Identifying Current Barriers in RPKI Adoption

Cecilia Testart[1], Josephine Wolff[2], Deepak Gouda[1], and Romain Fontugne[3]

[1]Georgia Institute of Technology
[2]Tufts University
[3]IIJ Research Laboratory

September 2024

Abstract

Society increasingly relies on the Internet as a critical infrastructure. Inter-domain routing is a core Internet protocol that enables traffic to flow globally across independent networks. Concerns about Internet infrastructure security have prompted policymakers to promote stronger routing security and the Resource Public Key Infrastructure (RPKI) in particular. RPKI is a cryptographic framework to secure routing that was standardized in 2012. In 2024, almost 50% of routed IP address blocks are still not covered by RPKI certificates. It is unclear what barriers are preventing networks from adopting RPKI. This paper investigates networks with low RPKI adoption to understand where and why adoption is low or non-existent. We find that networks' geographical area of service, size, business category and complexity of address space delegation impact RPKI adoption. Our analysis may help direct policymakers' efforts to promote RPKI adoption and improve the state of routing security.

1 Introduction

In the past two years, policymakers have grown increasingly focused on network and routing security. Concerns about routing security have prompted policymakers to take steps to try to protect the Internet infrastructure society relies on for commerce, communications, and connectivity by promoting stronger routing security. For instance, in April 2023, the Dutch government announced it would upgrade the security of all of its networks' routing infrastructure by the end of 2024 [6]. Also in 2023, the United States government released a new National Cybersecurity Strategy that included an objective to "secure the technical foundation of the Internet," in particular by taking "steps to mitigate [...] Border Gateway Protocol vulnerabilities" [33]. Even more recently, in June 2024, the Federal Communications Commission released a Notice of Proposed Rulemaking looking at whether broadband service providers would be required to prepare plans to mitigate routing security risks and then report on their progress in implementing those plans.

Motivated in part by these efforts to use policy to drive routing security, this paper considers how policymakers can best help or incentivize network operators to improve their routing security, and which organizations they should focus these efforts on, in light of differing adoption rates. Fundamentally, this paper seeks to help identify which organizations are

lagging when it comes to implementing routing security best practices, and how policymakers may best be able to assist those lagging organizations in overcoming various obstacles to implementation, or otherwise enable their adoption of those security practices.

Policymakers' growing emphasis on network security reflects the fact that inter-domain routing is a core Internet protocol that enables traffic to flow globally across different independent networks, or autonomous systems. However, the de facto protocol designed to enable that function—the Border Gateway Protocol (BGP)—has a critical vulnerability: it lacks a built-in mechanism for validating the information that networks share and use to select global routes for data traffic. This means that when networks decide where to send online traffic, they often have no way of verifying that they are sending it to a network that can properly deliver that traffic to its intended address. This creates an opportunity for networks to accidentally or deliberately try to intercept traffic by pretending they will be able to deliver it to its intended destination.

This is a major security problem, sometimes called BGP hijacking, that has enabled several serious incidents during which large portions of Internet traffic have been misdirected, potentially allowing for surveillance, espionage, or other forms of interference [11, 21, 22, 26, 30]. BGP re-routing has also repeatedly enabled cryptocurrency theft and fraudulent traffic [9, 10, 20, 32].

In 2012, the Internet Engineering Task Force (IETF) standardized the Resource Public Key Infrastructure (RPKI), a framework for networks to issue cryptographic records that can be used by other networks to validate data in BGP, effectively ensuring that online traffic could not be hijacked in this manner [17]. In recent years, many industry players have agreed that validating BGP data with RPKI records would improve routing security [5]. In fact, almost all Tier 1 transit providers currently filter out BGP messages with invalid data according to RPKI records [18]. However, networks need to issue RPKI records for the entire IP address space they use in order to fully benefit from RPKI protection.

In 2024, about 50% of IP address blocks advertised in BGP are still not covered by RPKI records despite the longstanding awareness of this security risk. Moreover, when looking at the address space originated by each network in the Internet, RPKI coverage is not uniform. There are several factors related to networks and the address space they use that may influence RPKI adoption. These include the geographic region the network operates in, the size, and the business category. However, it is still unclear what specific barriers are preventing certain networks from issuing RPKI records, as networks may experience varied challenges in their adoption process.

For policymakers to effectively support RPKI adoption and help organizations reach higher levels of adoption, they need a better understanding on how to target adoption efforts to specific groups of organizations that are struggling with RPKI implementation, as well as the particular barriers they face. This paper investigates networks with low RPKI adoption to understand where and why adoption is low or non-existent, and what approaches might be most effective in trying to promote adoption more widely. We study the characteristics of networks that are lagging to identify critical barriers that may be limiting RPKI adoption. Our empirical analysis is based on publicly available routing data, RPKI and Internet resources' delegation data from the Regional Internet Registries, and data from network operators' databases.

We find that there are four key characteristics that impact organizations' RPKI adoption levels: geography, network size, business category, and the complexity of the address space.

The geographic heterogeneity we believe results from the fact that the Regional Internet Registries (RIRs) have independently implemented the process and requirements for issuing RPKI records and, as a result, the levels of adoption vary across the geographical zone each RIR covers. Additionally, the size of a network is an important factor because RPKI requires additional management and operation, and smaller networks have a harder time adding that to their regular operations. Furthermore, networks from organizations unrelated to Internet services, such as educational and government networks, have even less awareness of RPKI and fewer incentives to adopt it than organizations with closer ties to online services. Finally, even for large networks, all IP addresses are not equal in terms of the effort required to issue RPKI records for them. There are legal and operational challenges linked to the delegation and sub-delegation of address space that may make RPKI adoption harder for some portion of address space they use.

2 Background

2.1 How RPKI works

The Resource Public Key Infrastructure (RPKI) is a framework to secure routing by providing an off-band system to validate information in BGP [17]. Currently, the framework allows network operators to register cryptographic records to assert which network(s) can originate which address blocks in BGP. For RPKI to work, there are two set of actions that need to take place:

1. Holders of address space need to register cryptographic certificates following the RPKI process to protect the IP address blocks they hold. These certificates are called Route Origin Authorizations (ROAs) and provide the Autonomous System Number (ASN) of the network authorized to originate the IP address block(s) in BGP. These records provide a cryptographically verifiable mapping between IP address blocks and origin network.

2. Networks need to use the RPKI ROA certificates to validate information in BGP, filtering invalid messages and effectively preventing the spread of invalid information. This step is referred to as Route Origin Validation (ROV) and it involves discarding any routes that according to RPKI records, appears to be fraudulent, hijacked or even just accidentally incorrect.

