on your smartphone that continuously computes the next turn to make on the best route to that destination [9].

1.1 Internet Addressing

IP addresses and ASNs are uniquely allocated by the Internet Assigned Numbers Authority (IANA) to five Regional Internet Registries (RIRs), each of which in turn assigns blocks of addresses to Local Internet Registries (LIRs, typically network operators) or National Internet Registries (NIRs), which further subdelegate to their customers, as shown in Figure 1[10]. Adding to this complexity, holders of IP addresses may buy, sell, lease, or loan control and use of those blocks to other network operators, temporarily or permanently. As well, network operators are subject to mergers and acquisitions, bankruptcies, and dissolution. Any such conditions may not be accurately reflected in the publicly visible records of the registries above them in the delegation hierarchy.

![Figure 1: IP address delegation model. The IANA delegates to the five Regional Internet Registries, which delegate to Local and National Internet Registries. Local Internet Registries assign addresses to customers.](image)

1.2 Internet Routing and the Border Gateway Protocol

BGP, like other Internet protocols, was developed and standardized within the Internet Engineering Task Force (IETF). BGP was developed explicitly as an “exterior gateway protocol,” specifically for the communication of routing data between networks rather than within networks, and has been the Internet’s sole global inter-domain routing protocol for thirty years.\(^1\) As a routing communication protocol, BGP allows networks

---

\(^1\)An earlier protocol, called EGP, was the first but BGP has been dominant for approximately three decades.
to “advertise” blocks of destination IP addresses to their neighboring networks and receive the routing information advertised by neighboring networks. Each neighbor may propagate or receive information about destinations that are farther “downstream” from these direct neighbors. When a network has a packet to deliver to a given IP address, its routing tables provide the necessary information to forward the packet to the appropriate neighbor network, which may repeat the operation to forward the packet toward its ultimate destination.

Here are the main components of a routing table entry as it might be displayed by a router’s user interface:

```
192.0.2.0/24   3257  58453  38040  23969
```

The left-most portion in this example is the IPv4 address block 192.0.2.0/24. The sequence of numbers on the right is the “AS_PATH,” composed of ASNs identifying the networks in the path to this destination IP address block.

As diagrammed in Figure 2, when an Internet router receives a BGP route advertisement in an “update” message, it will, according to its configuration, apply inbound filters to ignore BGP advertisements not aligned with configured routing policies, update its local routing table with the new information and, in many cases, pass resulting changes to other neighboring routers. When a packet arrives at a router, the router examines its routing table for the most specific matching route for the packet’s destination IP address and forwards the packet to the indicated “next-hop” router on the path to the destination. Thus, changing the contents of the routing table changes how (or even if) the traffic is delivered.

Figure 2: Routing and forwarding within an Internet router.Incoming BGP routing information from neighbors is processed in the “control plane,” ingested into the routing table, and forwarded onward to neighbors as governed by filter lists. Incoming data packets from neighbors are processed in the “forwarding plane,” where they are routed to appropriate neighbors based on information in the routing table, as governed by access control lists.

Evaluating the veracity of this association of an AS origin and an AS_PATH with each block of address space is the fundamental challenge of routing security. Today, the security of the Internet’s routing is imperfect; there is no unanimous consensus on the mechanisms by which routing information should be validated, no existing mechanism addresses the breadth of currently observed problems, and deployment of those mechanisms that do exist is incomplete.

The commitment of transmission capacity within and between networks is an expenditure of resources and, when there is contention for capacity, incurs opportunity cost. Routing information controls the level of traffic flow; hence, network operators define routing policies to help govern the flow of traffic.

Though BGP as originally designed had few explicit security features, it enables each network to apply its own policy regarding which information it accepts, uses, prefers, and retransmits to other networks. This control is exercised through, among other things, “filter lists,” which control the ingress and egress of routing information from the data plane of each router. Filter lists are typically built, either manually or via automation, from information received “out of band” through other mechanisms—normally from neighbors'

---

2A comparable example with an IPv6 address block would be 2001:db8:3af0::/48 3257 58453 38040 23969
Routing Policy Specification Language (RPSL) assertions, but even via email or phone calls between network operators. Routing information propagated by BGP itself is considered “in band” in this context.

In part, this lack of strong assurance is an accident of history, since the need for security in the Internet was largely perceived subsequent to the definition of foundational protocols like BGP, and in part as a consequence of the modular, compartmentalized nature of the Internet architecture. Protocols (the agreements and standards that govern the way networks exchange information to implement the network service) are purposely designed to be interoperable building blocks, each accomplishing its intended function, not agglomerated together with other functions into monolithic blocks.

2 Common Routing Security Problems

BGP has been the Internet’s sole global routing protocol for thirty years and a multitude of mechanisms have been explored for improving its security and resilience. Some have predominated for a time, but, to date, none have been universally adopted, nor have any addressed the full scope of routing security challenges. The Internet is thus still vulnerable to disruption by both accidental and intentional manipulation—whether false claims of direct connectivity to specific destinations, misrepresentation of the AS path to a destination, or routes that violate business agreements between networks. Such misinformation may be the result of a simple mistake such as a misconfiguration of a network device, or it may be the result of a purposeful attack by a malicious actor intent on exploiting the security vulnerability for its own ends. It is often difficult or impossible to ascertain the motivation behind routing security incidents; hence, we concentrate on the technical causes of incidents and their observed effects on the routing infrastructure.

We introduce the following term to describe common routing incidents. (See the glossary for complete definitions.)

- **route-hijack**: the malicious or accidental manipulation of BGP information such that either data is delivered to an improper destination or the normal data path between two destinations is altered in ways that could compromise confidentiality.

Note that, though we use terms such as “hijack” and “manipulation,” we are careful to state that the terms apply to either intentional (e.g., malicious attacks) or accidental (e.g., misconfiguration) actions. Attempting to classify events by the motivation of those responsible is difficult, and one should observe that any incident attributed to an accident could easily be repeated as an intentional attack, disguised as an accident. Likewise, security mechanisms designed to mitigate such incidents are largely independent of the question of the motivations of those responsible.

We also introduce terms to describe the technical causes of common BGP incidents, focusing on what BGP information is manipulated in an abnormal or unauthorized manner.

- **prefix-manipulation**: the unauthorized origination, or modification, of the destination address prefixes in a BGP update that can result in denial of service, delivery of data to unauthorized destinations, or unintended modifications of the path traveled by packets between two communicating systems.

- **path-manipulation**: the unauthorized modification (addition or deletion) of AS_PATH data in a BGP update, which can result in denial of service, delivery of data to unauthorized destinations, or unintended modifications of the above-mentioned path between two communicating systems.

- **route-leak**: the malicious or accidental propagation of BGP information beyond its intended scope, which can result in unintended changes in the routes used to forward data. Often these changes lead to loss of connectivity due to misdirected routing paths that are in violation of other policy filters or congestion collapse along the modified path.

Routing incidents are sometimes complex events with a variety of possible consequences. Thus, the terms above are meant to capture the vernacular mode of their description, not to provide a unique classification of BGP incidents.
In some cases, routing incidents disrupt the flow of Internet traffic. In others, they misdirect communications, allowing interception or manipulation. Routing incidents are not infrequent, and their effects vary greatly.

2.1 Route Misorigination

Route origin manipulation, also called “misorigination” or “unauthorized origination,” is the most common form of prefix manipulation. It occurs when a network falsely advertises that it is directly connected to one or more destination address prefixes belonging to another network, thereby soliciting traffic for those destinations to be delivered to the attacker rather than to the authentic user of the address space. If this false information is accepted by neighboring networks, traffic is forwarded to the attacker instead of its legitimate destination, causing a denial of service (DoS) or allowing the interception of traffic. It is thought that many misorigination incidents result from configuration errors rather than from intentional attacks, but there are also clear cases of malicious intent. In both cases, they harm users and demonstrate the fragility of the routing system.

Some spammers, also known as “fly-by spammers,” use misoriginated addresses to send spam email. Using IP addresses assigned to another party or not assigned to anyone may allow spammers to remain stealthy and elude spam filters, which depend on sender IP address reputation. In this way, a spammer might briefly impersonate the mailserver of a reputable company, in order to capitalize on, and co-opt, the reputation of that server and thereby evade filtration.

Misorigination attacks can also be used to mount more sophisticated Machine-in-The-Middle (MiTM) attacks against Internet services (Figure 3). MiTM attacks consist of an attacker interjecting itself into communications between authentic origin and destination, generally a client and server, representing itself as the server to the client and the client to the server. When successful, neither client nor server perceives that the privacy of their communications has been violated.

For example, the MyEtherWallet attack involved Amazon’s DNS service which is used to map the domain name MyEtherWallet.com to the IP addresses of the servers which host that application. The attackers redirected DNS lookups for MyEtherWallet to a malicious website instead of the legitimate one[11]. As a result, some people logging in to MyEtherWallet.com were connected to an imposter site and gave their credentials to criminals, who promptly drained cryptocurrency from the victims’ wallets.

2.1.1 More-Specific Prefix Attacks

More-specific prefix attacks are one of the most common forms of misorigination or hijack. When a destination IP address matches more than one route, a router’s decision-making algorithm selects the most specific of the routes, that is, the one that contains the smallest, or most-specific, block of IP addresses. If there are two routes, 192.0.2.0/23 from AS1 and 192.0.2.0/24 from AS2, in a router’s routing table and the router receives a packet with the destination address 192.0.2.1, the router selects 192.0.2.0/24 to AS2 because it is more specific. Attackers executing origin attacks use these more specific prefixes in order to increase the

---

3 Blocks of Internet addresses are referred to as “prefixes,” because it is the prefix of the block, the left-hand side, which defines it. The right-hand side is reserved for local use. The “prefix length” is the portion of the address which is uniquely
effectiveness of their attack (Figure 4). There have also been a number of instances of apparently accidental de-aggregation events where some process has injected many more-specific prefixes with the same origin as the legitimate announcements[12] [13].

![Figure 4: More-specific prefix attacks. By analogy, imagine packet is like a traveler trying to reach Los Angeles from Europe who sees a signpost that indicates that “The United States is to the west,” “California is to the west,” and “Los Angeles is to the east,” the traveler/packet may proceed east, even if at a greater distance, because “Los Angeles” is more specific—more precise—than “California” or the United States. Though this is an easy geographic error for a human to spot, it is difficult to codify algorithmically relative to the Internet’s complex and dynamic topology.](image)

2.1.2 Nearer Origin Attacks

A less common, and more difficult to accomplish, attack utilizes a prefix of the same specificity, injected into the Internet topology closer to the source of the traffic that is to be intercepted than to the authentic destination. If such an attack also forges the origin AS, it may be very difficult for monitoring systems to perceive.

2.2 Path Manipulation Attacks

Another category of weakness involves the BGP AS_PATH attribute[1]. This attribute identifies the ASes through which the BGP announcement message has passed. Consider our earlier example where the AS_PATH is the string of integers on the right-hand side:

```
192.0.2.0/24 3257 58453 38040 23969
```

Each AS will “prepend” its ASN to the left-hand side of the path it received from its neighbor. Thus, the AS_PATH should list, in right-to-left order, the ASes traversed by an announcement, with the most-recent AS at the left of the list and the originating AS as the final entry on the right. In our example above, AS23969 is the “origin” AS, which advertised to AS38040, which advertised it in turn to AS58453, then to AS3257, which is a direct neighbor of our point of observation in this example.

The primary purpose of the AS_PATH is to provide loop-prevention. Each router that receives a route checks the AS_PATH for the presence of its own ASN; if it finds it, it rejects the route. Because there is no inherent integrity check on the BGP AS_PATH attribute, any network that passes the BGP update can allocated through the delegation hierarchy in Figure 1. The longer it is, the fewer addresses remain for local use. Because the “prefix length mask” defines the demarcation point between assigned address and local-use in binary notation, we write it as a power of two. Thus a mask length and prefix length of /0 contains the whole Internet, a mask length and prefix length of /1 contains half the Internet, and a mask and prefix length of /24 contains 256 addresses, or one 2^24th of the Internet, 0.000006%. It is thus more specific than a /23, which contains 512 addresses. In the example above, the /23 block of 512 addresses 192.0.2.0/24 can be subdivided (perhaps through delegation) into 192.0.2.0/24 (the lower half, 256 addresses) and 192.0.3.0/24 (the upper half, the other 256 addresses). Each of those could be further subdivided into /25s of 128 addresses each, but the routing policy of most Autonomous Systems refuses prefixes of length greater than /24, to conserve scarce memory in their routing and forwarding tables.

