Mind Your MANRS: Measuring the MANRS Ecosystem

Ben Du
UC San Diego
bendu@ucsd.edu

Cecilia Testart
MIT/Georgia Tech
ctestart@gatech.edu

Romain Fontugne
IIJ Research Lab
romain@iij.ad.jp

Gautam Akiwate
UC San Diego
gakiwate@cs.ucsd.edu

Alex C. Snoeren
UC San Diego
snoeren@cs.ucsd.edu

kc claffy
CAIDA/UC San Diego
kc@caida.org

ABSTRACT

Mutually Agreed Norms on Routing Security (MANRS) is an industry-led initiative to improve Internet routing security by encouraging participating networks to implement a series of mandatory or recommended actions. MANRS members must register their IP prefixes in a trusted routing database and use such information to prevent propagation of invalid routing information. MANRS membership has increased significantly in recent years, but the impact of the MANRS initiative on the overall Internet routing security remains unclear. In this paper, we provide the first independent look into the MANRS ecosystem by using publicly available data to analyze the routing behavior of participant networks. We quantify MANRS participants' level of conformance with the stated requirements, and compare the behavior of MANRS and non-MANRS networks. While not all MANRS members fully comply with all required actions, we find that they are more likely to implement routing security practices described in MANRS actions. We assess the relevance of the MANRS effort in securing the overall routing ecosystem. We found that as of May 2022, over 83% of MANRS networks were conformant to the route filtering requirement by dropping BGP messages with invalid information according to authoritative records, and over 95% were conformant to the routing information facilitation requirement, registering their resources in authoritative databases.

CCS CONCEPTS

• **Networks** → **Web protocol security**; • **Security and privacy** → **Web protocol security**;

KEYWORDS

BGP, Routing Security, IRR, RPKI, MANRS.

ACM Reference Format:
Ben Du, Cecilia Testart, Romain Fontugne, Gautam Akiwate, Alex C. Snoeren, and kc claffy. 2022. Mind Your MANRS: Measuring the MANRS Ecosystem. In *ACM Internet Measurement Conference (IMC '22), October 25–27, 2022, Nice, France.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3517745.3561419

1 INTRODUCTION

The Internet consists of tens of thousands of individual networks interconnected via the Border Gateway Protocol (BGP). BGP relies on a mutual trust model: it lacks a mechanism to verify the authenticity of propagated routing information [25, 54]. This omission makes the global routing system vulnerable to both accidental and intentional compromises of its integrity. Over the past decade, intentional compromises have disrupted popular Internet services [39], supported spam campaigns [44, 57], and induced significant financial losses [33, 35, 49]. Accidental compromises remain frequent and can also cause widespread disruptions [34, 51].

In response to this long-standing threat, operators and researchers have developed mechanisms to allow Autonomous Systems to gain additional confidence in route advertisements upon which they rely. In the early 1990s, the operational community deployed Internet Routing Registries (IRR) [5], and later the Resource Public Key Infrastructure (RPKI) [30], to support authentication of routes against trusted databases. Unfortunately, the additional cost and complexity—including legal ramifications—of using these databases has hindered operator participation [29, 52, 56]. Moreover, the harm that route hijacks cause more commonly accrues to a customer of an ISP rather than the ISP itself, and they can be challenging to detect and report, so incentives to invest in countermeasures are not well aligned.

To encourage collective action in the adoption of routing security practices, a group of network operators started the Mutually Agreed Norms for Routing Security (MANRS) initiative in 2014 [2, 47]. Hosted by the Internet Society (ISOC), MANRS advocates for a set of security best practices—which they call *actions*—to prevent the propagation of incorrect routing information, restrict forwarding of traffic from spoofed IP addresses, and facilitate coordination between network operators.