The combination of the two step above, namely the existence of the cryptographically verifiable mapping that then allows networks at large in the Internet to validate the information in BGP, are need to reduce the spread of routing misconfigurations and hijacks, preventing traffic delivery to the wrong network and host. Hence, both aspects of RPKI are essential to improve routing security.

However, without the initial step, *i.e.,* registering RPKI certificates mapping IP address blocks to the network authorized to use them in BGP, even if most transit providers are filtering invalid BGP messages (step 2), organizations do not benefit from RPKI. Indeed without the registration step, it is impossible to identify invalid messages related to IP blocks not found in RPKI. Additionally, *all* organizations holding IP address blocks need to issue RPKI certificates to benefit from the increased adoption of this framework, independent

of organization size, place in the Internet topology or main business activity. Therefore, organizations whose networking teams primarily focus on providing connectivity for their internal needs, such as enterprises, utility company, hospitals and educational organizations, have to implement and deploy a suitable management process for issuing RPKI certificates. For these reasons, this paper focuses on the adoption of the first step for RPKI to work: the issuance of RPKI certificates covering IP address blocks routed in BGP.

Another important reason for focusing on the first step—the issuing of RPKI certificates—is that currently many large transit providers are already carrying out the second step by validating BGP data using RPKI records [4]. Almost all Tier 1 networks validate routing data. Indeed, a case study by network observability company Kentik found that during a route leak in August 2023, most RPKI-invalid routes from the leak were seen by less than 15% of RouteViews BGP collectors [15]. As such, if IP address blocks are covered by an RPKI certificate, invalid BGP messages related to those address blocks would have limited spread in today's Internet. In other words, organizations can really benefit and reduce their exposure to intended hijacks and unintended routing misconfigurations by issuing RPKI certificate to protect their IP address blocks.

Throughout this paper, when we discuss RPKI adoption, we specifically refer to the steps involved in the issuance of Route Origin Authorizations. To issue ROA certificates, the following considerations are relevant:

- Only the documented organization holders of IP address blocks according to one of the five Regional Internet Registries (RIRs) or to further delegation records, can issue RPKI certificates for those address block.
- To issue RPKI certificates, organizations have to follow the process determined by the RIR that delegated the address block.
- ROA certificates are cryptographically signed by different *signing engines*, however, organizations cannot always choose the engine, it depends on the relevant RIR and further delegations of address space. Signing engines allow varied levels of automation.
- If an organization was delegated address space before the existence of RIRs, the organization has to follow the process of the RIR assigned to the organization geographical zone. This process usually involves legal steps. This address space is referred to as *legacy* address space.
- An RPKI certificate may be issued for an IP address block, a.k.a. *prefix*, that has been further delegated and more specific prefixes are also routed. The RPKI certificate may cause routes to more specific prefixes, called *subprefixes*, to be invalid unless RPKI certificates are issued for those subprefixes.

In this paper, as further explained in section 3, we study RPKI adoption as the proportion of address space originated by a network that is covered by RPKI ROA certificates. Depending on the delegation status of address space, there might be address blocks for which the network originating them in BGP might not have the ability to issue ROA certificates for them. We still include that address space for adoption considerations. The rationale for this is that all networks originating address space must have a business relationship with the holders of address space if it is not themselves and can therefore play a key role in encouraging and facilitating RPKI adoption.

2.2 Related Work

Many studies have investigated RPKI Route Origin Authorizations (ROA) coverage of the IP address space [3, 7, 8, 12, 13, 19, 29, 34, 35]. Some works have studied RPKI coverage as an initial step to analyze the impact of Route Origin Validation (ROV) [13] in routing, to detect BGP hijacking [34], and to evaluate the overall readiness of the RPKI framework to improve routing security [3, 7]. Other studies have focused on specific characteristics, uses, and challenges in the issuance of ROA certificates [8, 12, 19, 29]. In 2015, [35] studied RPKI adoption by the hosting infrastructure of popular websites. Together, these works have emphasized the benefits of the RPKI framework, its readiness despite the slow adoption, and have issued recommendations on specific configurations and uses to reduce misconfigurations and increase protection.

However, RPKI adoption in practice is not only influenced by technical characteristics of certificates, but by all aspects involved in an organization's adoption of RPKI and issuance of ROA certificates, from the legal processes to the routing operations. For instance, [36] studied the legal barriers to RPKI adoption and explored potential means of trying to lower those barriers. Prior efforts studied RPKI adoption at an Internet- or RIR-wide level, without considering distinctions between networks and organizations behind specific address space and RPKI certificates. As a consequence, these studies provide limited visibility into specific barriers in the adoption process. In a study of RPKI adoption in the web ecosystem, only the popularity of a website was considered as a factor explaining adoption of the hosting infrastructure [35].

Furthermore, prior studies were conducted many years ago, before major transit network providers started using RPKI data to perform Route Origin Validation (ROV), and before the pandemic stressed the relevance of hygiene in the routing ecosystem. Indeed, the studies that issue recommendations to encourage RPKI adoption date from 2012 [34], 2015 [35, 13], 2017 [7, 8], and 2019 [3, 36]. As NIST's RPKI monitor shows, in August 2024, 52% and 54% of routed IPv4 and IPv6 address blocks respectively have adopted RPKI [24]. As such, we are not in the early adoption phase of RPKI.

In this paper, we study in depth characteristics of networks that impact the level of RPKI adoption, now that RPKI has proven to be the next step to strengthen routing security. We hope to better understand the types of obstacles that different organizations face, and how policymakers can best tailor their efforts to strengthen network security to different target organizations.

3 Data, Methodology and Pre-Processing

This empirical work uses publicly available data of core Internet protocols and the information from organization associated with the number resources, *i.e.,* IP addresses and network Autonomous System Numbers (ASNs), present in those datasets. The next section describe our sources and main methodology to infer RPKI adoption at the level of IP address blocks and then at the network level.

	IPv4		IPv6	
	Jan '19	Aug '24	Jan '19	Aug '24
Unique routed IP prefixes	781,613	1,170,482	63,197	258,071
Valid ROA certificates	59,874	482,192	10,111	112,882
RPKI covered prefixes (%)	96,021 (12%)	611,262 (52%)	10,462 (17%)	153,464 (59%)

Table 1: Dataset counts for routed prefixes, RPKI ROA certificates, RPKI coverage (% of RPKI adoption). Routed prefixes do not consider IP address blocks not intended to be routed globally.