4This feature, which is common to all BGP-speaking routers, has been exploited to prevent victims of path-manipulation attacks from seeing the attacks. If the victim’s ASN is inserted into the forged AS_Path, the victim’s routers reject the forged route, rendering it invisible to the victim. The same principle can be exploited more generally in conjunction with split-horizon routing and the BGP community attribute to minimize the visibility of hijacks, particularly to hide them from monitoring systems.
theoretically change this value in ways contrary to normal operation. Hence, a router receiving an update cannot be sure that the announcement traversed the networks indicated in the AS_PATH.

In a path manipulation attack, the AS_PATH attribute is manipulated, causing network traffic to not follow the legitimate path. For example, an attacker can advertise a path in which it falsely appears to be directly connected to the origin AS: this will have the dual effect of advertising to its neighbors (which will potentially propagate the announcement even further) an appealing – because short – path towards the corresponding prefix while still showing the legitimate owner AS as the origin. This type of attack can be difficult to detect because it is not uncommon in Internet routing for the best path to various destinations to change due to topology changes in the network such as “link state” changes (data transmission circuits failing and being restored).

A special case of path manipulation attack is when a legitimate path for a given prefix does not exist in the first place, but the attacker forges an announcement for such a prefix copying a legitimate path it has learned for a corresponding less specific prefix. Because more-specific routes are always preferred by routers, the attacker will attract all traffic towards the more specific prefix and will have the option to redirect it towards the legitimate origin thus performing a MiTM attack[14].

2.3 Route Leaks

Problems often arise when one network announces more or different routes than usual or routes that violate the explicit or implicit routing policies between it and its neighbor network (and often hence to their neighbors, and so on). Since routing information controls traffic flow, the result of a routing leak can be that a greater volume of traffic than intended may flow across some given network path(s) and cause them to become overutilized, congested, drop traffic, and lead to performance degradation or outage.

According to IETF RFC7908 Problem Definition and Classification of BGP Route Leaks, a route leak is the propagation of routing announcements beyond the intended scope[15]. In other words, an announcement from an AS of a learned BGP route to another AS is in violation of the intended policies of the receiver, the sender, or one of the ASes along the preceding portion of the AS_PATH. The intended scope is usually defined in terms of the business relationship between ASes, such as customer-to-transit provider, or peer-to-peer, and is implemented by the ASes through announcement filtering controls.

A route leak is often a violation of the “valley-free” rule, according to which, after traversing a provider-to-customer or peer-to-peer edge, the AS path cannot traverse a customer-to-provider or peer-to-peer edge. The result of a route leak can be redirection of traffic through an unintended path that may enable eavesdropping for traffic analysis or data modification. Because in most cases such violations cause traffic to flow along sub-optimal paths, the leak often leads to infrastructure overload or a DoS condition. To use a recent example, a small ISP in Pennsylvania started to announce (leak) routes for Cloudflare, Amazon, and Linode as a result of a technical error by one of its network administrators. This error caused those destinations to become unreachable from some parts of the Internet[16].

A motivated adversary can use a route leak in many ways, including traffic surveillance and reconnaissance activities as well as MiTM attacks manipulating the data passing through. The main danger of a route leak when used by an attacker is that an adversary can interpose itself in the path between a variety of networks and specific destinations with relative ease and raising little suspicion (as compared to the difficulty and risk of physically compromising the normal data path).

Extensions to BGP are being developed to address detection and mitigation of some common forms of route leaks. Some of these extensions leverage the infrastructure provided by RPKI and related BGP security extensions[17]–[20].

5The term “valley-free” is derived from the prevalent mode of diagramming Internet topological relationships. Packets can be thought of as being routed up (via transit), across (peering), and then down again (via transit), but never up, down, and up again, because that would require transit and money flowing the same direction.
2.4 Relationship to Higher-Level Attacks

A routing attack aims to corrupt the routing tables of networks and cause them to make improper forwarding decisions (often resulting in the data being forwarded to or through the adversary). However, the impact of BGP attacks goes way beyond simply their disruption of the routing ecosystem. BGP attacks can be used to facilitate highly effective attacks on higher-level applications.

BGP attacks exploit vulnerabilities in higher-level Internet services because they allow an adversary to be on the path of critical communication. This applies to simpler applications that are easily compromised when the adversary is capable of reading or altering network traffic (like DNS and unencrypted HTTP connections), as well as secure applications that are often assumed to be “protected” with cryptography (as demonstrated by BGP attacks on Tor, on cryptocurrency, and on TLS)\[21\]–\[23\]. Some research has explored application-specific defenses to BGP attacks in these various contexts, but these defenses are often not foolproof because BGP attacks violate the fundamental trust these various applications place in the network\[24\]–\[26\]. Thus, security against BGP attacks is not only essential for a secure routing ecosystem but critical for the plethora of applications built atop the Internet.

3 Routing Security Incidents

Here we summarize a few real-world incidents that illustrate the range and gravity of threats to the stability and security of the Internet’s routing system.

Though a few high-profile incidents have gained media and industry attention, many more have been reported over the years, including what appear to be cases of “serial offenders,” that is, ASes repeatedly injecting incorrect information over long periods of time\[27\]. Unfortunately, though, we do not yet have a complete and detailed understanding of how, when, where, why, or by whom the BGP system is abused. One major challenge is the lack of comprehensive and longitudinal data of confirmed events; operators and the Internet community mostly learn about these episodes through individual reports shared on operators’ mailing lists. Ground-truth information is thus scarce and limited to these episodes.

On the positive side, recent incident-monitoring efforts have started contributing to fill this gap and thus facilitate the detection of incidents. Furthermore, a significant fraction of the operational BGP world is transparent to the public, thanks to repositories providing pervasive and longitudinal data recording BGP messages exchanged by ASNs on the Internet—a sort of distributed “BGP flight recorder”. Specifically, entities such as Packet Clearing House (PCH)\[28\], RIPE Routing Information System (RIS) \[29\], and the RouteViews project \[30\] publish extensive BGP routing data, both real-time and historical. These public datasets, as well as similar private BGP feeds, play a major role in measurement studies of the Internet routing system in general and BGP security problems in particular, thus constituting a precious resource for post-event and forensic analysis. When publicly accessible, this infrastructure also enables automated incident-monitoring efforts that do not require access to private data feeds, thus broadening the opportunities available to the operational and research communities with consequent significant benefits.

3.1 Route-Hijacks

The AS7007 incident in April 1997 was arguably the first major Internet disruption caused by a security weakness in BGP\[31\] \[32\]. In this incident, a software bug caused a router to announce a large part of the global routing table as if it originated from a small network in Florida (AS7007). During the incident, a large portion of the Internet’s traffic was redirected to AS7007, where it was dropped, disrupting much of the world’s communication. Some ISP core routers became so overwhelmed that they had to be rebooted to recover. As observed by the rest of the Internet, this incident manifested itself as a route-hijack caused by prefix-manipulation. AS7007 announced direct connectivity to a large set of destinations that it was neither authorized for nor directly connected to.

Perhaps the most famous BGP route-hijack occurred in February 2008, involving the state telecom of Pakistan (PTCL) and YouTube. In that instance, the government of Pakistan ordered that access to YouTube be blocked within the country because of a video it insisted on preventing its citizens from accessing\[33\]. To
implement the block, PTCL announced more-specific prefixes for YouTube’s BGP routes in order to divert Pakistan’s domestic traffic bound for the video streaming service to an alternate destination within their own network. Once hijacked, PTCL’s goal was to drop Pakistani YouTube users’s packets, preventing them from accessing YouTube. What was planned as an intentional route-hijack through prefix-manipulation inside Pakistan took on global ramifications when PCTL accidentally leaked these routes to its international transit providers, who carried the routes around the world and thereby blocked YouTube for a large portion of the global Internet.

Since the PTCL-YouTube incident, there have been other instances of localized censorship implemented in BGP leaking out to the Internet. During both the Internet crackdown during the military coup in Myanmar in 2021 and the Russian crackdown of social media during its invasion of Ukraine in 2022, telecoms in each of these countries attempted to block access to Twitter using BGP route-hijacks to black-hole traffic[34]. In each case, the hijacked BGP route was propagated into the broader Internet (i.e., a route-leak) affecting Twitter users outside of the originating countries.

In 2008, researchers outlined how BGP could be manipulated to detour routes to enable a MiTM attack over the Internet[35]. The first documented case of a BGP-based MiTM attack like the one outlined in 2008 was discovered in 2013 originating in Belarus and targeting the networks of major US credit card companies and foreign governments[36].

Other similarly large route-leak incidents have occurred, disrupting Internet communications, including the Turk Telecom leak of December 2004, China Telecom incident of April 2010, and Telecom Malaysia incident of June 2015[37] [38] [39] [40]. Each of these disruptions lasted less than an hour and appeared to have been caused by misconfigurations, affecting address blocks indiscriminately. Large-scale leaks like these have become less frequent in recent years because of increases in the automation of router configuration in topologically central networks.

### 3.2 Route-Leaks

Not all large route-leaks involve the responsible network manipulating the prefix or path information so as to appear to be the origin of the route. In November 2018, MainOne, a large network in Nigeria, leaked routes received from several of its peers to its upstream transit providers. Among the leaked peers were major content networks such as Cloudflare and Google. MainOne’s transit provider, China Telecom, failed to filter these incoming erroneous announcements from MainOne, integrated them into its own routing tables, and proceeded to propagate them onward to its many providers, customers and peers. Consequently, a significant portion of Internet traffic bound for these content networks was detoured through China and Nigeria, disrupting access to these services. Shortly afterward, MainOne confirmed that the leak was caused by its mistaken router configuration, but the detoured traffic could still have been subject to interception or manipulation[41].

In June 2019, Allegheny Technologies leaked thousands of routes learned from one transit provider (DQE Communications) to another (Verizon). The routes Allegheny leaked included many more-specifics that had been generated by an internal route optimizer employed by DQE. The result was that these leaked more-specific routes propagated throughout the Internet and misdirected substantial amounts of Internet traffic to Allegheny, causing a severe disruption[16].

For two and a half years from 2015 to 2017, China Telecom leaked routes from Verizon’s Asia-Pacific network that were learned through a common South Korean peer AS. The result was that a portion of Internet traffic from around the world directed to Verizon Asia-Pacific was misdirected through mainland China. Without this leak, China Telecom would have only been in the path of traffic to Verizon Asia-Pacific originating from its customers. Additionally, for ten days in 2017, Verizon passed US routes to China Telecom through the common South Korean peer, causing a portion of US-to-US domestic traffic to be misdirected through mainland China[42].
3.3 IP Squatting

This report focuses mainly on the disruptions or security implications of hijacking IP addresses in use at the time of the incident. There are, however, also bad actors that announce normally unrouted IP address ranges that do not belong to them for the purpose of evading IP-based reputation services and complicating attribution of other follow-on malicious behaviors. This phenomenon is commonly referred to as “IP squatting” but is effectively a route-hijack of address space that is intentionally not announced to the public Internet by its rightful owners.

Since there is no effective legal or technical measure preventing this practice, bad actors can announce previously unused IP ranges belonging to others until networks on the Internet take steps to block them for this bad behavior. In July 2018, a network that became known as the “BGP hijack factory” was removed from the Internet through a collective action[43]. However, this remedy was unusual and such extraordinary action cannot be counted on for routine prevention.

3.4 Using BGP to Subvert HTTPS

BGP attacks are capable of subverting the security properties offered by HTTPS[23]. One real-world example occurred in 2022 when attackers launched a cross-layer BGP attack (i.e., used a BGP attack to compromise a higher-layer application) that hijacked requests for a javascript file being loaded by a cryptocurrency trading platform called KLAYswap. The targeted javascript file was being loaded securely over HTTPS, which is based on state-of-the-art TLS encryption. To bypass the security protections offered by TLS, the adversary requested a certificate for the domain hosting the javascript file from TLS certificate authority ZeroSSL. Using its ongoing attack that routed ZeroSSL’s traffic to the adversary, the adversary tricked ZeroSSL into believing the adversary was the legitimate owner of the domain. This caused ZeroSSL to issue a trusted TLS certificate for that domain to the adversary. With this certificate in hand, the adversary served its malicious javascript to end users over an unwarrantedly-trusted HTTPS connection. When users on the KLAYswap platform loaded the malicious javascript, it caused them to unknowingly transfer their cryptocurrency to the adversary which amassed $2 million worth of stolen cryptocurrency over the duration of its attack. This the first known attack that used BGP to target an HTTPS connection, but we have since seen this same strategy used in subsequent attacks[44], and it mirrors previous domain name hijacks such as those conducted by the Iranian military, which achieved the same goal by similar means[45] [46]. Further details of the KLAYswap incident can be found in the Appendices.