However, MANRS has not taken on rigorous enforcement of these best practices. ISOC provides some aggregated statistics from external sources [1] but declines to publicly detail non-conformance. (Instead, ISOC provides individual operators with private monthly reports regarding conformance.) Previous work has found inconsistent adherence of MANRS members to specific recommendations, e.g., the Source Address Validation action (Recommended Action #2) [32], but we are not aware of an independent study of MANRS members' overall conformance with MANRS actions. Lack of empirical assessment of conformance frustrates a collective understanding of how effective MANRS is at achieving its objectives. Indeed,

IMC '22, October 25–27, 2022, Nice, France
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9259-4/22/10…$15.00
https://doi.org/10.1145/3517745.3561419

this lack of understanding recently prompted U.S. regulators to launch a Notice of Inquiry to ascertain whether there was a role for government intervention to improve routing security [17].

In this paper, we analyze the MANRS ecosystem, including the characteristics of networks that participate, and their conformance with MANRS actions. Our main contributions are as follows:

- We characterize the networks that have joined MANRS since its inception, including network size, type, and geographic distribution (§7).
- We analyze the extent to which MANRS networks differ from non-MANRS networks in their implementation of best practices (§8–9). We consider the level of deployment by each network and discuss the effect of thresholds of conformance for considering compliance.
- We study the impact of MANRS networks on the whole Internet, in terms of RPKI registration (§8.6) and Route Origin Validation deployment (§9.4).

2 BACKGROUND

For the benefit of uninitiated readers, in this section we describe the mechanism of BGP origin hijacks, defenses introduced to help prevent them, and the MANRS requirements to adopt such defenses.

2.1 BGP hijacking

A legitimate BGP announcement includes a destination prefix and a list of Autonomous Systems (ASes) that Internet traffic needs to traverse to reach that destination prefix. BGP hijacking is the unauthorized modification of any part of a BGP announcement by another AS; Sermpezis et al. [50] taxonomized BGP hijacking based upon the attribute an attacker modifies. In a *prefix origin hijack*, an attacker falsely claims it is the origin of a BGP announcement, i.e, an attacker announces the prefix on behalf of the victim. In a *path hijack*, the attacker modifies the AS path to place itself between the victim and the rest of the Internet. Researchers, operators, and engineers have spent decades developing proposals to prevent both types of hijacks, but none has yet been operationally deployed [27, 31, 43, 54, 55]. There is growing consensus that, at least in the short term, improved security will require network operators and other critical actors to undertake enhanced operational practices that restrict the ability of malicious actors to disrupt normal activities. This consensus inspired the creation of the MANRS initiative that advocates for a certain set of operational best practices.

2.2 Internet Routing Registry

The Internet Routing Registry (IRR), introduced in 1995, is a collection of databases designed to share routing policy information among networks [5]. *Authoritative* IRR databases are managed by the five Regional Internet Registrars (RIRs) and each contains only IP address space managed by the respective RIR. Other organizations (as well as RIRs themselves) can provide *non-authoritative* IRR databases, which may contain less accurate information [20, 28]. Merit operates the RADb [37] which mirrors many other databases into a single collection [36].

One of the most important objects in an IRR database is the `route` object, which a network creates to register the route (prefix and origin AS) it intends to originate in the global BGP routing system. If a network wants to authorize more than one AS—e.g., a customer AS—to originate a prefix, it can use the `as-set` object for this purpose. Networks can use the IRR to filter and drop received BGP announcements according to how well the announced information matches the corresponding IRR-registered route objects. A route object can match exactly *(valid)*, not exist at all *(not found)*, or exist with a more-specific prefix length *(invalid prefix length).* Some IXPs and cloud providers use `as-set` to determine from which ASes to accept BGP announcements [3, 4].

2.3 Resource Public Key Infrastructure

The Resource Public Key Infrastructure (RPKI), introduced in 2012, is a set of cryptographically attested databases containing authenticated prefix-origin information [30]. Each of the five Regional Internet Registrars is a trust anchor for the IP address space in its service region. IP address holders can obtain certificates from their RIR that allow them to cryptographically sign (or *register*) Route Origin Authorization objects (ROAs) for their address space. The RIR can host these certificates and ROAs, or provide ISPs with their own CA certificates to sign ROAs for themselves and their customers.