3.1 Data sources

To study RPKI certificates adoption, we use two publicly available datasets that provide a global view into the routed address space and the valid RPKI certificates. First, we leverage the routing data from globally deployed BGP collectors from RIPE RIS [25] and RouteViews [28]. Second, we use RIPE NCC's Validated ROA Payload (VRP) [31], which provides a list of the cryptographically valid RPKI ROA certificates updated daily. Table 1 shows the count of routed prefixes and valid RPKI ROA certificates fetched at the beginning and end of our measurement window.

To analyze network characteristics, we integrate several datasets relevant to Internet resources. First, to geolocate networks by Autonomous System Number (ASN), we use delegation files published daily by RIRs [27]. To geolocate IP address blocks, we use the Maxmind dataset, made available through the Internet Health Report [14]. To evaluate a network size, we use CAIDA AS Rank [1] which provides the customer cone size, *i.e.,* the number of networks that are customers and customers of customers of a network.

3.2 Inferring RPKI adoption

To infer the RPKI status of routed prefixes, we follow the procedure described in the reference standard document from the IETF, RFC 6811: BGP Prefix Origin Validation [23]. Using datasets fetched on the same day, we consider that a given block of IP address space —a prefix— has adopted RPKI if there is a valid RPKI ROA certificate with *(i)* a prefix covering the IP address block[1] and *(ii)* with the authorized origin network in the certificate matching the origin of the IP address block in BGP.

3.3 RPKI adoption from the network perspective

Many networks have RPKI certificates that cover some of the prefixes they originate but not all of them. Indeed, routed prefixes originated in BGP do not need to exactly match the ones included in ROAs. Operators often de-aggregate prefixes in smaller address blocks for traffic engineering purposes. In addition, routed prefixes may have overlapping address space to facilitate the operation of large transit networks and reduce the size of the global routing table.

[1]Prefix A is covered by prefix B if the set of IP addresses A represents is entirely found in B. A can be equal to B or A can be a subset of B's IP addresses.

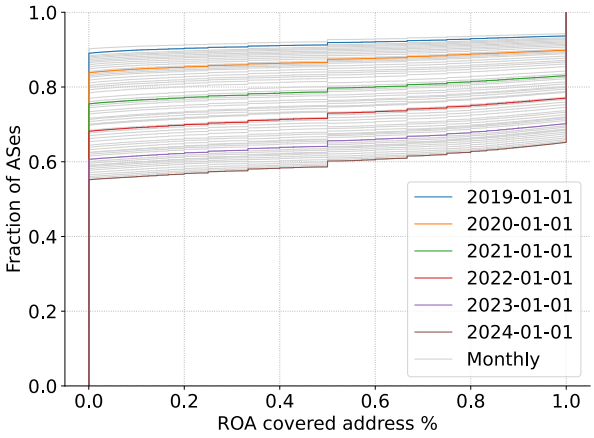


Figure 1: Cumulative Distribution Function of networks by the percentage of RPKI adoption of routed address space.

We compute the share of address space originated by a network that has adopted RPKI, *i.e.,* is covered by ROA certificates, by first computing the size of the routed address space originated by each network, identified by the Autonomous System Number (ASN). Then, we compute the share of that address space that is present in RPKI, meaning that a valid certificate has a covering prefix.

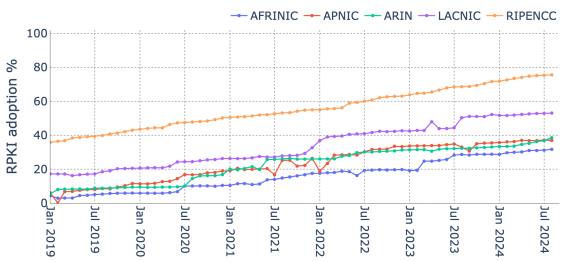
The distribution of networks by level of RPKI adoption has a bimodal behavior that is consistent over time: most networks either have no/low adoption or full/high adoption. Figure 1 shows the Cumulative Distribution Function (CDF) of networks (ASNs) by RPKI adoption level.[2] Each line represents a different month, from January 2019 until January 2024. Every year, there are very few networks in *partial* adoption and most have either very low or very high adoption. Networks adopting RPKI for at least one routed prefix increased from about 10% in 2019 to almost 45% in January 2024.

We note that our analysis is based on routed prefixes and RPKI data, which provides a meaningful view of RPKI adoption in IPv4. Unfortunately, these metrics are not the most appropriate to assess the state of RPKI adoption in IPv6. Given the size of the IPv6 address space and routed prefixes, even small IPv6 prefixes can be divided in thousands of subnets. Thus, neither prefix size nor count of addresses relate to the share of active subnets in an IPv6 address block. Therefore, neither the share of IPv6 prefixes nor the share of IPv6 address space present in RPKI provide a useful and representative level of adoption. We leave to future work to find better metrics to study RPKI adoption in IPv6.

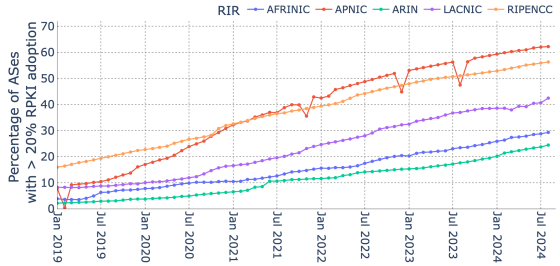
4 Results

In this work we are interested in understanding RPKI adoption from the perspective of networks that route traffic towards the end hosts in IP address blocks. To do so, we study RPKI adoption by the network that is at the origin of BGP path toward IP address blocks. From this perspective, the level of adoption of a network is the share of address space that the network originates that is covered by RPKI records (see section 3.3 for more details).

[2]IPv4 space is shown, IPv6 has similar results



(a) RPKI adoption by address space.



(b) RPKI adoption by networks

Figure 2: RIR RPKI adoption

	IPv4		**IPv6**	
RIR	Total %	RPKI adoption %	Total %	RPKI adoption %
AFRINIC	5.05	28.26	5.82	7.72
APNIC	27.43	36.87	28.80	43.45
ARIN	38.68	32.04	14.00	76.40
LACNIC	6.90	47.30	8.81	57.21
RIPENCC	21.94	72.97	42.57	68.95

Table 2: Percentage of routed prefixes and RPKI adoption by RIR for IPv4 and IPv6.

4.1 Geographic influence on RPKI adoption

Regional Internet Registries (RIRs) are the root of trust to verify the cryptographic validity of RPKI records. Each RIR has independently set up the process to issue and publish ROAs in their region. As a consequence, RPKI adoption has followed different trends.