The KLAYswap attack is particularly notable because it involved a BGP attack successfully exploiting a system that was compliant with current best security practices. Even more aggressive application-layer defenses like DNSSEC and better TLS certificate error behavior would have been ineffective at preventing this attack because the adversary did not manipulate any DNS responses and served its malicious code over a trusted encrypted connection. In the current web ecosystem, millions of other websites including those following best practices are vulnerable to this type of attack[23].

4 Routing Security Solutions

The dynamism of Internet routing has been a hallmark of its success; nevertheless, incomplete deployment of mechanisms for validating routing messages, and the lack of rigorously maintained external data to support such validation, are significant weaknesses in the global routing system.

The Internet community has worked for decades to develop and deploy strategies and technologies that address the risks associated with global BGP operations, introducing data sources and mechanisms that can be used to check the validity of BGP information:

- BGP data collection and anomaly monitoring
- BGP route filtering using IRR data
- BGP data integrity verification using RPKI data

Other forms of checks discussed in this section relate to
- BGP session protection
- Source Address Validation (SAV)

All these strategies should be considered complementary, though they address different aspects of the problem space and have different deployment considerations. For instance, some may require given router software support or different skill sets on the part of operator staff. Different solutions have different deployment properties in terms of benefits or risks for early adopters or require different levels of coordination among implementors.

Additionally, the considerations and recommendations can and have varied over time, particularly as technologies and their implementations have matured. Hence, earlier reports\cite{47} \cite{48} \cite{49} \cite{50} that may make some different recommendations from this one should not be viewed as contradictory.

### 4.1 BGP Monitoring and Anomaly Detection

Monitoring is essential to understanding—through evidence—how Internet BGP routing is affected by abuse and misconfigurations. It can also serve as a defense or mitigation mechanism. BGP monitoring projects have evolved into an ecosystem of complementary and interdependent efforts. This ecosystem can be divided into three categories of work, each building upon the previous (Figure 5).

![Figure 5: BGP monitoring ecosystem. BGP routing data is collected (left), subjected to automated analysis to provide anomaly detection (center), which in turn is used to inform our understanding of events and their causes (right).](image)

BGP data collection projects aggregate routing data contributed by thousands of participating network operators. This takes two forms: periodic “snapshots” of the state of the routing table at specific instants in time, and of streams or recordings of flows of BGP route updates, as viewed at some point in the network. They are available in a assortment of formats. The wide variety of geographic and topologic points of view captured in these datasets is important because each provides a different and complementary view, contributing to a more complete understanding of the Internet’s state and the nature of interactions within its routing system.

Automated anomaly detection and incident monitoring efforts analyze BGP datasets and flows to distinguish suspicious or problematic BGP events from the background noise of millions of routine updates each second, the majority of which do not even affect the primary paths selected by routers for the forwarding of traffic. They present information and visualizations to aid further analysis and automated response.

Observatories, network planners, and analysts in both the public and private sectors utilize this selected information to understand the evolving shape and direction of the Internet, to engage and cooperate with the operational community, and inform policy in areas as diverse as competition, civil defense, economic development, urban planning, and human rights.

Depending on their characteristics, BGP incident-monitoring systems can

- Be helpful in attack detection and mitigation. Note that a BGP misorigination event affects two classes of victims: the AS owning the network prefix improperly originated and the ASes accepting the illegitimate route. Both types of organizations have an interest in detecting and mitigating these events, but their operational contexts and the role played by monitoring are very different.
- Provide situational awareness and inform policy-makers, law enforcement and stakeholders, also contributing to transparency and accountability. Ideally, monitoring can allow us to understand who is affected, how and to which extent, what are the timing, frequency, and duration of these events, how technically an attack is carried out, and so forth.
- Enable research such as for discovering new issues and attack types, testing defense methodologies on real data, and developing and evaluating new detection techniques.
- Serve as a troubleshooting tool for operators, such as when a misorigination is the result of a misconfiguration.

Monitoring systems can be distinguished into “prefix- or AS-focused” and “global” and further subdivided based on their characteristics and applications.

### 4.1.1 Prefix- or AS-Focused Monitoring Systems

One class of monitoring systems focuses on monitoring specific prefixes, with the typical users being the ASes responsible for routing those prefixes. These systems can be operated by third parties or self-operated. In the first case, an AS registers their information (e.g., prefixes owned or announced) to receive automated notifications. Examples are commercial products from Cisco, Thousand Eyes, and others. In self-operated systems, such as the ARTEMIS open-source software, the AS leverages existing infrastructure (e.g., PCH, RIS, RouteViews) or private BGP feeds to monitor their own prefixes autonomously. Both approaches face limitations. In systems operated by a third party, there is a trade-off between confidentiality and accuracy. The more information an AS shares with a third-party monitoring service provider, the narrower a/band more accurate the alerts the system can generate. However, many operators are reluctant to share detailed information about their routing policies and economic agreements, which they consider confidential. On the contrary, the accuracy of such systems, especially in terms of false positives (flagging legitimate routes as suspicious), is a known concern, exacerbated by lack of detail on the methodologies adopted by proprietary software services.

Self-operated systems do not suffer from the confidentiality issue and, when open-source, are transparent about their methodologies and capabilities. Still, they also suffer from false positives and false negatives, since certain attacks or misconfigurations cannot be fully validated even when all the confidential information available to the victim AS is accessible[51]. For example, this happens for misorigination events where the attacking AS is placed in the path, with a fake adjacency, more than one hop away from the origin.

Furthermore, a challenge both types of systems face is how to share knowledge automatically and continuously with the monitoring system, as router configurations, peering agreements, and policies change over time and may be hard to extract in an automated fashion. An example is the list of ASes a large operator, present in many Internet exchange points, peers with, and with respect to which prefixes.

Prefix- or AS-focused monitoring systems can be used by an operator to trigger a prompt reaction with the purpose of mitigating the event, for example, by announcing more specific prefixes[52].

### 4.1.2 Global Monitoring Systems

Another category of monitoring systems seek to monitor all the prefixes originated on the public Internet. They can provide situational awareness and support research and troubleshooting. Such systems can be privately run by an operator to monitor and evaluate incoming BGP routes announced to their routers or they can be centrally run by a third party and make their detection results publicly available. Two examples are bgpstream.com [53] with its Twitter feed and GRIP (Global Routing Intelligence Platform), an experimental open-source research platform providing public dashboards and alerts[54]. Designed with a different goal, these systems typically do not leverage ground-truth information (e.g., routing policies and configurations) provided by individual ASes. They instead resort to heuristics to detect and flag suspicious events (See Appendices). For this reason, from a public perspective, validation by operators is often necessary to fully confirm the nature of an event. However, affected ASes can benefit from the alerts and internally assess the nature of each specific event. Whereas, in the absence of complete ground-truth information, alerts should be taken with caution. As an aid, some monitoring systems include a confidence level associated with each inference.

The heuristics used by these systems vary in sophistication and can be combined to increase confidence in the output. Researchers actively work toward improving heuristics and proposing new approaches. One class of simple heuristics is based on historical routing data. For example, suppose a log of past BGP update
messages shows that a particular IP prefix is always originated by AS X; that is, AS X is always the last hop in the AS_PATH. In such a case, any new BGP announcement with a different last-hop AS (e.g., AS Y) looks suspicious. Similarly, a BGP announcement may be suspicious if the AS_PATH includes an edge (e.g., AS A followed by AS B) that has not appeared recently or ever in the past. However, a reliance on historical data as a proxy for ground-truth is prone to false positives and false negatives. For example, a seemingly new AS-level edge may appear in an AS_PATH because BGP selected an alternate route after a failure or with the addition of a new AS-level adjacency in the Internet topology. An anomaly-detection system may wrongly flag the BGP route as suspicious, leading to a false positive. As another example, RPKI offers an obvious opportunity to flag events that appear as potential misoriginations–when a prefix is covered by a ROA, a monitoring system can use this information to flag an RPKI-invalid announcement. Other heuristics are based on the relations between the suspected victim and attacker ASes and leverage meta-data datasets typically published by third parties. For example, if these two ASes are known to be owned by the same organization (“siblings”), it is very unlikely that the event is malicious and more likely that it is intentional. Similarly, if the two ASes are in a customer-provider relationship or if the suspected victim is among the customers (within the “customer cone”) of the suspected attacker, it is less likely that the event is malicious. Finally, global incident-monitoring systems are key to supporting broader monitoring efforts, which may aggregate these sources at the AS-level or across reporting periods.

4.1.3 Monitoring and Anomaly Detection to Improve Security

A suspicious announcement may trigger an alarm to alert a human administrator, or may drive an automatic routing decision that prefers a “normal” route over a suspicious one or even filters suspicious routes entirely. (See Pretty Good BGP (PGBGP)[55] for an example design.)

BGP monitoring solutions have several significant advantages over other BGP security solutions. Anomaly-detection techniques are incrementally deployable by individual ASes, without requiring cooperation from other ASes, let alone global adoption. ASes that avoid selecting suspicious routes can achieve immediate security benefits. Large ASes with many BGP neighbors often learn many BGP routes for the same IP prefix, making it likely that they learn some more credible routes that they can select instead of risking using a suspicious route.

Still, anomaly-detection techniques are not a panacea. A reliance on historical data as a proxy for ground-truth is prone to false positives and false negatives. To limit the impact of false positives, an AS could have a soft response to anomalies, such as temporarily lowering the preference of a suspicious route (to select a “normal-looking” route while, in parallel, investigating the suspicious route), rather than permanently filtering the suspicious route. This approach would prevent many short-lived attacks while limiting the impact of false positives. Alternatively, false negatives could arise if a strategic adversary can evade the anomaly-detection system attacks by carefully influencing the historical record, or by manipulating BGP routes in ways that appear consistent with past history. The likelihood of mistakes—whether false positives or false negatives—in detecting suspicious routes can be reduced by collecting and analyzing BGP data from a larger and more diverse set of vantage points.

BGP security solutions based on anomaly detection can be used in concert with other defenses. For example, historical BGP data can be a stand-in for ground-truth information when more authoritative data is lacking. For example, a security solution could use RPKI data for ASes that participate in the RPKI and historical data for other ASes. Anomaly detection can also be a second line of defense—part of a “belt and suspenders” approach—to ensure that the primary mode of defense does not miss important security events.

4.2 Route Filtering Using Internet Routing Registry Data

Network operators employ different types of filtering to control the flow of routing information, both inbound and outbound. Inbound filters can be built using information communicated between partner networks at provisioning time and subsequently. However, to improve the scaling properties of managing these configuration items, some automation schemes have been developed. One of these involves using published data to build routing permit-list filters automatically.
The Internet Routing Registry (IRR), in operation since 1995, is a distributed database of routing information\[56\]. IRR data is used to help debug, configure, and engineer Internet routing. The IRR contains information that helps to build BGP filters to help control the flow of BGP announcements.

IRR databases are operated by RIRs such as ARIN and the RIPE NCC, large ISPs such as Lumen and NTT, and independent organizations such as the Routing Arbiter Database (RADb), which preceded all the others.

The degree of authoritative information held by different operators varies. IRR databases operated by RIRs are now considered to hold the most authoritative data, since the RIRs also operate the databases that hold IP address and ASN information and implement validation of submitted data based on that information. IRR databases operated by the RADb and ISPs often contain stale and outdated information as they have no mechanism for the expiry of data which is no longer accurate or relevant.

Routing Policy Specification Language (RPSL) is the language used to register routing policies and configurations in the IRR\[57\]. RPSL is based on database “objects.” Each database object contains some routing policy information and some necessary administrative data. Some objects used by RPSL to encode routing policies are the Maintainer Object, the Route Object, the Autonomous System Object, and the AS-SET Object.

The Maintainer Object is used to provide authorization information for registrations. It lists the contact information and describes security mechanisms to update other objects. Route Objects define prefixes that originate from an ASN. They are grouped with other routes of the same origin AS.

The Autonomous System Object defines the import and export policies of an AS. Autonomous System set Objects (AS-SET) are used to group Autonomous System Objects or, recursively, other AS-SET Objects into a set. They are useful for defining groups with specific policies such as peers, customers, or providers.\[6\]

### 4.3 Route Filtering Using Resource Public Key Infrastructure Data

The RPKI allows entities that are allocated resources, such as IP addresses, to sign policy statements cryptographically indicating their intended use in routing. Like the IRR databases, the RPKI functions as a distributed database of routing policy. This set of protocols and practices is fairly complex, so we will delve into an extra level of technical detail since some observations and recommendations are illuminated by such particulars.