To filter BGP announcements using the RPKI, a practice known as *Route Origin Validation*, networks need to run Relying Party (RP) software [38]. This RP software downloads ROAs and certificates from the trust anchors, checks the validity of the certificate chain, and generates a list of validated ROA payloads (VRPs). The most important fields of a VRP are `IP prefix`, `ASN`, and `max length`. The RP then validates BGP announcements against covering VRPs, i.e., those whose `IP prefix` contains the prefix in the BGP announcement. The resulting *RPKI status* of a BGP announcement is one of:

- *Not found*: The BGP prefix has no covering VRP.
- *Invalid ASN*: No `ASN` in any covering VRP matches the BGP origin AS.
- *Invalid prefix length*: The BGP origin AS is valid but the announced prefix is more specific than allowed by the covering VRP's `max length`. (Sometimes combined with *invalid ASN*.)
- *Valid*: the BGP prefix and origin AS agree with those in a covering VRP.

2.4 MANRS

The Mutually Agreed Norms for Routing Security (MANRS) initiative launched in 2014 and has had steady growth in membership ever since [47]. Figure 2 shows the growth of MANRS in terms of both organizations and ASes.

MANRS currently provides four programs with different security action sets [2] intended for different types of network operators (Figure 1): Internet service (transit) providers (ISPs); content distribution networks (CDNs), including cloud providers; Internet exchange points (IXPs); and equipment vendors. We focus on the first two categories in this paper.

MANRS for Network Operators (ISP).

- *Action 1*: Prevent propagation of incorrect routing information by checking the validity of their customers' BGP announcements.