RIRs have significant differences in the level of RPKI adoption and it varies by IP version (IPv4 vs IPv6). Table 2 summarizes the statistics of the routed prefixes and RPKI adoption per RIR. RIPE, covering Europe and Middle East, is a clear leader in RPKI adoption and AFRINIC is the zone with lower adoption in both IPv4 and IPv6. ARIN, the North-American zone considerably lags behind in RPKI adoption for IPv4. However, even if IPv6 is significantly less prevalent in ARIN than in other RIR zone, ARIN is a leader for RPKI adoption in IPv6.

Moreover, when looking at RPKI adoption by address space and networks in the past 5 years, we find that different types of networks have been driving RPKI adoption for different RIRs. Figure 6 shows RPKI adoption at RIR-level over time, from the perspective of address space (Fig. 2a) and from perspective of networks (Fig. 2b) for IPv4. Combining the trends from both graphs, we can infer how much of the address space in each RIR has adopted RPKI and the share of networks that have contributed to that adoption.

A striking difference by RIR is the size of the routed space of networks driving RPKI adoption in their zone. In RIPE, ARIN, and LACNIC zones, RPKI adoption is driven by networks routing large amounts of address space, as a smaller share of networks represents a larger share of RPKI covered address space. In particular, in ARIN less than 25% of network have more than 20% of their routed address space covered by RPKI ROAs, but that represents close to 32% of all ARIN's IPv4 address space. In contrast, in APNIC, network-wise adoption is higher than address-wise adoption, with more than 60% of networks exhibiting

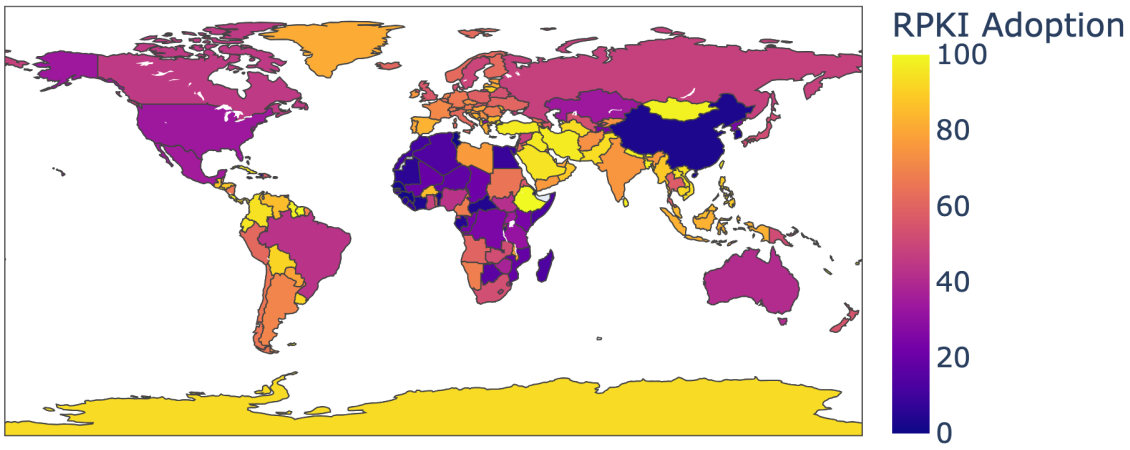


Figure 3: RPKI Adoption of Countries in August 2024; Middle-east nations have the highest RPKI coverage, while China has the lowest coverage among large nations

adoption rates of more than 20%, but that 60% represents only about 40% of the APNIC address space. Finally in AFRINIC adoption levels are similar from both perspectives.

Even within RIR regions, the adoption of RPKI is not homogeneous across countries in the same RIR zones. We use IP geolocation data to assign IP address blocks to a country and study their RPKI status in January 2024. Figure 3 reveals the level of RPKI adoption by country.

In the RIPE zone, which includes the Middle East, most countries have over 50% adoption of RPKI. We attribute this success to RIPE's community efforts to train and promote RPKI adoption as well as the development of tools for RPKI certificate issuance and management. Furthermore, Middle Eastern countries including Israel, Turkey, Iraq, Iran, Lebanon, Oman, Saudi Arabia exhibit more than 90% RPKI adoption. We hypothesize that either due to market concentration of network operators at a country level, or due to concerns about the increase of BGP hijacking attacks impacting those countries, most network operators in those countries have very high levels of adoption. Conversely, Italy and Kazakhstan are the only countries in the RIPE zone with lower RPKI adoption of 34% and 12% respectively.

In Latin America and the Caribbean, the LACNIC zone, most countries have more than 80% RPKI adoption. For LACNIC, we hypothesize that proactive initiatives led by LACNIC, training and pushing RPKI registration, have been helpful in getting most countries ahead in RPKI adoption [16]. Two notable outliers are Mexico and Brazil, both with less than 40% adoption of RPKI ROAs. Then, RPKI coverage is almost null in Haiti, we could only find a single ROA certificate covering address space in Haiti.

In APNIC, there are large countries in the two extremes of RPKI adoption. On the one side most countries have over 50% adoption, which we attribute to the APNIC efforts to support RPKI adoption with training and outreach activities. On the other side, China and South Korea have almost no adoption of RPKI. China, despite originating the second largest address space on IPv4 and largest in IPv6, has only RPKI certificate covering 2.4% and 1.8%

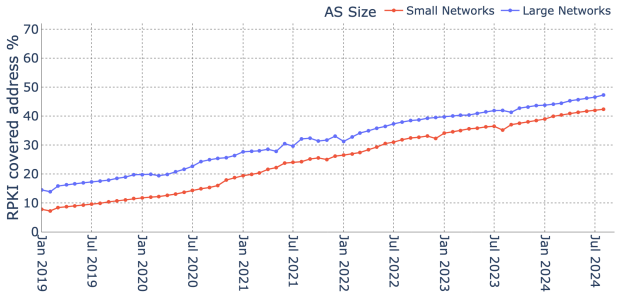


Figure 4: IPv4 RPKI Coverage of prefixes originated by top 10 percentile and bottom 10 percentile ASes (by amount of address space originated); Larger ASes consistently have a higher ROA coverage.

of routes for IPv4 and IPv6 respectively. French Polynesia also has very low adoption of RPKI (11%), which contrasts with the very high RPKI adoption in Metropolitan France (over 80%).

In the ARIN zone in North America, the countries with the largest amount of address space by far are the US and Canada, with 35% RPKI and 61% RPKI adoption, respectively. This makes the US one of the countries with large address space with the lowest level of RPKI adoption. Most Caribbean Island have over 50% adoption of RPKI. One notable exception is Jamaica, which has no RPKI coverage.