At a high level, RPKI is an improvement over the IRR in three ways. First, there is a tight coupling between resources (IP prefixes) as allocated by the RIRs and the authority to create policy statements about these resources. The RPKI model follows the hierarchical allocation from IANA described in Section 1.1. Second, statements about resources may be verified by evaluating signatures using public key cryptography.\[7\] Third, the delay between publication of a statement and operational application to routing is on the order of tens of minutes rather than tens of hours.

The authority of the RIR members to create the signed material maps to the resources they have been issued by the RIR. This is contrary to the IRR model, where data authenticity needs to be inferred from the database that it is in. The first two improvements mentioned above combine to guarantee that an entity that is not the holder of a resource is unable to sign policy statements about it.

The RPKI can be thought of as a tree structure rooted in the five RIRs and following the same delegation model used for IP addressing depicted in Figure 1. Resource certification is the first step in using the RPKI to publish cryptographically signed routing policy information and is comprised of establishing an appropriate service agreement with the relevant RIR and enrolling your number resources (i.e., IP address blocks and ASNs) into the RPKI. The RIR ensures that the organization requesting enrollment is the registered owner of those resources, establishes the RPKI authentication and access control policies for those resources and

---

\[6\] Similarly to using “whois” data for RIR and domain information, to query information in the IRR, use the “whois” command and “WHOIS” protocol\[58\]. Some IRR databases (such as the RADb) also support a web interface to perform IRR queries. Automation can be used to fetch the relevant data and find all “route” objects (for IPv4 address blocks or “route6” for IPv6 blocks) that contain a given ASN in their “origin” field. If AS-sets are used, recursive iteration may produce lists of hundreds or even thousands of entries.

\[7\] Each of the five Regional Internet Registries runs a Certificate Authority (CA) with a public/private keypair to sign or issue derivative objects (which can be other CAs) whose validity can, in turn, be verified by using the public key material\[59\].
creates and publishes a signed resource certificate that covers all number resources registered (Figure 6). This resource certificate serves to establish a validation chain to the RIR’s trust anchor and to scope the set of addresses and ASNs a user is permitted to use in subsequent RPKI signed policy declarations. That is, resource certification establishes the basis of trust in the ownership of number resources and the permissible scope of subsequent RPKI signed objects.

Figure 6: Resource Certification. Enrolling your number resources in the relevant RIR’s RPKI services and establishing resource certificates serves to establish a validation chain to the RIR’s trust anchor and to scope the set of addresses and ASNs a user is permitted to use in subsequent RPKI signed policy declarations.

4.3.1 RPKI Route Origin Validation

The first and predominant type of policy declaration published using the RPKI is a Route Origin Authorization (ROA). A ROA is an authoritative, signed statement that describes which networks are allowed to originate BGP advertisements of a given prefix (Figure 7). Networks can use ROA data to validate if the first AS in the AS_PATH of a received BGP update is, in fact, authorized to announce the prefix it contains. This is known as RPKI Route Origin Validation (RPKI-ROV). The primary purpose of RPKI-ROV is to enable routers to ignore those updates that are found to be invalid.

Figure 7: Creating Route Origin Authorization objects. Only the properly authenticated and authorized parties can create these cryptographically verifiable attestations.

RPKI-ROV was specifically designed to provide a scalable and robust authorization mechanism for BGP route advertisements. The design goals for the solution required that the authority to create ROAs for specific prefixes be strictly bound to the address allocation hierarchy maintained by the RIRs, that any user of such authorization data be able to independently validate the authenticity and integrity of that data, and that routers should not have to perform cryptography to use the data to enforce BGP policies. The attributes of current RPKI-ROV technology, RIR administered resource public key infrastructure, the use of signed objects based upon that infrastructure and the used of RPKI validating caches to collect, validate and distill ROA data before providing it to routers is a direct reflections of these design requirements.

Since the RPKI delegation tree is rooted in the five RIRs, each of them is considered a Trust Anchor (TA). To perform ROV, networks use relying-party (RP) software to download and validate ROAs starting at the Trust Anchors run by the RIRs. The RP software is configured with a Trust Anchor Locator (TAL) file for each of the RIRs; these are small cryptographically signed files containing Uniform Resource Identifiers (URIs) that describe where on the Internet to find the Publication Point (PP) for the rest of the RPKI information published by that RIR entity. Running on a server known as a “validating cache”, the RP software uses that
information to iteratively find, download, and cryptographically verify the ROAs and ancillary information (resource certificates, manifests, certificate revocation lists)(Figure 8). The resulting list of validated ROA payloads (VRPs) is then fed from the validating cache server(s) to routers using the RPKI to Router (RTR) protocol[60], [61]. VRPs are then compared to route announcements seen in BGP, resulting in one of three possible statuses: Valid, Invalid, or NotFound[62]. Using ROAs and BGP, networks can build routing tables while discarding invalid advertisements.

Figure 8: Collecting RPKI data to feed to BGP-speaking routers. Network operators need various components to make use of RPKI data.

4.3.2 RPKI-ROV notes

RPKI-ROV has residual vulnerabilities to certain types of scenarios or attacks. It must not be considered a complete solution but part of an overall program of complementary countermeasures.

RPKI-ROV has two main deployment components:

- Publishing ROAs about IP address space under administration.
- Using data published by others to validate BGP announcements received from other networks.

The two actions are not technically bound together; a given actor (address holder, network operator) need not implement in a particular order or can do one without the other indefinitely; the benefits realized only accrue based on what has been implemented. Indeed some networks have not published ROAs for legacy address space. This topic is discussed in greater detail a later section with the same title.

Coverage of IP address space by published ROAs has been growing steadily and is nearing 40% for both IPv4 and IPv6 in October of 2022 (up from under 10% five years earlier) [63]. While this statistic may give one sense of the relative protection afforded by RPKI-ROV, in a February 2022 estimate, the majority of traffic on the Internet is sent to destinations with BGP routes secured by ROAs[64].

A significant feature in the design of RPKI-ROV is that it does not require hardware upgrades to routers as it is not resource-intensive. Offloading potentially complex processing to the validating cache server(s) shields the routers from instability derived from such processing.

RPKI-ROV uses a “fail-open” model; specifically, RFC7115 [65] states that:

As origin validation will be rolled out incrementally, coverage will be incomplete for a long time. Therefore, routing on NotFound validity state SHOULD be done for a long time. As the transition moves forward, the number of BGP announcements with validation state NotFound should decrease. Hence, an operator’s policy should not be overly strict and should prefer Valid announcements; it should attach a lower preference to, but still use, NotFound announcements, and drop or give a very low preference to Invalid announcements.

The requirement to accept BGP announcements that are NotFound is critical for other aspects of system resiliency as well. Specifically, when a bootstrapping a router or set of routers, they must be able to fetch

8A BGP update is “valid” if prefix in the BGP announcement received by the router matches the origin ASN and its maximum length from at least one ROA that covers that address block. If it does not match, e.g., the origin ASN is different from the ROA, or the prefix is more specific than the maximum length specified, then the prefix is marked as “invalid.” If the prefix does not match any ROA, then it is marked as “NotFound.” More details can be found in the chapter “Using RPKI data” of the community maintained RPKI documentation.
the RPKI information and hence must accept routes by default. Likewise, if a router loses connection to its configured cache(s), it must be able to continue to function. Ability to reliably forward packets is more important than the improvements to reliability that are afforded by RPKI-ROV.

4.3.3 IRR Compared with RPKI-ROV

As mentioned earlier, published IRR data can be used to build inbound route filters to decide what advertisements to accept or ignore via a given BGP session. RPKI-ROV can check the validity of the origin AS of each BGP announcement coming across a session. Some limits and drawbacks include, but are not limited to:

- Some IRR data has a poor authorization model—information can be published other than by the authorized user of the IP address blocks in question.
- IRR data can become stale or can be the subject of “replay” attacks; it has no expiry date.
- Because IRR data is typically used with recursive expansion of each origin AS (or other AS-SET) within an AS-SET, filters can grow to hundreds or thousands of lines. There is no motivation to keep these bounds in check. Rather there is more incentive to be overly permissive—to make sure things work rather than prevent possibly unauthorized paths or origins.
- By itself, RPKI-ROV performs only a basic origin validity check but does not provide for more granular control of the flow of routing information. IRR data, however, can be used for enumerating components for filter generation.

4.3.4 BGP AS_PATH Validation

RPKI-ROV enables operators to filter BGP updates for specific prefixes that appear to originate from unauthorized ASes. Though RPKI-ROV can protect Internet routing from many misconfigurations and simple route origin attacks, it does not address the threat posed by more sophisticated attacks that modify the BGP AS_PATH attribute.

The path attribute in BGP describes the full sequence of connected networks that are transited to reach a given destination prefix; this is a key input into BGP routing and policy decisions for selecting a “best path” among multiple candidate routes. Such routing decisions can be as simple as choosing the route with the shortest AS_PATH, but often complex policies are applied to the AS_PATH to filter routes whose reported sequence of networks is in conflict with established business relationships or security policies.

Malicious actors can manipulate the AS_PATH in a BGP update message in various ways, including falsely adding new networks or deleting networks from the path to affect a variety of goals including these:

- Detour data traffic to eavesdrop, enable on-path attacks on end-to-end security mechanisms, and cause delays or disruption of traffic. Detoured traffic eventually makes it to the intended destination, but not over the intended path.
- Misdeliver data traffic to malicious endpoints.
- Manipulate routing through unauthorized BGP announcements as a foundation for cyber-attacks or the sending of spam.
- Deny service by “black-holing” entire networks so that others cannot reach them.
- Cause routing instability by injecting spurious BGP messages into the system that affect global BGP stability and control algorithms.

One obvious malicious path manipulation is to “forge the origin” of a BGP message, thwarting RPKI-ROV by inserting an authorized origin AS to the right of the actual (unauthorized) origin (Figure 9). It is thus important to understand that RPKI-ROV is vulnerable to this type of intentional attack.

To address these vulnerabilities in the currently deployed BGP infrastructure, the IETF has standardized a set of BGP and RPKI extensions, called BGPsec, to enable cryptographic protection of the AS_PATH attribute. These extensions are in the early stages of implementation testing and are not yet ready for production use. BGPsec enables receivers to perform BGP path validation (BGP_PV) by replacing the AS_PATH attribute of BGP4 with a BGPsec_PATH attribute[66]–[69]. The new path attribute includes a “secure path” element and signature blocks that provide authentication and integrity protection for the path data. Some more
technical details about BGPsec are included in the Appendices. While industry experts are actively working to ready BGPsec for general use, BGPsec is several years away from substantial uptake and the success of its adoption depends on operational experience gained through incremental deployment.

Another proposed approach to AS_PATH validation, that may be considered complementary to BGPsec, is Autonomous System Provider Authorization (ASPA)[18]. ASPA can automatically detect and mitigate invalid portions of the AS_PATH in announcements using a shared signed database of customer-to-provider relationships with a new RPKI object. ASPA is designed to mitigate route leaks, but it can also mitigate or reduce the negative impact of path-manipulation attacks. At the time of this report, ASPA has not been adopted as an IETF standard, so it remains to be seen whether it will be implemented.

4.4 BGP Session Security

The BGP protocol establishes a Transmission Control Protocol (TCP) session over which each adjacent pair of routers communicates, exchanging BGP routing information.

Some risks exist to the integrity and stability of the BGP session itself including TCP reset spoofing, in which an attacker sends TCP RST (reset) packets to a target with random sequence numbers[70]. If a reset packet with a valid sequence number is received by a BGP peer, there is no way to determine if the packet is from the legitimate peer or a spoofed source; the connection is reset, and the BGP session is terminated.

The general problem of spoofed source addresses is discussed in Section 4.5. Here we discuss some solutions specific to BGP sessions.

4.4.1 Transmission Control Protocol-Authentication Option

Transmission Control Protocol-Authentication Option (TCP-AO) adds authentication information to a TCP segment so that a receiver can ensure that the segment was sent from the proper source[71]. Implementation is relatively new and meant to replace Message Digest 5 (MD5) authentication, since MD5 has been deprecated[72]. TCP-AO addresses these concerns by using stronger cryptographic algorithms and implementing a better key management system.

4.4.2 Generalized TTL Security Mechanism

Generalized TTL Security Mechanism (GTSM) is a router control-plane protection mechanism[73]. It protects the router from a variety of potential attacks, such as CPU-exhaustion, by limiting traffic that can reach the BGP application.