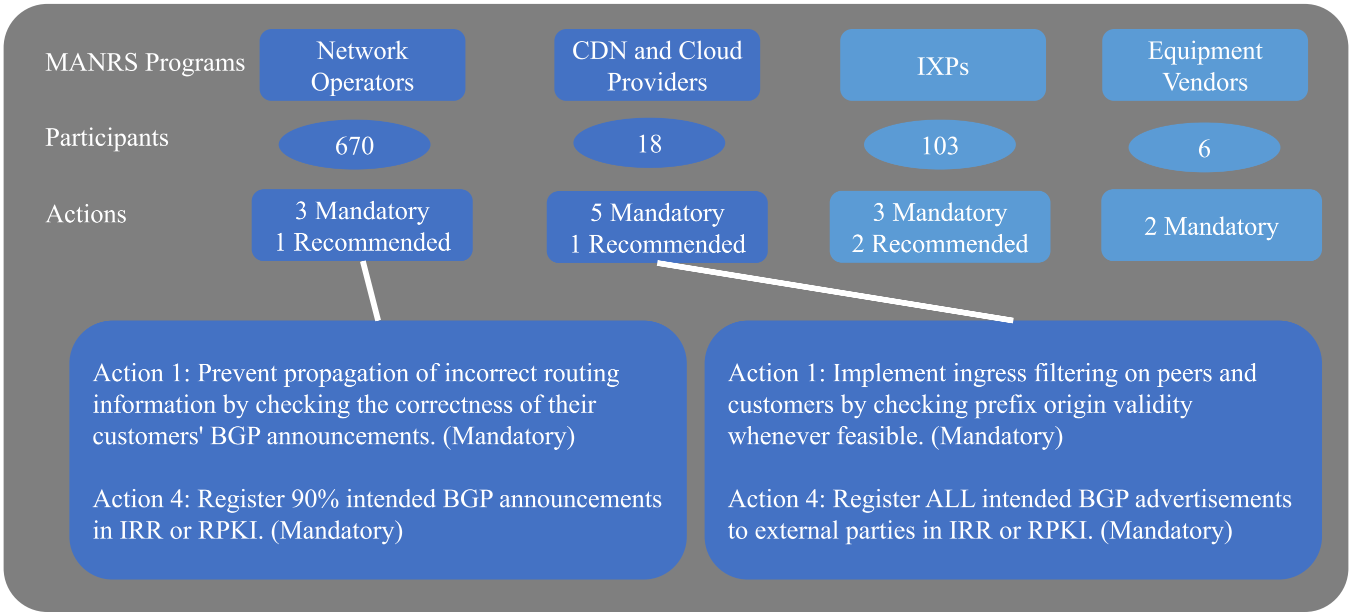

MANRS Programs
Network Operators
CDN and Cloud Providers
IXPs
Equipment Vendors
Participants
670
18
103
6
Actions
3 Mandatory 1 Recommended
5 Mandatory 1 Recommended
3 Mandatory 2 Recommended
2 Mandatory
Action 1: Prevent propagation of incorrect routing information by checking the correctness of their customers' BGP announcements. (Mandatory)
Action 4: Register 90% intended BGP announcements in IRR or RPKI. (Mandatory)
Action 1: Implement ingress filtering on peers and customers by checking prefix origin validity whenever feasible. (Mandatory)
Action 4: Register ALL intended BGP advertisements to external parties in IRR or RPKI. (Mandatory)

Figure 1: MANRS has 4 programs and each program includes a set of mandatory and recommended actions. We focus on the ISP (Network Operator) and CDN/Cloud Provider categories, and the two actions in each category related to route registration and route filtering.

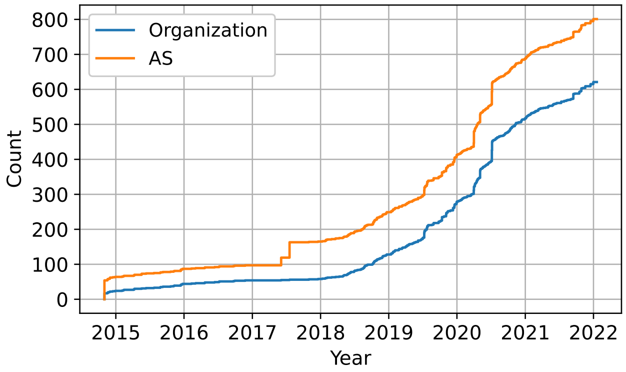


Figure 2: MANRS participants have grown significantly over the past 7 years, especially in the last 3 years.

- *Action 2 (optional)*: Filter outbound traffic with spoofed source IP and run the CAIDA Spoofer software [32] to prevent DDoS attack traffic from being originated from the participant's network.
- *Action 3*: Maintain up-to-date network contact information in IRR databases or PeeringDB.
- *Action 4*: Register intended BGP announcements in IRR or RPKI. Using RPKI is recommended.

MANRS for CDN and cloud providers.

- *Action 1*: Implement ingress filtering on peers and customers by checking prefix-origin validity whenever feasible.
- *Action 2*: Same as Action 2 for ISPs, but mandatory for CDNs.
- *Action 3*: Same as Action 3 for ISPs.
- *Action 4*: Register all intended BGP advertisements to external parties in IRR or RPKI.
- *Action 5*: Encourage peers to adopt MANRS.
- *Action 6 (optional)*: Provide monitoring tools to peers.

In this work, we focus on Action 1 and Action 4 in the ISP and CDN programs because they are the most relevant to MANRS networks' behavior in BGP.

3 GOALS AND ASSUMPTIONS

MANRS attempts to encourage routing security practices through the collective action of network operators. Our goal in this paper is to evaluate the current state of the initiative in terms of its participants, their routing behavior and its impact in the broader routing ecosystem, and discuss potential improvements. Figure 3 outlines the analysis to achieve our goal.

RQ1: Who is part of MANRS? To understand where MANRS has gained traction, we look at the geographical distribution of ASes in MANRS and their service regions. We use customer-cone size, size of originated address space, and size of address space covered by RPKI objects of ASes to further characterize MANRS participants and their significance in each RIR.