Finally, in AFRINIC, most countries with large address space has low levels of RPKI adoption. We hypothesize that the challenges with AFRINIC organization, finance and legal situation have impacted RPKI adoption. However, there are some large countries with significant RPKI adotpion such as Kenya (58%), Ghana (79%), Côte d'Ivoire (79%), Angola (59%) and Mauritius (96%).

We note that globally, there are a few countries with 100% adoption of RPKI (bright yellow in Figure 3). Upon investigation we find that those countries have very few prefixes located within their borders. As an example, Christmas Island and Falkland Islands have 2 and 3 prefixes respectively and a 100% RPKI coverage. In countries with the largest amount of address space, we find Taiwan, Iran, and Bangladesh have the highest percentage of RPKI adoption, with the address space covered by ROAs exceeding 98% for each of them.

The next sections look at other characteristics of networks impact RPKI adoption even for networks within the same region.

4.2 Small Network Challenges with RPKI Adoption

Geographic differences in RPKI adoption indicate that size impacts adoption. To study the impact of network size in RPKI adoption, we categorize networks by the size of address space they host publicly on the Internet. We use the IPv4 prefixes networks originate in BGP to decide whether a network is in the largest 10% of networks in an RIR zone and globally, and consider it a large network accordingly. We consider small networks the ones that originate a single prefix in BGP, representing about 35% of networks globally, 18-42% of networks in each RIR. For Figure 4 depicts the RPKI adoption (share of RPKI coverage) for large and small networks globally. We also compute the same metric for each RIR zone.

Globally, our data analysis reveals that large networks have been driving RPKI adoption

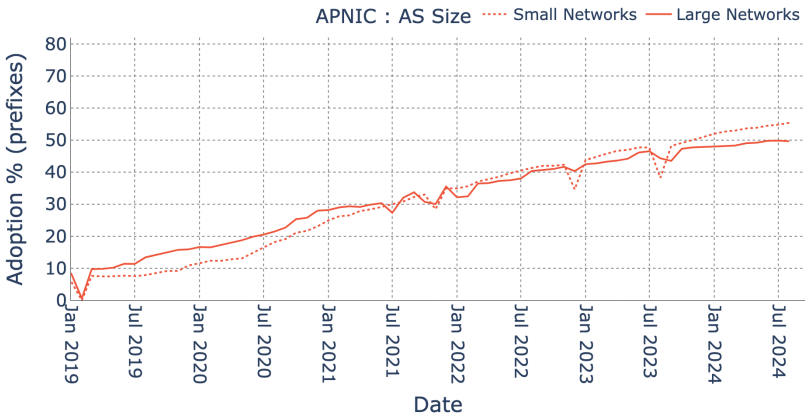


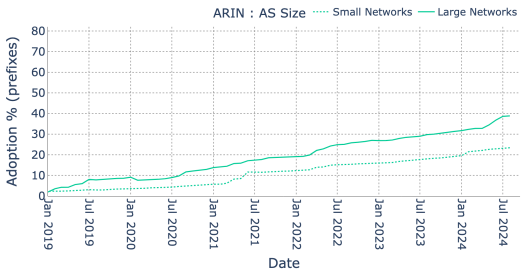
Figure 5: RPKI adoption in APNIC for large (top 10 percentile) and small (bottom 10 percentile) networks has followed a similar trend in the past 5 years

from the start. Large networks started adopting RPKI earlier and still have higher levels of adoption. At the time of writing, more than 50% of IP address space routed by large networks has adopted RPKI, whereas small networks adoption is still bellow 45%. We argue that in general, larger networks have more resources, larger network engineering teams and have more awareness of new technology, reducing the barriers to RPKI adoption. On average, small network adoption level is lagging one to two years behind the adoption rates of large networks, but the differences vary significantly by RIR zone.

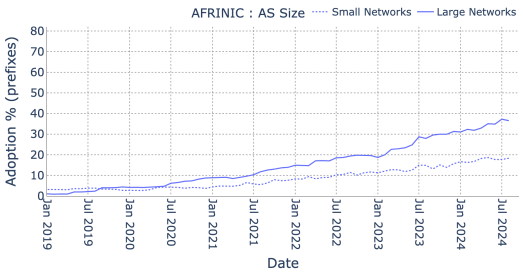
The APNIC zone is an exception with respect to the size of networks driving RPKI adoption. In all RIRs except APNIC, large networks have notably more RPKI adoption than smaller networks. In contrast, in APNIC, small networks started RPKI adoption at the same time and have followed a similar trend. Figure 5 depicts RPKI adoption for large and small networks in the past 5 years for APNIC (red) and all the other RIR zone together (blue). We hypothesize that the community efforts of APNIC to create awareness about routing security and develop training and support material for network operators had led to higher adoption in smaller networks. Already in 2019, APNIC had many events and training available to the community (cite). In the APNIC zone, more than 50% of small networks' address space is covered by RPKI. In the past year, small networks' adoption has even surged above the adoption in large networks.

In contrast, in the ARIN and AFRINIC zones, small networks have low adoption of RPKI and more critically, the gap with large networks is consistently increasing. Back in 2019, large and small networks in these zones had comparable levels of adoption. However, in July 2024, only 22% of ARIN and 19% of AFRINIC's address space from small networks is covered by RPKI, representing 65% and 55% of large networks adoption respectively. In these zones, we believe the lack of incentive, awareness and complexity of operationalizing the issuance of RPKI ROAs has deterred smaller networks from adoption.

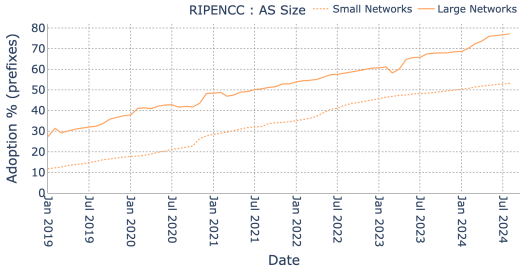
In the LACNIC zone, small networks adoption has stagnated in the last few years when compared to that of larger networks. In July 2024, small networks in LACNIC had the level of adoption large networks had 5 years ago. In the last 5 years, small network adoption has slowly increased from about 21% to 34%, *i.e.,* a 62% increase, whereas large networks have gone from 35% to 65%, almost an 85% increase. More research is needed to reveal why the behavior of small networks in that zone has changed in the past years.