By default, a BGP speaker sets the IPv4 Time To Live (TTL) or IPv6 Hop Limit (HL) to 1 when connecting to other external BGP speakers. Networks that peer with each other are directly connected, so a TTL or HL of 1 is logical—the devices are indeed one hop away. However, an attacker could nonetheless craft a packet such that the TTL reaches 1 when it arrives at the target router.

GTSM changes the logic by setting the TTL or HL to its maximum value of 255. The receiver is configured to filter any packet that arrives with a TTL less than 255. This dramatically reduces the range of devices
that can attack a router to those that are directly connected.

GTSM has been available for some time in many common router platforms. GTSM does require that the party on each side of the BGP session implement the configuration.

4.5 Source Address Validation

4.5.1 Spoofing of Source Addresses

The header of every packet on the Internet contains the address of the sender and the address of the destination. Routers use the destination address to decide how to get the packet closer to its destination. The source address is used by the recipient of the packet to know where to respond.

By default, routers do not examine the source address in a packet, since it contributes nothing to determining the best path to the destination. There is an implicit trust that the source provides truthful information about where the packet came from, and hence where the recipient should send replies. If the source address is wrong, then bidirectional communication fails because the destination responds to a machine which is not expecting the response and thus drops it. This is analogous to putting a return address on an envelope and dropping it in the mail: the post office does not verify that the return address is correct. The assumption is that the sender wants to receive a reply, which requires that the recipient know the correct return address. In an environment where people and devices are trusted, this generally is not a problem. In today’s Internet, we need to be more careful.

An attacker can exploit this lack of source address validation in several ways. The most common exploit is a DoS attack (Figure 10). An attacker can send packets to a host, but rather than include the correct source address of the originating machine, the source address is spoofed to be that of the target. The intermediate machine has no way to verify the validity of the source address, so it responds assuming it is legitimate and sends traffic to the target machine.

![Figure 10: Spoofed source address traffic flow. Denial of Service attacks often use spoofed source addresses to hide the true origin of the attack. A machine infected with malware sends traffic with the spoofed source address of the intended victim. The receiving machine may respond to the victim, sending it unsolicited traffic. Denial of Service attacks often use compact queries, which are designed to elicit responses of maximum size, amplifying the effect of the attack.](image)

The situation is worse when abusive traffic exploits UDP-based applications such as DNS and NTP[74]. It is possible for an attacker to send a small request to a legitimate DNS or NTP server and expect a very large response. For example, NTP servers have a feature called “get monlist,” which allows a legitimate requestor to ask the server for a list of machines that have recently contacted the server for time synchronization. The request is small, but the response is large. Exploiting this asymmetry is the key feature of such an attack.

Though this topic is not strictly related to the BGP protocol, it is an important aspect of traffic forwarding and suffers from similar ecosystem complexity and deployment challenges.

4.5.2 Source Address Validation to Protect Against Spoofed Packets

By default, routers do not validate that hosts are truthful with their source address in packets sent into the network. Several tools and techniques can be used to detect and mitigate this problem.
Source Address Validation (SAV), or “Best Common Practice 38”[8] is most effective when implemented as close to the source as possible[75]. SAV works by checking if the source address of the incoming packet matches what should (or could) be expected from the incoming interface: “Can I reach the source of this packet from the same interface on which it arrived?” The deeper into the network a packet travels, the larger the cone of valid source addresses, making SAV less effective.

Ideally, SAV is implemented on the first-hop router, where there is usually a single subnet per interface and the strictest filters can be put in place. There are two primary methods of implementing SAV: static access control lists (ACLs) and unicast Reverse Path Forwarding (uRPF)[75]. Access control lists are configuration statements implemented in a router to check characteristics of packets as they enter or exit a router. For SAV, a router checks the source address of each packet on an ingress interface and ensures that the source address is valid for that interface. A problem with ACLs for SAV is that they need to be tailored to each interface they are applied to, because different addresses will be valid with respect to each interface. Automation can help with this, but for an operator with thousands of router interfaces, implementation and maintenance is challenging. Also, depending on the internal hardware and software design of the router platform, performing such processing can be computationally challenging.

An alternative to ACLs is the more dynamic uRPF. This method uses the information learned from the routing table to determine if a router would send traffic to the source address of packets over the same interface on which they arrived. Though easier to implement than ACLs from a management point of view, uRPF can suffer from performance problems (as with ACLs) and also topology constraints[76]. Because the Internet is highly interconnected and redundant, multiple valid paths may exist between source and destination. Therefore, when applied away from the edge of the network uRPF can become so permissive as to be nearly ineffective. Standards have been proposed to enhance uRPF to give operators more options to deploy it, but router vendor support remains limited to principally Cisco[77].

Deployment of SAV is a collective-action problem. Operators that deploy SAV help ensure that their networks are not the entry point of spoofed packets. The beneficiaries of this effort are almost entirely other network operators. Therefore, it is critical that a majority of operators take the effort to ensure that spoofed packets are dropped as close to the entry point to the network as possible. SAV was first proposed in the IETF in January 1998, and was enshrined as a Best Common Practice in May 2000, yet today, more than two decades later, deployment of SAV continues to be limited principally to larger networks.

Measurement and detection of effective SAV generally requires operators to deploy test points within their network. CAIDA’s Spoof project has produced open-source tools that test and report on the effectiveness of SAV filtering techniques[78]. Using this tool, operators can run both ad-hoc and scheduled tests to check the effectiveness of SAV measures. However, performing exhaustive tests is infeasible because it scales with the number of the network’s edge interfaces. In a service provider network this may require tens of thousands of interfaces to be checked.

5 Challenges of Adoption and Future Direction

5.1 A Collective-Action Problem

The routing ecosystem is too complex for us to expect a unitary solution, or one that involves just a few entities. It is a global environment in which small changes in distant places create ripples throughout the world. Taking the YouTube incident as an example, there is only so much YouTube could have done to protect itself. It was up to Pakistan Telecom or its upstream provider to block this fake announcement and save YouTube, or for other networks on the path to do the same, which is what transpired. This illustrates the fact that solutions exist, but need to be applied at scale by many of the networks participating in the global routing system.

Improving routing security cannot be achieved by simply updating the BGP routing protocol. Such changes need to be deployed, which means asking ISPs to incur costs, sometimes significant since they require redesign or replacement of legacy network management systems. Deployment of these measures only marginally contributes to the protection of the ISP, because its security is to a significant extent in the hands of other
networks. Furthermore, the network operators and other entities (software and hardware vendors, RIRs, etc.) that constitute the Internet span a variety of jurisdictions and business models.

In “Why Information Security Is Hard,” Ross Anderson argues that, contrary to the common view that information security comes down to technical measures, “many of the problems can be explained more clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons”[79]. The challenge of security of global interdomain routing can be described as a collective-action problem, in which the participants understand that they are better off providing a solution but fail to produce a concerted action because of conflicting interests or lack of incentives. Norms help overcome similar situations in other circumstances. They do so when the desired behavior is clearly understood and agreed and the parties involved are willing to cooperate, driven by common activities and objectives. Mutually Agreed Norms for Routing Security (MANRS) is an example of an effort to foster concerted action by convening stakeholders across the Internet ecosystem to discuss, aggregate, and publicize routing security standards and best practices.

5.2 Non-Technological Factors

To this point we have alluded to non-technological factors that challenge the deployment of improvements to routing security. Most so far involve added costs with unclear or unquantifiable return on investment or first-mover or collective-action problems. To provide a complete picture of the routing security landscape, more specific discussion of non-technological factors is warranted.

5.2.1 RPKI Software Ecosystem

ROV is currently the only RPKI-based security functionality used operationally. The five RIRs support it, there is open-source software available for the creation, publication and use of data, and all major router vendors and many open-source projects have implemented support for RPKI-ROV with BGP. In this section, we review the state of this software ecosystem.

The five RIRs each use their own CA software implementations, one of which has been open-sourced recently (RIPE NCC). Several NIRs operate RPKI services as a child Certificate Authority (CA) under their RIR. The NIRs all use one of two open-source solutions, one of which has not been actively maintained since 2018.9 Network operators most often use their RIR or NIR’s portal to manage ROAs in a CA which is managed by the RIR or NIR—this model is often referred to as a “hosted RPKI system.”

Most, but not all, RIRs and NIRs allow operators to run their own delegated CA system (Figure 11). One NIR (nic.br) does not offer any hosted RPKI service, instead requiring that operators run their own CA.10

There are five relying-party software implementations in widespread use, all of which are open-source[80]. Some projects are actively developed, while others appear to be no longer maintained. There is more

---

9 Community-maintained lists of CA software, RP software, RTR server software and router support are available as part of the RPKI documentation.
10 Details on RIR and NIR interactions are summarized as part of the documentation for the Krill CA software.
Several router vendors participated in the development of the RPKI standards in the IETF, ensuring the technology offered an end-to-end solution for route origin validation. The RPKI to Router protocol (RPKI-RTR) was specifically designed to deliver validated prefix origin data to routers. RTR, as well as origin validation functionality, has been available in various hardware platforms and software solutions.

5.2.2 Reliable Funding for Internet Infrastructure Software

Operators implementing routing security measures need to be able to rely on mature implementations that are supported during the lifetime of operation. Contrary to what is usual in other sectors, much fundamental Internet infrastructure software is available free of charge.\(^{11}\) Though this by no means precludes operational or capital expenditure for operators, it does mean that funding for developers is not tied to the use of their software. In the absence of income from use, many professional developers working on Internet infrastructure software rely on either donations and grants or income from paid feature development or support. Some developers function as a cost center within a larger organization.\(^{12}\) The decoupling of funding and use allows for the whole world to depend on software that is sustained by few.\(^{13}\)

We illustrate the relevance of this imbalance between funding and use to routing security with two examples. Out of an estimated 2,000 installations of the Routinator RP software and 1,400 networks using the Krill delegated CA software, fewer than ten fund their development.\(^{80}\)\(^{13}\) The majority of operators do rely on the stability, continued existence and future development of the software, but do not contribute to this end.

There is a disconnect between buying network equipment with expensive support contracts and failing to fund the open-source software upon which, in many cases, that very equipment is dependent. Often, technical staff at network operators are willing to support development, but their corporate structure does not let them because such software is not something one can purchase in a shrink-wrapped box with a support contract. Sponsoring the development of a feature can be problematic, because the default assumption by legal departments is that software development results in the sponsor owning the intellectual property, which is incompatible with the free and open-source software model (Figure 12).

Figure 12: Society’s dependence on free and open-source software, as illustrated in the XKCD cartoon referring to the Java Log4j library. Dependency, Copyright 2021, Randall Munroe, CC BY-NC 2.5.

Several questions arise from this reality. In the absence of stable income for developers, who can network operators expect to pick up the phone when bugs are found or support is required? Though free and open-

---

\(^{11}\) This includes operating systems, databases and service daemons for DNS, routing, time synchronization and the web. We focus on routing security here.

\(^{12}\) A good example of open-source software sustained as a cost center within a larger organization is BIRD, a project used for route servers at some Internet exchange points. It is developed and funded by the Czech top level domain registry, cz.nic, from unassociated domain-registration revenue.

\(^{13}\) Funding figures and estimates of Krill CA usage provided by NLnet Labs.
source software allows for modification and shared problem solving, development and long-term maintenance of software is specialized work.\textsuperscript{14} What is acceptable risk to society of fundamental software going unmaintained from lack of interest or funding, in the face of collective dependence on Internet connectivity? Is funding to be solved within the multistakeholder model for Internet governance\textsuperscript{82}? Is it a matter for the operators to take care of their software supply chain? Or is there some role for the public sector? We argue that reliable funding for Internet infrastructure software is an unsolved problem. In the absence of a clear answer, it is up to operators to think about diversity and continued sustainability of routing security implementations, in particular when these are available for free as open-source software.

5.2.3 Legacy Address Space

For a network operator to create ROAs, it needs an agreement with one of the five RIRs. This poses a problem for some users of IPv4 address space in the United States. Approximately 35% of the address space in the ARIN region (USA, Canada, and the Caribbean) consists of “legacy” delegations, predating the existence of the RIR system, and not yet covered by a Registry Services Agreement (RSA) or Legacy Registry Services Agreement (LRSA)\textsuperscript{83}. The issue of legacy space is not unique to the ARIN region, but the vast majority of legacy space is now under ARIN’s purview.