RQ2: Are MANRS networks conformant with MANRS actions? We seek to assess how conformant MANRS members are to Action 1 and Action 4 of the MANRS ISP and CDN programs (§2.4), which relate to the origination and propagation of incorrect routing information. These actions are not new or unique to MANRS; they were proposed to improve routing security many years ago but their implementation has struggled. Currently, MANRS does not enforce the implementation of these actions despite being required

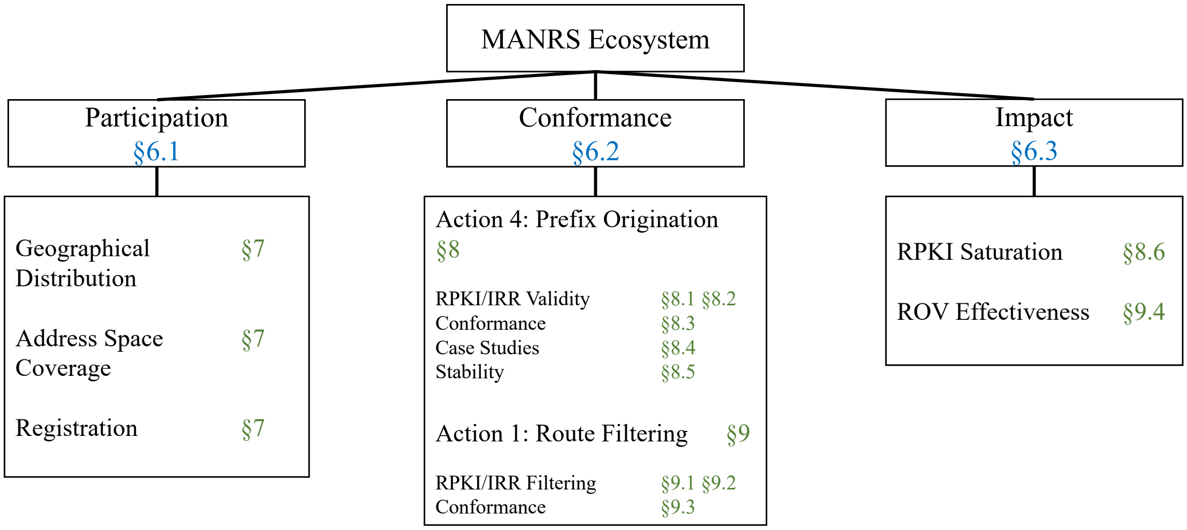


Figure 3: Structure of the paper. Methodology sections are in blue and results sections are in green.

for members. Therefore, we want to evaluate the extent to which MANRS members actually employ these actions.

We cannot reasonably expect all MANRS members to be continually and entirely conformant to MANRS actions. Operating a large network, maintaining objects in routing registries, and coordinating with customers are all laborious and error-prone tasks, even with the help of automated tools [12]. In addition, operators have reported technical caveats that prevented them from complete ROV deployment [41], and many commercial ISPs are not filtering customers' announcements [7, 23]. As a result, operators need to constantly monitor their resources to ensure that their—and their customers'—advertisements match IRR and RPKI entries, and may have to communicate with customers to create or update ROAs.

MANRS Action 1 for CDNs, which relates to the propagation of incorrect routing announcements from either MANRS members or their customers, allows propagated announcements to be more specific than the records registered in IRR. Such a mismatch in prefix lengths is generally due to prefix de-aggregation in the context of traffic engineering practices [16]. Thus, we treat BGP announcements with IRR status of *invalid prefix length* as conformant to MANRS Actions 1 and 4.

RQ3: What is the impact of MANRS on the broader routing ecosystem? We want to gauge the effect MANRS has in securing the routing system. First, we evaluate if MANRS networks indeed have better security practices than non-MANRS networks. Specifically, we assess AS behavior with respect to registering RPKI ROAs for its prefixes and performing route origin validation In addition, we measure if MANRS members reduce the number of invalid prefixes transiting their networks.

4 RELATED WORK

Relevant previous research covers the measurement of RPKI ROA registration, RPKI Route Origin Validation (ROV), IRR registration, and MANRS conformance.