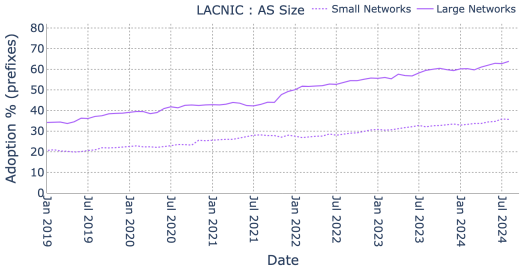
(a) ARIN zone



(b) AFRINIC zone



(c) RIPE zone



(d) LACNIC zone

Figure 6: Large and small network RPKI adoption in different RIR zones

Finally, in the RIPE zone, small networks have almost the same rate of adoption as larger networks but still lag behind about 2 years in adoption levels. In 2019, small networks in RIPE had 11% of adoption versus 28% for large networks, a 17 points difference. In July 2024, small networks have about 55% adoption versus 75%, a 20 points difference, and the level large networks had in mid 2022.

4.3 Low RPKI adoption in non-ISP networks

The differences in RPKI adoption by network size inspire us to look deeper in other network characteristics that impact adoption. The networks that connect to the public Internet are not all in the business of providing Internet related services. As an example, there are many educational and government networks that connect to the Internet. In this section we investigate whether the non-ISP networks, in particular government and educational networks, have lower RPKI adoption when compared to Internet Service Providers or other Internet Service adjacent networks.

Business classification of a network is a challenging problem as the mapping from network numbers to the actual organization that uses it and then its business model is convoluted. A network is visible in routing and RPKI through its Autonomous System Number (ASN), which is delegated by RIRs. Using RIRs' WHOIS databases, it is usually possible to get the name of the organization that manages an ASN, though it may differ from the organization that was delegated the number.[3] Then, many organizations and conglomerates operate in an array of business sectors, making it difficult to classify them into one category. Finally, there may be very little data to classify smaller organizations or sub-units of organization appear

[3]Publicly available RIR's delegation files [27] provide an exact mapping from resources to organizations. However, those files have opaque IDs to identify organizations for privacy concerns.

in the RIRs database as the owner of ASNs. As a consequence, in the network classification task, there is no authoritative or widely accepted dataset.

In the publicly available datasets that categorize networks by business sectors there is little agreement on the categories and thus on the networks part of those categories. However, there are a few sectors where we see high levels of agreement and equivalency between the two datasets with widest coverage: BGP.Tools [2] and *(ii)* Stanford ASdb [**?**]. BGP.Tools and ASdb have two very different approaches to classify ASes by business categories, use different category labels, which do not necessarily align, and both cover less than 50% of networks in the Internet. Nonetheless, in the business categories of government, academia and select Internet-related businesses, we find high levels of agreement and we focus on those sectors.

Table 3 reveals the RPKI adoption of networks in selected BGP.Tools and ASdb categories related to government, academia and Internet services where both datasets present similarities in the category name and agreement in the networks that are part of it.

We find that government and academic networks have very low levels of RPKI adoption. BGP.tools has a more strict labeling for government networks and less than 5% of the address space from those networks is covered by RPKI certificates. ASdb includes government and regulatory agencies, administration, departments and related services in the equivalent category. With that definition, the address space from those networks is close to 15% adoption, still far from the 50% average for routed address space. For academia and educational institutions, using both datasets we evaluate the RPKI adoption to about 28%. We note that both government and academic networks are mostly small networks and as such face the challenges small networks have for RPKI adoption, including lack of awareness, training and management tools for RPKI certificate. In addition, many of those networks have little incentive in terms of revenue for adoption as their users are unlikely to move to a competitor to improve their security stance. This may be true for most networks whose business does not involve Internet services.

In contrast, for Internet-related network types, we find average-to-high levels of adoption. In particular, for Internet Service Providers (ISPs) providing satellite Internet, we find they have very high levels of adoption, evaluating it to 80% or more with both datasets. We hypothesize that given the complexity and recent development of their service, those organizations have fewer challenges when incorporating RPKI in their operation. For the ISP and hosting categories, even though our datasets don't fully agree on all the networks included in them, we see that their level of adoption is about average. In these categories, there are networks of all sizes, from large ISPs to very local ISPs. We speculate that some of the challenges of RPKI adoption faced by small organizations are still present even if the purpose of those networks is to provide Internet service.

4.4 Deterrence from Address Delegation Complexity

Early on in our study we found that most network have either low or high RPKI adoption but that there are few networks in between with *partial* adoption (see Section 3.3). When studying in more detail the networks in partial adoption, we find that most of them are large networks. Given that large networks are overall driving RPKI adoption, we investigated further the partial adoption of these large networks. We find that quite a few of those networks

[4]ASdb category: Government and Regulatory Agencies, Administrations, Departments, and Services

BGP.Tools labels	**RPKI cov.%**	**ASdb labels**	**RPKI cov.%**
Government	20.3	Gov. and Reg. Agencies[4]	15.5
Academic	23.84	Colleges, Univ., and Prof. Schools	21.99
Mobile Data/Carrier	46.04	Phone Provider	33.34
Server Hosting	51.19	Hosting and Cloud Provider	57.41
Home ISP	45.06	Internet Service Provider (ISP)	44.78
Satellite Internet	85.84	Satellite Comm.	52.05

Table 3: RPKI coverage of address space originated by networks (ASNs) from select BGP.Tools and ASdb categories.

are indeed Tier 1 networks, *i.e.,* some of the largest networks of the Internet, providing transit to thousands of smaller networks, and originating sizable amounts of address space. Thus, we investigate RPKI adoption of Tier 1 networks to shed light on the partial adoption of RPKI.

AS Rank	ASN	Org. Name	# Prefixes	Addr Size in /24	RPKI coverage %
1	3356	Lumen	938	116,864	0.10
2	1299	Arelion	86	872	95.18
3	174	Cogent	4136	106,561	0.55
4	2914	NTT	261	26,819	95.04
5	6762	Telecom Italia	161	412	46.12
6	6939	Hurican Electric	225	2236	68.83
7	3257	GTT	913	26,146	11.23
8	6453	Tata	96	2242	86.89
9	6461	Zayo	198	6194	3.76
10	3491	PCCW Global	449	3951	97.37

Table 4: Characteristics of the 10 top ranked networks using RPKI

Within the select group of Tier 1 networks, though most of them have high level of RPKI adoption, some networks are in partial adoption and very few have almost no adoption. Table 4 includes the RPKI adoption of the top 10 networks as ranked by the CAIDA AS Rank methodology [1]. Figure 7 has the longitudinal view of the RPKI adoption in IPv4 address space of select Tier 1 networks. In both Table 4 and Figure 7 we find networks with high RPKI adoption, networks in partial adoption, and some with almost no adoption.