The early Internet deployments were experimental or designed to support scientific research. Even the most optimistic predictions during this development phase did not envision the pervasive nature of today’s Internet. According to Vint Cerf:

So I said 32 bits, it is enough for an experiment, it is 4.3 billion terminations–even the defense department doesn’t need 4.3 billion of anything and it couldn’t afford to buy 4.3 billion edge devices to do a test anyway. So at the time I thought we were doing an experiment to prove the technology and that if it worked we’d have an opportunity to do a production version of it. Well… it just escaped! It got out and people started to use it and then it became a commercial thing\textsuperscript{84}.

Under the circumstances, initial management of IP number resources was informal, with records being kept on paper\textsuperscript{85}.

During this time, the network was expanding globally, and various standards bodies proposed regional registries to provide resource management\textsuperscript{86} \textsuperscript{87} \textsuperscript{88}. Réseaux Internet Protocol Européens (RIPE) was established in 1992 and now serves Europe. APNIC was established to serve Asia and Oceania in 1993. ARIN was established in 1997 and now serves for the United States, Canada, the North Atlantic islands, and much of the Caribbean. LACNIC (Latin America) was split from ARIN in 1999, and AfriNIC consolidated the African continent from portions previously served by ARIN, RIPE, and APNIC in 2004.

The establishment of the RIRs created a problem: how to deal with resource allocations that predated the existence of the RIRs.

ARIN agreed to provide services that existed at the time of its establishment to resource holders in its service region. Specifically, registration and directory services (WHOIS) and reverse DNS, are key functions provided to legacy holders. RPKI ROA management and RIR -operated IRR databases are newer services that are unavailable for resources not covered by an RSA. Though third-party IRR databases exist, the RPKI cryptographic root of trust is in the RIRs, so there is no alternative way to create ROAs. Resource holders must enter into a contractual agreement with a regional registry in order to realize the protection for their resources that RPKI-ROV might afford.

Many legacy resource holders have been reluctant to enter a formal agreement with an RIR due to concerns that doing so may negatively impact either their use of the resources or their financial obligations in the future \textsuperscript{89}.

\textsuperscript{14}The routing world has always relied on extensive personal communication between operators to solve operational issues. In the context of this report, routing security software is security software in a space of evolving standards. Developers need to actively track standards development and adapt to real-world use. They need to reliably maintain and support their implementations for long-term stable use by network operators.
5.2.4 AFRINIC Situation

Threats to the Internet routing architecture need not attack routers directly; they can be directed against higher-level targets such as the routing protocol standardization process (as in the Chinese government’s attempts to get remote packet inspection capabilities included in the BGP protocol definition[90] [91]). The RIRs, which manage unique allocation of ASNs and IP addresses, can also be imperiled. As of the date of this report, AFRINIC, the African Regional Internet Registry, has for more than two years been under legal challenge by a Chinese-held hosting company. This firm and its proxies are holding more than six million disputed IPv4 addresses, with a present market value of more than $360 million. They have opened a series of forty-six legal actions against AFRINIC in the Mauritius courts, succeeding in, among other things, temporarily freezing AFRINIC’s accounts and halting AFRINIC’s board meetings and elections[92] [93]. This type of activity can pose an existential threat to the continued operation of Registry functions vital to the operation of the Internet and to improvements to routing security[94] [95].

6 Observations

This paper reviews many shortcomings in BGP and provides examples of these shortcomings causing problems, through either malicious action or simple mistake.

- The problem of ensuring reliable interdomain routing is complex and doing so on a global scale requires that we rely on information from remote and unknown sources.
- The Internet’s routing table is essentially crowd-sourced, built in a multiplicity of independent instances by each of tens of thousands of individual network operators. The result is a globally shared resource and a common good.
- The Internet routing system’s capacity to respond dynamically to change and its freedom from any central point of failure are great strengths, yet they also pose concomitant risks.
- Though most routing security incidents appear to be unintentional, some are clearly malicious. Attributing intentionality is difficult, but security improvements make the Internet more resilient to both intentional and unintentional misrouting.
- Routing security incidents have not constituted an existential threat to the Internet, nor have any rendered the Internet generally unusable; nonetheless, it is important that we pursue continuous improvement.
- There are a multiplicity of applicable security practices. Many are technologically complicated to implement and maintain, and many result in increased fragility of already complex systems.
- There are many parties with roles to play in securing the Internet’s routing system and this report makes many recommendations, but not all recommendations are applicable to all parties.
- Efforts to improve routing security suffer from a collective-action problem: most improvements cannot be deployed unilaterally, and most protect others more than they protect the party that implements them. First-movers often realize little immediate benefit from the costs and risks they bear.
- BGP is one of the most mature Internet protocols. Its simplicity has been a strength, rendering it flexibly adaptable to more than three decades of changing demands. Changes to the BGP protocol proceed at a deliberate pace and this judiciousness reflects the inherent complexity of making changes to a global system consisting of millions of routers operated by tens of thousands of independent organizations, each of which bear their own costs and risks.
- Though innovative work has been done on future communications protocols which include their own routing mechanisms, it is not realistic to imagine a wholesale replacement of BGP within the context of the current network. New routing protocols will most likely emerge in conjunction with a new global network, not within the context of the Internet[96]–[98].
- The tens of thousands of networks that constitute the Internet operate under diverse legal systems and business models. For this reason, no top-down prescriptive approach is possible, nor could it hope to achieve the degree of global harmonization that the Internet routing community already achieves voluntarily[7].
- Progress has been made by building on areas of consensus such as the reliance on Regional Internet Registries (RIRs) and commitment to a shared and reliable routing commons.
• Internet governance is a global, multistakeholder process, which takes place in many fora and venues including the IETF and other standards bodies, the various regional and sectoral Network Operator Groups (NOGs), RIR community meetings, and a multiplicity of email lists and discussion fora.
• The standardization process is a success. It is an open, global, multistakeholder governance process that has identified problems and proposed an array of adaptable complementary solutions.
• The development and global deployment of new technologies in the operational network may take decades, and this is inherent in the complexity of the process, not a sign of failure.
• Though there have been many proposals to improve routing security, some of which have been abandoned, this demonstrates a strength of the process and governance model, not a weakness.

7 Recommendations

7.1 General Recommendations

Ultimately, sound routing security relies on the effective translation of the aforementioned technologies to their operational practice. IP address and autonomous system number holders must actively maintain information in public repositories that describe their intended routing policy. Network operators must actively retrieve this information to configure the behavior of their networks to be consistent with the published policy.

For networks of moderate size or larger, the machinery to fetch, generate, and apply public routing policy must be automated. Though not as dynamic as the Internet BGP routing table, these public routing policy attestations are not static, and best practices require network behavior to be updated on at least a daily basis.

Network operators also need to provide mechanisms to ensure that their users have visibility of how the networks are interpreting published routing policy. For example, if a network is rejecting routes due to ROV or inconsistencies with IRR databases, that information needs to be accessible to the affected parties.

The systems that support routing security ought not be considered auxiliary to business-critical systems; rather, routing security must be an integral part of the overall operational environment. An organization’s operational practice should also include ensuring that its customers and peers are aware of its implementation of routing security, and of how they can best leverage its practices to better protect their networks. For example, customers may benefit from an organization’s practices when its routes have covering ROAs. (More detailed operational considerations related to RPKI appear in the Appendices.)

7.2 Recommendations to Network Operators

The term “network operators” may typically be thought to refer to ISPs. Here we use the term broadly to include any entity that operates a computer network connected to the Internet. This encompasses not only ISPs but also CDNs, cloud computing providers, as well as enterprise networks, both commercial and noncommercial.

• Explicitly include routing security in their operating plans and procedures, to ensure the security and resilience of their Internet-connected information systems and services. When systems rely on external Internet services (e.g., cloud computing, content distribution, monitoring, security services), contracts should explicitly define routing security requirements.
• Enroll Internet number resources (i.e., Internet protocol addresses and Autonomous System Numbers, ASNs) in applicable Resource Public Key Infrastructure (RPKI) services, such as those of RIRs, reviewing and executing any agreements necessary to participate in those services.
• Issue RPKI route origin authorizations (ROAs), which use cryptographic signatures to associate their Internet address blocks with the ASNs of the networks authorized to announce them.
• Implement RPKI route-origin validation (ROV) in their BGP infrastructure and ignore any BGP routes ROV determines to be invalid.
• Maintain IRR information including route, as-set, and possibly aut-num types to allow for IRR-based route filtering.
• Ensure the continued financial support of diverse open-source routing security software to ensure the life cycle of enhancements and bug fixes.
• Contribute to routing data collection efforts—such as PCH, RIPE RIS, and Route Views—and to open platforms for routing security analysis by providing data and event validation.
• Although not strictly related to routing, network operators should apply source address validation to packets entering their network, where technically feasible, to lessen the risk from source address spoofing[8].

7.3 Recommendations to Policy-makers

• Respect and encourage the multistakeholder standards development and collaboration processes of the Internet operational community. Unilateral, or even multilateral regulation may have negative consequences as operators attempt to comply narrowly with regulation. To the extent that regulation is considered, set goals and outcomes rather than specifying technology, and encourage and support the multistakeholder standards process to develop solutions.
• Work with the Internet community to address the regional policy and incentive issues that slow the adoption of standardized routing security technologies (see 5.2.3).
• Fund long-term monitoring programs for Internet routing. The data commons of Internet routing information for analysis, monitoring, and study should be considered necessary infrastructure for transparency and health of the routing ecosystem.
8 Appendices

8.1 KLAYSwap Cryptocurrency Attack

The 2022 attack against the Korean cryptocurrency exchange KLAYswap demonstrated the viability of BGP attacks to undermine the security of common web-based applications.[99] The attack on KLAYswap exploited several vulnerabilities and web development patterns of KLAYswap’s cryptocurrency exchange web app. Although KLAYswap was the victim of the adversary’s overall attack, it was not the target of the adversary’s manipulation of BGP. The adversary used BGP to hijack the IP address of a server that belonged to Kakao and was hosting a specific piece of javascript code used by the KLAYswap platform (Figure 13). The adversary’s objective was to serve a malicious version of this code file that would ultimately cause users of the KLAYswap platform to transfer their cryptocurrency to the adversary’s account unknowingly. However, like MyEtherWallet, KLAYswap and Kakao were using TLS, so without the adversary presenting a valid certificate to complete the TLS connection the adversary’s code would not be loaded. This did not stop the adversary; it used an attack known in the research community in which, after launching the initial attack, it requested a certificate from a CA for the domain name of Kakao’s server that was hosting the javascript file[[100]]23.

![Figure 13: KLAYswap vulnerability. In the 2022 attack against cryptocurrency exchange KLAYswap, the attacker hijacked the BGP prefixes of KLAYswap’s service provider Kakao, substituting a route to the attacker’s server.](image)

CAs operate under guidelines intended to deter the issuance of malicious certificates. These guidelines require the CA to verify that the party requesting the certificate has control of the domain names in the certificate[101]. One of the approved verification methods involves contacting the server at the domain through an unencrypted HTTP connection and verifying the presence of a specific piece of content requested by the CA (this cannot be done over an encrypted and authenticated connection since the party requesting the certificate may be requesting a certificate for the first time).

During the attack, when the CA attempted to verify domain ownership, its request was routed to the adversary’s server because of the BGP hijack. This falsely led the CA to believe the adversary was the legitimate owner of the domain and caused it to issue a certificate to the adversary. The adversary then completed the attack by using this certificate to establish an “authenticated” connection with KLAYswap users and serve its malicious code. Ultimately $2 million was stolen from KLAYswap users over several hours.

8.2 RPKI Ecosystem and Operational Considerations

We have covered the differences between IRR and RPKI and the use of ROAs to filter routing information based upon origin validation. The following subsections discuss considerations for RPKI-ROV deployment by various actors including network operators, measurement and monitoring providers, and publication point operators.

Implementation of RPKI-ROV involves multiple actors. The roles required of each party depend on how RPKI is implemented by the resource owner or network operator. There are four main components to the
ecosystem: certification authorities (CAs) that perform the RPKI enrollment and access control functions and maintain the scoped hierarchy of resource certificates used to digitally sign RPKI data objects; publication points that store and provide remote access to RPKI and supporting meta data; and, RPKI validating caches (VCs) that download global RPKI data, validate the signatures on the signed objects, and provide BGP routers with a distilled summary of the validated RPKI data.

As noted in section 5.2.1 both the certificate authority and publication point components can be implemented in a hosted model in which those functions are provided by the relevant RIR, or a network operator may choose to implement a delegated model in which they operate subordinate RPKI CAs and publication points themselves. Hybrid models (in which the network operator maintains its own RPKI CA but publishes the resulting RPKI data in the RIR’s publication point) have been made available by some RIRs.