4.1 RPKI registration prevalence

In 2017 Wählisch et al. [58] found that large CDNs and website hosting providers were reluctant to register ROAs in the RPKI, limiting its adoption. In 2019, Chung et al. [15] found a significant increase in IPv4 address space covered since 2012, and saw fewer misconfigurations over time, showing positive trends in RPKI registration. In this work, we measure ROA registration over time by MANRS and non-MANRS ASes to evaluate if MANRS ASes are more likely to adopt RPKI.

4.2 Deployment of Route Origin Validation

In 2017, Reuter et al. [45] used custom BGP announcements from the PEERING testbed to measure ROV and found 3 ASes that deployed ROV. In 2021, Rodday et al. [48] expanded this methodology using traceroutes and found 10 ASes that deployed ROV with high confidence. In 2022, Chen et al. [14] used similar methodology, increased the measurement scale, used a Bayesian inference method to post-process the results, and inferred 3,107 ASes deployed ROV, but those estimations were not validated.

In 2018, Cartwright-Cox [13] measured network-level ROV deployment by collecting ICMP Ping responses from both RPKI-valid and RPKI-invalid prefixes and found 616 ASes that deployed ROV. In 2020, Huston and Damas [24] used web requests to identify 7 ROV-deploying large transit providers. Using passive observation, Testart et al. [56] noticed increasing ROV deployment among large transit providers from 2018 to 2020, which suggested increased benefits of registering one's prefixes in RPKI.

These studies raise the challenge of measuring ROV when (temporarily) invalid announcements may be due to operational changes, misconfigurations and adjustments, as mentioned in (§3). In this paper, we adapt previous passive methodologies to measure ROV for MANRS and non-MANRS ASes using information available in the Internet Health Report (IHR)(§5.3). In addition, we use other metrics provided by the IHR to evaluate the overall presence of MANRS ASes in paths toward invalid prefixes.

4.3 IRR Registration

In 2013, Khan et al. [28] quantified the BGP announcements (obtained from the CAIDA prefix2as dataset [11] from 2010 to 2013) that matched IRR records and found 71% of records matched, with significant evidence of outdated records in IRR databases. Despite the fact that the IRRs cover more address space than the RPKI, its low accuracy [20] motivated development of the RPKI in the first place.

4.4 Conformance to MANRS actions

To our knowledge, the only published research on MANRS conformance focused on a non-mandatory action - Source Address Validation (SAV). In 2019, Luckie *et al.* [32] found no evidence that MANRS networks were more likely to properly deploy SAV than non-MANRS networks. In this work, we focus on conformance to other MANRS actions, which are mandatory (Action 1 and Action 4, §2.4).

5 DATASETS

We use the following datasets to analyze the MANRS networks and their routing behavior.

5.1 CAIDA Datasets

We obtained CAIDA's Routeviews Prefix to AS mappings Dataset for IPv4 and IPv6 [11] from 2015 to 2022 (*prefix2as dataset*) for historical routing analysis of MANRS networks. We also used the April 2022 snapshots of CAIDA's inferred AS-to-organization (*as2org dataset*) [10], AS relationship (*AS Relationship dataset*) [9], and AS rank (*AS Rank dataset*) [8] datasets to facilitate further analysis.

5.2 List of Participating MANRS networks

We downloaded the list of participants in the MANRS Network Operators Program and the MANRS CDN and Cloud Providers Program on May 1, 2022 from the MANRS website [2]. We refer to this as the *MANRS ISP dataset* and the *MANRS CDN dataset*. The Internet Society kindly provided us the dates when each MANRS participant joined their corresponding MANRS programs; we refer to this list as the *historical MANRS dataset*.

5.3 Internet Health Report

We obtained BGP and ROV data from the Internet Health Report (IHR) developed by IIJ Research Labs [26]. The IHR Route Origin Validation module reports routed (prefix, origin AS) obtained from RouteViews [42] and RIPE RIS [40] along with IRR and RPKI information. The main attributes we use are: *prefix, origin AS, RPKI status, IRR status, transit AS,* and *AS Hegemony score*. RPKI status and IRR status are computed according to the RFC 6811 Route Origin Validation process [38].