The longitudinal study of RPKI adoption of Tier 1 networks reveals that some of those networks have been in partial adoption for most of the 5 years of the study. Many of these networks have slowly increased the RPKI coverage of their address space over time. For instance, Telefonica (AS 12956) has increased RPKI adoption from less than 20% in 2019 to 92% in 2024. In that same period, Telecom Italia has gone from no adoption to almost 50%.

There are also networks that adopt RPKI very fast, and in a few months they go from no adoption to almost full adoption. For example, Comcast (AS7922) went from about 10% RPKI adoption to 98% in June 2021.

When looking at the differences between Tier 1 networks that adopt fast and the ones that go slowly, we find that the ones that adopt slowly tend to have more complex IP

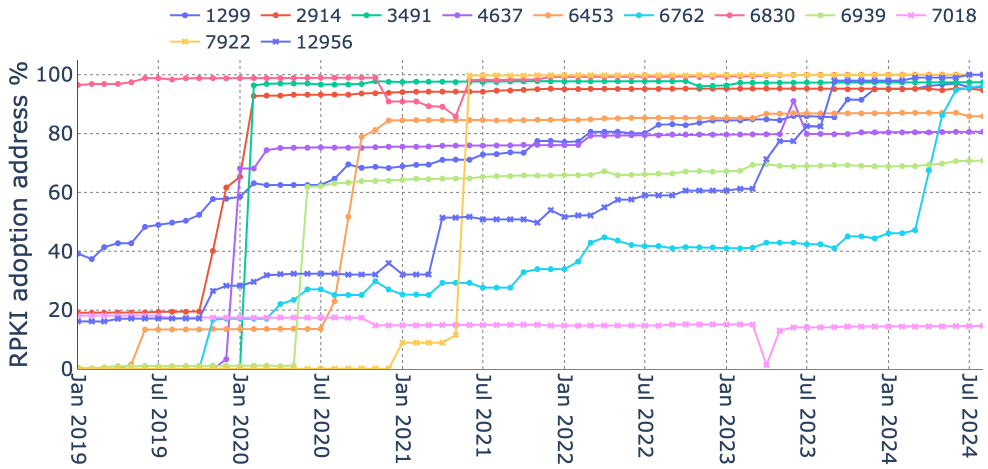


Figure 7: IPv4 RPKI adoption over time of selected Tier 1 ASes.

delegation within their address space. These networks are originating address space that has been delegated to other organizations or, in some cases, can even have multiple sub-delegations within the address space they hold and originate. Both these cases make RPKI adoption more difficult. In the former case, where a large network originates address space that another organization is delegated, the large network cannot create RPKI certificates for that address space as the control of the related RPKI certificates is in the hands of the holder of the address space. This happens when an ISP originates address space directly delegated by an RIR to a customer.

In the latter case, where there are sub-delegations of address space, in BGP we see many sub-prefixes of the large network being originated by other networks. In this case, if a large network decided to issue an RPKI certificate for a large address block that is sub-delegated with sub-prefixes originated by other networks, the sub-prefix routes would be considered RPKI invalid unless the sub-prefix and the other origin are in another RPKI certificate. In other words, the adoption by the large network requires coordination with the (smaller) networks using the sub-delegations in BGP in order to prevent availability issues in the impacted addresses.

We also investigate why some Tier 1 networks with high levels of RPKI adoption, such as PCCW (AS3491), and NTT (AS2914) have stagnated their adoption at a level slightly below 100%. We find that the prefixes lacking RPKI coverage also tend to be delegated to other organizations, as ISPs often originate prefixes on behalf of their customers.

In summary, the study of Tier 1 RPKI adoption trajectories reveals that not all address space is equal in terms of effort required to cover IP address blocks with RPKI certificates. For some address space, the network originating it in BGP may not have the ability to issue RPKI certificates. For other address space, coordination with other networks is needed to prevent traffic delivery failures. Thus, RPKI adoption is not always a straightforward process of issuing RPKI certificates for all address space.

5 Conclusions

In the last five years, the adoption of RPKI certificates to increase security of routed address space has moved from the early adoption face to the early majority phase of technology adoption. In April 2024, the overall RPKI adoption of routed IPv4 address space passed the 50% bar. However, to continue improving the state of routing security, we need the next 50% to adopt RPKI. With our detailed analysis of RPKI coverage depending on several characteristics of resources, we identify barriers that are hindering the adoption of ROAs, as well as some of the driving factors that have pushed the RPKI ecosystem to its current state. We summarize our majors findings below and hope they may help direct policymakers' efforts to improve the state of routing security .

Small stakeholders need targeted support: RPKI adoption is not a trivial step for networks since it makes the operation more challenging with more steps and more risks of errors. We find that RPKI adoption is lagging in small networks, even when small networks need to issue only 1 or 2 certificates total to cover their address space. More than 50% of small networks have no RPKI adoption at the time of writing. To encourage the next tier of RPKI adoption, smaller stakeholders require more support for RPKI implementation, including awareness, operational training and management tools.

Bottom-up community-driven efforts have paid off: RIR zones with more community focused initiatives to encourage RPKI adoption have higher adoption rates. RIR zones with less adoption can learn from the successful initiatives from other zones how to best engage different parts of the community and support RPKI adoption.

Additional support for non-ISP networks: Networks of organizations whose primary business is not related to Internet services such as educational and government organizations, have higher barriers and less incentives to adopt RPKI. More research is needed to find an approach that will make a change for these networks. They may require support from their transit provider or the RIR that delegated the address space to issue and manage their RPKI certificate.

Encouraging coordination across the ecosystem: IP address delegation and Internet routing are independent aspects of address space that RPKI forces to relate. Thus, coordination costs and challenges between organizations make RPKI adoption more difficult and slow for some address blocks. Aligning incentives or pairing effort levels between larger transit networks and smaller ISPs, as well as between network providers and their customers with direct IP addresses delegations, would enable RPKI adoption in address space with complex delegation structure.

Acknowledgments

This work is based on research sponsored by U.S. NSF grant OAC-2419735. The views and conclusions are those of the authors and do not necessarily represent endorsements, either expressed or implied, of NSF.

References

[1] Caida as rank. http://as-rank.caida.org/.

[2] BGP.Tools. Browse the internet ecosystem.

[3] Chung, T., Aben, E., Bruijnzeels, T., Chandrasekaran, B., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A., Rijswijk-Deij, R. v., Rula, J., and Sullivan, N. RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. In *Proceedings of the Internet Measurement Conference* (Amsterdam, Netherlands, Oct. 2019), IMC '19, Association for Computing Machinery, pp. 406–419.