The RPKI CAs and the publication points should be considered critical infrastructure. The authentication, integrity, availability and timeliness of the data they provide can have significant impact on the security and stability of global Internet routing. Given their importance, it should be assumed that these services will be subject to focused attacks that attempt to corrupt, forge or deny access to their data. The underlying information systems should be engineered using the best practices for scalable, highly available public facing Internet services.

There are multiple dimensions to consider with respect to the performance of an RPKI ecosystem. The frequency at which RPKI objects (e.g., ROAs) are updated, the validity period of signed objects, the frequency at which publication points make available changed RPKI data, the frequency at which VCs poll publication points for updated RPKI data, and the frequency at which routers poll caches for updates to the resulting validated RPKI data.

There are obvious tradeoffs in several of these dimensions, for example shorter validity periods and more frequent updates reduce the window in which stale data might be used by routers downstream in the RPKI ecosystem. But having shorter validity periods might also result in the expiration of RPKI data should a publication point become unreachable. Likewise, the more frequent the update of publication points, and the polling of data by VCs and routers, the more responsive the end-to-end system becomes to changes in the RPKI data (e.g., the demand driven turn up of new ROAs authorizing a DDoS mitigation service to announce routes to a targeted prefix). But having more frequent updates and polling creates more load on the components producing and consuming the data.

8.2.1 RPKI Measurement and Monitoring Practices

Given the complexity of the overall RPKI ecosystem, the multiple actors and technologies involved, and the range of potential resilience and performance issues involved, it is important to measure and monitor the behavior of the component systems, the data produced and its impact on the global routing system. In the sections that follow we examine some measurement and monitoring recommendations for different aspects of RPKI operations.

8.2.2 ROA Creation

When a resource owner creates ROAs, it is important to check if the published RPKI objects match routing intent. ROA creation is often a manual process or scripted from other network policy or configuration data sources. As such, there is a possibility of ROAs being created that don’t actually align with the intended routing policy or that policy having unintended impacts on the global routing system.

For this reason, it is important for RPKI CA operators to provide users feedback on the potential impact of ROA creation before actual creation and publication of the ROA objects. Of particular importance would be flagging BGP announcements in the existing routing tables that would become invalid if the ROA was created.

RPKI users should monitor the RPKI-ROV status of routes to their own address prefixes and routes that originate from their own autonomous system. Any changes in RPKI-ROV status should be alerted for further analysis.
8.2.3 Operating RPKI Validating Cache Software

When running RPKI Validating Cache software, the operator should ensure that it is up to date (to fix bugs and security issues), and that the software is receiving the expected number of RPKI objects from remote publication points and that RPKI updates are propagating properly through the system. Given that the global RPKI data is constantly changing, monitoring should focus on alerting if there is a significant change in the number of objects received from each publication point or on an aggregated per RIR basis.

The RPKI specification requires manifests that enumerate the complete list of objects contained at each publication point[102]. Operators should monitor the validating caches error logs for failures to connect to specific publication points, or mismatches between published manifests and the objects retrieved from a given publication point.

While measures of significant changes in the number of objects received is a less definitive signal of problems in the system, error logs of publication connection failures or manifests and data mismatches is a clear signal of operational issues that should be investigated.

8.2.4 Operating RPKI Publication Points

The availability and performance demands on entities operating RPKI publications points are significant. Even a short unavailability of a publication point is visible to third parties throughout the Internet that are running RP software. And given that two protocols (RPKI Repository Delta Protocol (RRDP) and rsync) are used to deliver RPKI data to its users, two services (with slightly different meta data) need to be monitored.

Though rsync is reliable, it is an older protocol with a less natural model for scaling and monitoring. Rsync also lacks server authentication, making it relatively easy to impersonate a server. This does not threaten the integrity of the RPKI— all data is cryptographically signed making it really difficult to forge data—but it is possible to withhold information or replay old data[103]. There is little native monitoring available for rsync infrastructure. One approach available is to screen scrape logs and expose metrics from these.

Publication points have two major aspects they can monitor. First, they should observe that the published information matches what is expected, and that this information is being updated. This can possibly be done using a backend system (for example, a CA system) as a source of truth for the intent of what is published.

The second aspect is the consumption of objects by RPs. A publication point can detect (transient) unavailability either by requests from monitoring infrastructure being rejected or by detecting a drop in the rate of requests, as well as an increase (after RRDP issues) of fallback to rsync connections.

8.2.5 Operating RPKI Certification Authorities

This report does not focus on CAs. The most important role of the CA is to ensure that objects the CA intends to distribute are effectively published and up to date. This can be done with two monitoring components: checks that objects are current, and, for example, manifests are not close to expiry; and, checks that the objects that are published (i.e., visible to RPs) match the data within the CA. This second check provides on the pipeline from the internal CA data to the publication of RPKI objects.

8.2.6 Monitoring Approach

These monitoring steps can be automated or performed manually. The best practice for parties running RPs is to monitor for liveliness. An RP operator likely also wants to investigate the RP logs when alerted, because any component (CA, publication point, RP) can be the root cause of a problem. Many monitoring systems use metrics similar to or compatible with Prometheus, with various RPs (routinator, octorpki, rpki-client with third-party code), supporting software (stayrtr, rtrmon), and multiple CA implementations (Krill and RIPE NCC) providing metrics in this format.

Though any party running an RP can alert on many root causes, the operator should ensure alerts are actionable for the party receiving them. In practice, this means that a party that runs an RP may not want to have alerts for minor issues. A good guide for alerts is Ewaschuk’s article on his philosophy for alerting[104].
As mentioned above, the availability of publication points and CAs is more important than that of an RP. Issues with a publication point affect and are visible to third parties. Because of this, at a minimum, publication points should be to monitor the availability (from multiple topological perspectives) of the repository, as well as measure protocol usage to detect issues (e.g., detect RRDP issues by noticing fallback to rsync).

Large-scale publication points and CAs (e.g., RIRs or major network operators) should have 24x7 monitoring and be reachable to report issues. Worldwide (topological) visibility is hard. In practice, real issues (e.g., a single CDN point of presence not receiving updated files) have been detected by a third-party monitoring systems. It is recommended that large-scale publication points also have fallback infrastructure available, such as a secondary CDN that is not active by default, to mitigate issues in the third-party components they use for object publication.

A RPKI repository publishes data used for improving security of Internet routing. A typical RPKI repository is made up of CAs and authoritative publication point servers that make RPKI object data available to all relying parties. Much like the DNS name space, the RPKI data can be delegated, in this case from a “parent” CA to a “child” CA and served by a different PP server.

In practice, the five RIRs each operate top-level PP servers consisting of RPKI object data associated with the IP address blocks and AS numbers they administer. However, in the “delegated” model described above, resource holders may wish to publish RPKI data on a different PP server of their choosing—in which case the location of the server for the “child” RPKI data is among the information served by the PP for the “parent” CA. Since to have a complete view of “the RPKI data” RPs must acquire all RPKI signed objects from all PPs, the performance, availability and integrity of all PPs is of utmost importance. Otherwise, the time it might take for an RP to converge or reach completion could be compromised. In practice, the process of gathering all the data and processing the integrity checks to arrive at a finished “run” is on the order of minutes. An underperforming PP could negatively affect such convergence[105] [106].

PP server operators should deploy systems with high availability and integrity in mind. Redundancy, DoS protections, and service monitoring are just some of the well-known considerations for any PP server system deployment. RP software and client operators should also be designed and deployed to handle transient problems or extended PP outages gracefully. Some emerging approaches have borrowed from the content-delivery paradigms used for web and other data such as caching, replication, and load distribution.

If a PP becomes unavailable or the RPKI data it publishes is unreliable, security of Internet routing associated with that data is at risk. At best, validation of object data may not be possible. At worst, incorrect object data may lead to undesirable routing system decisions. Today, the currently relatively small number of PP servers, numbering in the dozens globally, are loosely monitored by a variety of organizations, but there is a lack of consistent RP client software behavior and best current practice guidelines for PP operators.

### 8.3 BGPsec details

The BGPsec secure path element is similar to the AS_PATH of BGP but is encoded to collapse duplicate adjacent ASes within a path (the result of AS-path-prepending) and includes a per-hop flag used to support operations within BGP confederations. The signature block includes a Subject Key Identifier (SKI) and a signature for each AS in the secure path element. The signatures added by BGPsec-enabled routers when announcing a route to a neighboring AS are a signed hash computed over elements of both the secure path and signature block elements, the prefix being announced and the target AS the update is being sent to. BGPsec routers must be provisioned with the private keys necessary to create the outbound signatures, and the corresponding public keys must be embodied in resource certificates published in the RPKI. Such key pairs may be unique to a given AS, or even unique to individual routers.

BGPsec-enabled routers that receive updates with BGPsec_PATH elements are able to validate that each of the signatures found in the update and label the entire update as being either “valid” or “not-valid.” For each hop in the secure path, a BGPsec receiver uses the SKI to select the correct public key from data provided

---

15 Including in the hash the AS number of the peer the route is about to be announced to, prevents cut-and-paste attacks that replay BGPsec updates to other unintended peers.
by an RPKI-validating cache and computes and validates the same signed hash function as the transmitter. Local BGP policies determine how the validation result impacts the local decision process (e.g., if not-valid updates are ignored or de-preferenced when selecting a best path).

There are many other details of the design of the BGPsec protocols that can be examined in the cited references. Some other key attributes of the protocols worth noting include these:

- The capability to use BGPsec between two peers is negotiated during the establishment of each BGP session.
- Each BGPsec update includes only a single prefix to avoid the complexity of packing and unpacking prefixes along a path.
- A BGPsec Path must be contiguous and complete—that is, the protocol does not support partially signed paths. Thus a BGPsec update must be signed when originated and can propagate only across eBGP peering sessions that have negotiated the use of BGPsec.
- When a BGP router needs to forward a BGPsec route to a peer that does not support BGPsec, BGPsec_Path attribute is stripped and replaced by an unprotected BGP4 path attribute.
- The BGPsec protocol is designed to support multiple cryptographic algorithms.

Although the IETF BGPsec standards have been complete for approximately five years, adoption by commercial router vendors has been lagging. To some extent this represents the natural evolution of the industry gaining comfort and experience with the global RPKI infrastructure and BGP origin validation first, before moving forward with the commercialization and deployment of path validation technologies. Having said that, it should be recognized that BGPsec represents a more complex change to the global BGP infrastructure than origin validation. Unlike origin validation, BGPsec requires several changes to the syntax and semantics of the BGP protocol “on the wire” and requires routers to store larger messages (e.g., the signature blocks) and perform more computationally demanding operations (e.g., generating and validation cryptographic signatures) than are currently required by current BGP.

Multiple BGPsec prototypes, reference implementations and test tools exist and research has been done to both characterize and optimize the memory and processor impact of BGPsec processing in Internet routers; nevertheless, concerns remain regarding the potential performance impact on legacy routers of wide scale deployment[107]–[110]. Despite recent growing interest among network operators and policy-makers in BGPsec path validation, until commercial vendors and key open-source routing platforms offer robust and scalable BGPsec implementations, operational deployment will remain limited[111].
Glossary

ACL (Access Control List) Device configuration (typically on a router) that permits or blocks packet data based on a specified characteristic such as protocol, source or destination address, or combination of such characteristics.

ARIN (American Registry for Internet Numbers) The Regional Internet Registry (RIR) serving North America, Caribbean, North Atlantic, along with Antarctica, Bouvet Island, Heard and McDonald Islands, and St. Helena.

AS (Autonomous System) A collection of routing infrastructure and blocks of IP addresses under the coordination and management of a common administrative entity that presents in BGP a defined set of routing policies and resources (i.e., prefixes) to the Internet. Each AS is assigned a unique Autonomous System Number that identifies it in BGP routing. Examples of ASs include the networks operated by enterprises, Internet service providers, and content distribution networks.

AS_PATH (Autonomous System Path) An attribute of the BGP protocol that encodes the sequence of autonomous systems that have announced or forwarded the route to the current BGP receiver. In general, the AS_PATH indicates the sequence of networks that should be traversed to reach a given prefix if the route was selected as the “best path” to the destination. The AS_PATH is a key input to the BGP decision process and is typically used in policy enforcement (e.g., to filter routes based on their path) and to optimize route selection (e.g., by choosing routes with shorter paths).