The AS Hegemony score is a metric introduced by Fontugne *et al.* [22]. It uses sampled BGP data to estimate the fraction of AS paths that transit a given AS to reach a specified set of address space. It varies between 0 and 1, the higher the score the more an AS is present in paths towards the given destination address space.

IHR considers the origin AS of each prefix a trivial transit AS with hegemony value of 1 (trivially, every announced prefix is always provided transit by its origin AS). We extracted those cases into the *IHR prefix-origin dataset* and used the remainder as the *IHR transit dataset*.

We found errors in RPKI status and IRR status information reported by IHR between April 7 and May 6, 2022, and alerted the developers. For our analyses, we corrected the RPKI status and IRR status fields using the RPKI and IRR datasets below.

5.4 RPKI and IRR archives

Since 2011, RIPE NCC has published daily lists of validated ROA objects from all five RPKI trust anchors (APNIC, ARIN, RIPE NCC, AFRINIC, and LACNIC) [46]. We downloaded the monthly validated ROA archives from 2014 to 2022; we refer to this as the *RPKI dataset*. There are 22 IRR database providers that publish their daily IRR snapshots [36]; we collected data that started in November 2021 to May 2022 and refer to this as the *IRR dataset*.

6 METHODOLOGY

We measure the MANRS ecosystem in the following three aspects: participation, conformance, and impact. We also describe our AS classification process.

6.1 Prefix Origin Classification

RPKI validity For RPKI, a prefix origin is *Valid* if there is at least one VRP with prefix, ASN, and max length attributes all matching the route. If all VRPs covering the route have an ASN different from the route's origin AS then the route is *Invalid*. If at least one VRP has a matching ASN but the Max Length attribute is not covering the route, then the route is classified as *Invalid Length*. A route is *Not Found* if no VRP covers it.

IRR validity For IRR, we apply the same classification method as RPKI, but since there is no standardized max length attribute in IRR, we consider the prefix length as the max length value for IRR entries.

6.2 AS Customer Degree

The routing complexity of a network increases with its customer degree, especially when additional route filtering is deployed. To perform a fair comparison of conformance between ASes of similar routing complexity, we classify ASes into three sizes by their number of AS-level customers inferred by CAIDA's AS Rank [9], using the thresholds defined by Dhamdhere et al. [18]:

- **Small networks**: $CustomerDegree \leq 2$
- **Medium networks**: $2 < CustomerDegree \leq 180$
- **Large networks**: $CustomerDegree > 180$

6.3 MANRS Participation

We study the following aspects of MANRS participation.

Geographical Distribution We use the *as2org dataset* to find the countries of headquarters of the MANRS organizations (ISPs and CDNs) and the RIRs that allocated their corresponding ASes, and match the information in our *historical MANRS dataset* to obtain a distribution of MANRS ASes by RIR over time.

Routing Table Presence We use the *prefix2as dataset* and the *historical MANRS dataset* to find the MANRS ASes in the BGP table and calculate the fraction of IPv4 address space announced by them per year.

Registration Completeness We use the *as2org dataset* to identify all ASes allocated to each MANRS member organization, including those not registered in MANRS. We manually check the correctness of this dataset in our case studies. We then calculate the fraction of ASes in the MANRS participants list over all ASes of each organization. We also use the *prefix2as dataset* to calculate the fraction of IP address space originated by registered MANRS ASes over total address space originated by all ASes of each organization.

6.4 MANRS Conformance

In the *IHR prefix origin dataset* and the *IHR transit dataset*, we define a prefix-origin pair to be *MANRS-conformant* if its RPKI status is Valid, or its IRR status is Valid or Invalid length (given IRR does not have a max len attribute), and *MANRS-unconformant* if it is RPKI Invalid or (RPKI NotFound, IRR Invalid).