[4] Cloudflare. Is BGP safe yet? `https://isbgpsafeyet.com/`.

[5] Du, B., Testart, C., Fontugne, R., Akiwate, G., and Snoeren, A. C. Mind Your MANRS: Measuring the MANRS Ecosystem. In *Proceedings of the ACM Internet Measurement Conference on - IMC '22* (Nice, France, Oct. 2022), p. 14.

[6] Forum Standaardisatie. Secured internet routing of Dutch government by end of 2024. `https://www.forumstandaardisatie.nl/nieuws/secured-internet-routing-dutch-government-end-2024`, 2023.

[7] Gilad, Y., Cohen, A., Herzberg, A., Schapira, M., and Shulman, H. Are We There Yet? On RPKI's Deployment and Security. In *Proceedings 2017 Network and Distributed System Security Symposium* (San Diego, CA, 2017), Internet Society.

[8] Gilad, Y., Sagga, O., and Goldberg, S. MaxLength Considered Harmful to the RPKI. In *Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies* (New York, NY, USA, 2017), CoNEXT '17, ACM, pp. 101–107. event-place: Incheon, Republic of Korea.

[9] Goodin, D. How 3ve's BGP hijackers eluded the Internet—and made $29M. `https://arstechnica.com/information-technology/2018/12/how-3ves-bgp-hijackers-eluded-the-internet-and-made-29m/`, 2018.

[10] Goodin, D. How 3 hours of inaction from Amazon cost cryptocurrency holders $235,000. `https://arstechnica.com/information-technology/2022/09/how-3-hours-of-inaction-from-amazon-cost-cryptocurrency-holders-235000/`, 2022.

[11] Hiran, R., Carlsson, N., and Gill, P. Characterizing Large-Scale Routing Anomalies: A Case Study of the China Telecom Incident. In *Passive and Active Measurement*, D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, M. Roughan, and R. Chang, Eds., vol. 7799. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 229–238.

[12] Hlavacek, T., Jeitner, P., Mirdita, D., Shulman, H., and Waidner, M. Behind the Scenes of RPKI. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY, USA, Nov. 2022), CCS '22, Association for Computing Machinery, pp. 1413–1426.

[13] Iamartino, D., Pelsser, C., and Bush, R. Measuring BGP Route Origin Registration and Validation. In *Passive and Active Measurement* (Cham, 2015), J. Mirkovic and Y. Liu, Eds., Lecture Notes in Computer Science, Springer International Publishing, pp. 28–40.

[14] Internet Initiative Japan Inc. Internet Health Report. `https://ihr-archive.iijlab.net`, 2023.

[15] Kentik. A Tale of Two BGP Leaks. `https://www.kentik.com/blog/a-tale-of-two-bgp-leaks/`.

[16] LACNIC. Evolution of rpki: Towards higher levels of security in regional routing, January 2023.

[17] Lepinski, M., and Kent, S. An Infrastructure to Support Secure Internet Routing. RFC 6480, Feb. 2012.

[18] Li, W., Lin, Z., Ashiq, M. I., Aben, E., Fontugne, R., Phokeer, A., and Chung, T. RoVista: Measuring and Analyzing the Route Origin Validation (ROV) in RPKI. In *Proceedings of the 2023 ACM on Internet Measurement Conference* (New York, NY, USA, Oct. 2023), IMC '23, Association for Computing Machinery, pp. 73–88.

[19] Li, Y., Zou, H., Chen, Y., Xu, Y., Ma, Z., Ma, D., Hu, Y., and Xie, G. The Hanging ROA: A Secure and Scalable Encoding Scheme for Route Origin Authorization. In *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications* (London, United Kingdom, May 2022), IEEE Press, pp. 21–30.

[20] Madory, D. Bgp hijack of amazon dns to steal crypto currency. `https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/`, 2018.

[21] Madory, D. Learning from recent major BGP routing leaks. `https://www.slideshare.net/apnic/learning-from-recent-major-bgp-routing-leaks`, February 2018.

[22] Madory, D. Large European Routing Leak Sends Traffic Through China Telecom. `https://blogs.oracle.com/internetintelligence/large-european-routing-leak-sends-traffic-through-china-telecom`, June 2019.

[23] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and Austein, R. BGP Prefix Origin Validation. RFC 6811, Jan. 2013.

[24] National Institute for Standards and Technology. RPKI Deployment Monitor. `https://rpki-monitor.antd.nist.gov/`.

[25] NCC, R. Routing Information System (RIS), 2023.

[26] Newman, L. H. Why Google Internet Traffic Rerouted Through China and Russia. https://www.wired.com/story/google-internet-traffic-china-russia-rerouted/, Nov. 2018.

[27] NRO. Rir statistics: Nro extended allocation and assignment reports.

[28] of Oregon, U. University of Oregon Route Views Project, 2022.

[29] Oliver, L., Akiwate, G., Luckie, M., Du, B., and claffy, k. Stop, DROP, and ROA: effectiveness of defenses through the lens of DROP. In *Proceedings of the 22nd ACM Internet Measurement Conference* (New York, NY, USA, Oct. 2022), IMC '22, Association for Computing Machinery, pp. 730–737.

[30] Paganini, P. BGP hijacking - Traffic for Google, Apple, Facebook, Microsoft and other tech giants routed through Russia. https://securityaffairs.co/wordpress/66838/hacking/bgp-hijacking-russia.html, Dec. 2017.

[31] ripe.net. Index of /rpki/.

[32] Ryu, S. Post mortem of klayswap incident through bgp hijacking. https://medium.com/s2wblog/post-mortem-of-klayswap-incident-through-bgp-hijacking-en-3ed7e33de600, 2022.

[33] White House. National Cybersecurity Strategy Implementation Plan. https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf, 2023.

[34] Wählisch, M., Maennel, O., and Schmidt, T. C. Towards detecting BGP route hijacking using the RPKI. *ACM SIGCOMM Computer Communication Review 42*, 4 (Aug. 2012), 103–104.

[35] Wählisch, M., Schmidt, R., Schmidt, T. C., Maennel, O., Uhlig, S., and Tyson, G. RiPKI: The Tragic Story of RPKI Deployment in the Web Ecosystem. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks* (New York, NY, USA, Nov. 2015), HotNets-XIV, Association for Computing Machinery, pp. 1–7.

[36] Yoo, C. S., and Wishnick, D. Lowering Legal Barriers to RPKI Adoption. *SSRN Electronic Journal* (2019).