ASN (Autonomous System Number) A numeric identifier (16- or 32-bit) used in BGP to identify a specific Autonomous System (e.g., AS 1234)

ASPA (Autonomous System Provider Authorization) A proposed extension to RPKI standards currently under development to enable networks to declare the complete list of their authorized transit providers. This information can be used to detect and mitigate some forms of route leaks and to enhance the robustness of other filtering mechanisms (see SAV).

BGP (also specified as BGP4) (Border Gateway Protocol) The standard protocol to exchange routing and reachability information among ASes on the Internet. The information carried in BGP allows routers to choose the “best path” to a given block of destination addresses based on the AS_PATH, and local policies configured by each network operator.

BGPSec (BGP Security) An extension to BGP to enable path validation by adding digital signatures to the AS_PATH as BGP messages pass through ASes. BGPSec relies on the RPKI for creation and distribution of the keying material necessary to validate these signatures.

Black Hole Used as a verb, to denote the routing of a packet to a router’s “null interface,” which has the effect of deleting the packet, or “dropping” it. Both “black hole” and “drop” (from “drop on the floor”) are colloquialisms for the most CPU-efficient action that may be taken to discard a packet due to a violation of policy, as it traverses a router.

CA (Certificate Authority) In public key cryptography, the Certificate Authority is the organization that acts as a trusted third party to validate identity and sign and issue digital certificates to entities. Relying parties (i.e., users of the PKI) typically configure the CA’s public key as a trust anchor to bootstrap the ability to validate the hierarchy of certificates issued to its enrolled entities.

CDN (Content Distribution Network) A system to distribute content (such as video, large software updates) as geographically close to users as possible. CDNs improve performance and reliability by minimizing the amount of fallible network between a user and the content they wish to retrieve.

DNS (Domain Name System) The distributed and decentralized service that translates domain names (such as www.bitag.org) to the IP addresses that are used to locate and route data to a system or service.

DoS/DDoS (Denial of Service/Distributed Denial of Service) An attack designed to disrupt or interfere with legitimate access to a resource such as a website by overwhelming network or computational...
resources. A Distributed DoS involves many machines distributed around the Internet contributing to such an attack, thus making defense or mitigation difficult.

**Filter List** Router configuration that permits or blocks the outbound transmission of routing data, or the inbound integration of received routing data into the local routing table, based on a specified characteristic such as prefix or AS_Path content, or combination of such characteristics.

**HL (Hop Limit)** IPv6 equivalent of IPv4’s Time To Live.

**HTTP(s) (HyperText Transfer Protocol (Secure))** An application layer protocol that was originally designed to enable exchange of hypertext documents on the world wide web. Today there are many other uses of HTTP including providing the APIs, data transport for micro-services, and device configuration. HTTP is unencrypted and unauthenticated, whereas HTTPs utilizes TLS encryption and authentication to protect the conversation.

**IANA (Internet Assigned Numbers Authority)** The IANA coordinates the Internet’s globally unique identifiers, including IP addresses, ASNs, protocols, and the root of the domain name system.

**IETF (Internet Engineering Task Force)** The international standards development organization that develops and publishes the specifications that define the Internet protocol suite and related applications.

**IRR (Internet Routing Registry)** A database of network addressing, topology, and policy information that can be used by network operators to assist in configuration, control, and troubleshooting of Internet routing.

**ISP (Internet Service Provider)** A network operator that offers Internet access to customers.

**IXP (Internet Exchange Point)** The sites of Internet bandwidth production, where network operators interconnect to exchange customer routes and traffic. Most IXPs are noncommercial consortia of the participating network operators, and most IXPs exist within single metro areas. As of 2022, there are approximately 750 IXPs active in 151 countries[112].

**LIR (Local Internet Registry)** In some regions, RIRs allocate blocks of number resources to subtending registries that handle resource management in a subsection of the RIR’s region.

**LRSA (Legacy Registration Services Agreement)** A variant of the ARIN RSA clauses that can apply to so-called legacy resources issued to organizations prior to ARIN’s incorporation[113]. Though at one time the LRSA was a distinct document, today LSRA issues are addressed in the base RSA document and the clauses differ only in the fee structure.

**MD5 (Message Digest 5)** A cryptographic function to produce a 128-bit hash that can be used to validate data. Originally specified in 1991, it is now considered problematically weak for many uses and has been broadly deprecated.

**MiTM (Machine in The Middle, or sometimes Man in The Middle)** An attack in which communications are redirected to a machine that would not normally be privy to the flow of traffic, and which impersonates each of the authentic parties to the other. Once insinuated into the path of communication, such a machine can be used to capture or modify traffic. In the context of routing security, see “route-hijack.”

**NIR (National Internet Registry)** While APNIC and LACNIC principally allocate addresses directly to LIRs, they also allocate blocks of number resources to subtending national registries in some countries, which then further sub-allocate to LIRs within those countries. ARIN, RIPE, and AFRINIC do not entertain subsidiary NIRs. LACNIC deals with only two NIRs, in Mexico and Brazil, which predated its existence, while APNIC actively certifies new NIRs.

**NRO (Network Resource Organization)** The organization of the five Regional Internet Registries (RIRs), in which common issues related to Internet number registration are coordinated.

**NTP (Network Time Protocol)** A messaging system which synchronizes computer system clocks across the Internet.
Packet  The fundamental unit of data communications, each packet contains a header, which includes the source and destination addresses and the information necessary to direct and interpret the packet, and a payload, which is the data that users or applications are trying to communicate. The Internet’s routing system operates on packet headers, and does not examine or act upon information in the payload.

Path-manipulation  The unauthorized modification (addition or deletion) of AS_PATH data in a BGP update that can result in denial of service, delivery of data to unauthorized destinations, or unintended modifications of the forwarding path between two communicating systems. Examples of path-manipulations include (a) forging the first (origin) AS in the AS_PATH to subvert RPKI-ROV, and (b) deleting elements in the AS_PATH to impact path selection by other networks. Note that path-manipulations can occur as result of accidental misconfigurations or of malicious attacks.

Peering  One of the two forms of interconnection between networks, the other being “transit.” In a peering relationship, network operators exchange only customer routes (and therefore traffic) but not the routes (and traffic) that they learn via transit. Peering is cost-neutral (no money is exchanged between the parties) and is used at the Internet exchange points at the center of the Internet’s topology. Only one peering relationship exists in any routed path between two points in the Internet, at the “center” of that path, while transit relationships lead “downward” in both directions from the peering relationship to each endpoint.

Prefix-manipulation  The unauthorized origination, or modification, of the Network Layer Reachability Information (NLRI, also commonly referred to address prefixes) in a BGP update that can result in denial of service, delivery of data to unauthorized destinations, or unintended modifications of the path between two communicating systems. Note that prefix-manipulations can occur as result of accidental misconfigurations, or malicious attacks. Likewise, the unauthorized origination or modification of BGP prefix data can occur by the origin (i.e., first) network in the AS_PATH or any subsequent AS that forwarded the route.

RADb (Routing Arbiter Database, subsequently Routing Assets Database)  A popular commercial IRR operated by Merit Networks.

RFC (Request For Comments)  A series of numbered documents that establish Internet standards; managed by the IETF.

RIPE NCC (Réseaux Internet Protocol Europeens–Network Coordination Centre)  The RIR that serves Europe, the Middle East, and Central Asia.

RIR (Regional Internet Registry)  The five regional multi-stakeholder Internet governance organizations responsible for managing the assignment of IPv4 and IPv6 addresses and ASNs. RIRs also maintain RPKI and reverse DNS services for the number resources they manage. The five RIRs are AFRINIC (Africa), APNIC (Asia-Pacific), ARIN (US, Canada, and portions of the Caribbean), LACNIC (Latin America and portions of the Caribbean) and RIPE (Europe and the Middle East) Together they form the Number Resource Organization (NRO).

ROA (Route Origin Authorization)  A data object in the RPKI created and digitally signed by address block owners to enumerate the ASes that are authorized to announce BGP routes to these destinations.

Route-bijack  The malicious or accidental manipulation of BGP information such that either data is delivered to an improper destination or the normal data path between two destinations is altered in ways that compromise confidentiality, privacy, policies, or optimal routing. Such events can result in DoS, loss of data confidentiality, impersonation attacks, data manipulation, and abuse of resources such as address blocks.

Route-leak  The propagation of BGP routing announcements beyond their intended scope—other words, an announcement from an AS of a learned BGP route to another AS in violation of the intended policies of the receiver, the sender, or one of the ASes along the preceding AS path. Route-Leaks are commonly the result of misconfigurations and often result in unintended changes in the routes used to forward data. Often these changes lead to loss of connectivity because they specify paths that either violate policy filters or congest the newly-selected path.
Route origin manipulation The unauthorized origination of address prefixes in a BGP update that can result in denial of service, delivery of data to unauthorized destinations, or unintended modifications of the path between two communicating systems. Note that route origin manipulations can occur as result of accidental misconfigurations, or malicious attacks.

RPKI (Resource Public Key Infrastructure) A special-purpose public key infrastructure and repository system that permits the detection of accidental routing misorigination. In the RPKI ecosystem, root CAs operated by RIRs issue digital certificates to verified owners of blocks of IP addresses and ASNs and operate repositories to store data objects digitally signed using those certificates.

RPKI-ROV (Route Origin Validation) A BGP route filtering process that uses distilled data from RPKI ROAs to check if the origin (i.e., first autonomous system in the AS_PATH) is authorized to announce routes to a given prefix.

RPKI-RP (RPKI Relying Party) Software used by network operators to collect data from global RPKI repositories and perform X.509 validation on their contents (e.g., ROAs, Resource Certificates).

RPKI-RPA (Relying Party Agreement) An agreement, either explicit or implicit, that may be required by RIRs for RPs to use the TALs. The RPA limits the liability of the RIR in the event of harm experienced by a relying party as a consequence of their use of RPKI.

RPKI-TAL (Trust Anchor Locator) In the RPKI, the Trust Anchor Locator is a file used by RP software to bootstrap the process of retrieving the ROAs and other cryptographic objects needed to perform ROV.

RPSL (Routing Policy Specification Language) The standard that defines the type and format of objects used in an IRR database.

RSA (Registration Services Agreement) A contract between an RIR and a network operator or other resource recipient that details the rights, responsibilities, and limitations governing the allocation and use of Internet number resources.

SAV (Source Address Validation) Process by which a router examines the source address of an incoming packet and determines if it is permissible to receive packets from that source on the specific interface on which it arrived. SAV is used to mitigate the effects of spoofed packets.

TCP-AO (Transmission Control Authentication Option) A standard that adds cryptographic information to TCP traffic to allow for message authentication (checking to ensure the senders is trusted). Designed to replace MD5 by providing stronger cryptographic functions.

Transit One of the two forms of interconnection between networks. In a transit relationship, the “upstream” network operator provides a full set of BGP routes, reflecting reachability for the entirety of the Internet, to the “downstream” customer network, typically in exchange for payment. Peering is the other form of interconnection between networks.

TTL (Time To Live) A counter of how many routers an IPv4 packet has passed through. TTL is set by the originator of a packet; each router decrements this counter, and when it reaches zero the packet is discarded. This mechanism prevents routing loops, which traffic to go in circles. See also Hop Limit (HL) for IPv6.

uRPF (Unicast Reverse Path Forwarding) Check A mechanism used by routers to determine if the source address of an incoming packet is valid or spoofed by checking the routing table to see if the address can be reached using the interface on which the packet arrived (see SAV).
References


Report Contributors and Reviewers

- Maria Adamczyk, AT&T
- Maarten Aertsen, NLnet Labs
- David Belson, Cloudflare
- Henry Birge-Lee, Princeton University
- Jay Borkenhagen, AT&T
- Ken Calvert, University of Kentucky
- Rich Compton, Charter
- Alberto Dainotti, Georgia Institute of Technology
- Amie Elcan, Lumen
- Nick Feamster, University of Chicago
- Andrew Gallo, George Washington University
- Brad Gorman, ARIN
- Ties de Kock, RIPE NCC
- John Kristoff, Netscout
- Barry Latch, SkyUK
- Nimrod Levy, AT&T
- Jason Livingood, Comcast
- Doug Madory, Kentik
- Doug Montgomery, NIST
- Jennifer Rexford, Princeton University
- Andrei Robachevsky, Internet Society
- Arturo Servin, Google
- Barbara Stark, unaffiliated
- Matt Tooley, NCTA
- Steve Wallace, Internet2
- Greg White, CableLabs
- David Winner, Charter

Editors

- Doug Sicker, BITAG
- Tony Tauber, Comcast
- Bill Woodcock, Packet Clearing House