Prefix Origination Behavior We use the *IHR prefix origin dataset* to obtain the prefixes originated by each AS and their RPKI and IRR statuses. We calculate the RPKI origination validity ($OG_{RPKIvalid}$) for each AS using Formula 1:

$$OG_{RPKIvalid} = \frac{\textit{\# of RPKI Valid prefixes}}{\textit{total \# of originated prefixes}} \times 100\% \qquad (1)$$

We then calculate the IRR origination validity ($OG_{IRRvalid}$) for each AS using Formula 2:

$$OG_{IRRvalid} = \frac{\textit{\# of IRR Valid prefixes}}{\textit{total \# of originated prefixes}} \times 100\% \qquad (2)$$

We then calculate the MANRS Action 4 Conformance ($OG_{conformant}$) for each AS using Formula 3:

$$OG_{conformant} = \frac{\textit{\# of MANRS-conformant prefixes}}{\textit{total \# of originated prefixes}} \times 100\% \qquad (3)$$

Route Filtering Behavior It is challenging to measure ROV deployment at scale, and no previous work has done so with high confidence and sufficient validation (§4.2). Instead of measuring ROV deployment, we analyze the prevalence of RPKI Invalid announcements that propagated through each AS. We then use the *IHR transit dataset* to obtain the BGP announcements propagated by each AS and their RPKI statuses and calculate the RPKI propagation invalidity ($PG_{RPKIinv}$) for each AS using Formula 4. We discuss the limitations of our methodology in §11.

$$PG_{RPKIinv} = \frac{\textit{\# of RPKI Invalid + RPKI Invalid Length prefixes}}{\textit{total \# of propagated prefixes}} \times 100\% \qquad (4)$$

We calculate the IRR propagation invalidity (PG_{IRRinv}) for each AS using Formula 5.

$$PG_{IRRinv} = \frac{\textit{\# of IRR Invalid prefixes}}{\textit{total \# of propagated prefixes}} \times 100\% \qquad (5)$$

We identify the direct customers of each AS using the *AS Relationship dataset* and focus on BGP announcements from customers. We calculate the MANRS Action 1 Unconformance (PG_{unc}) for each AS using Formula 6.

$$PG_{unc} = \frac{\textit{\# of MANRS-unconformant prefixes}}{\textit{total \# of propagated customer prefixes}} \times 100\% \qquad (6)$$

6.5 MANRS Impact

To study the impact of MANRS networks, we quantify their level of completion in RPKI registration and overall ROV effectiveness.

RPKI Saturation To conduct historical analysis on RPKI registration, we use the annual snapshots of the *prefix2as dataset* from 2015 to 2022 and *RPKI dataset* snapshots with matching dates, and use the Route Origin Validation (ROV) algorithm [38] to calculate the RPKI status of all BGP announcements for each snapshot. We then calculate the RPKI saturation, denoted $RSat_m$, for MANRS ASes defined by Equation 7.

$$RSat_m = \frac{\textit{ROA covered MANRS Routed Address Space}}{\textit{Total MANRS Routed Address Space}} \times 100\% \qquad (7)$$

We also calculate the RPKI saturation for non-MANRS ASes ($RSat_n$) defined by Equation 8.

$$RSat_n = \frac{\textit{ROA covered non-MANRS Routed Address Space}}{\textit{Total non-MANRS Routed Address Space}} \times 100\% \qquad (8)$$

Overall ROV Effectiveness To study the overall ROV deployment of MANRS networks collectively, we analyze whether RPKI invalid (and invalid prefix length) BGP announcements are more likely to propagate through MANRS networks than non-MANRS networks. Intuitively, if MANRS networks have more effective ROV deployment than non-MANRS networks, RPKI invalid announcements should be less likely to propagate through the former.

Using the *IHR transit dataset*, for each prefix origin pair PO_k, we find its transit ASes and denote the hegemony score of each MANRS AS H_{ASi}^{MANRS} and non-MANRS AS H_{ASj}^{XMANRS}. The list of transit AS hegemony scores is denoted below:

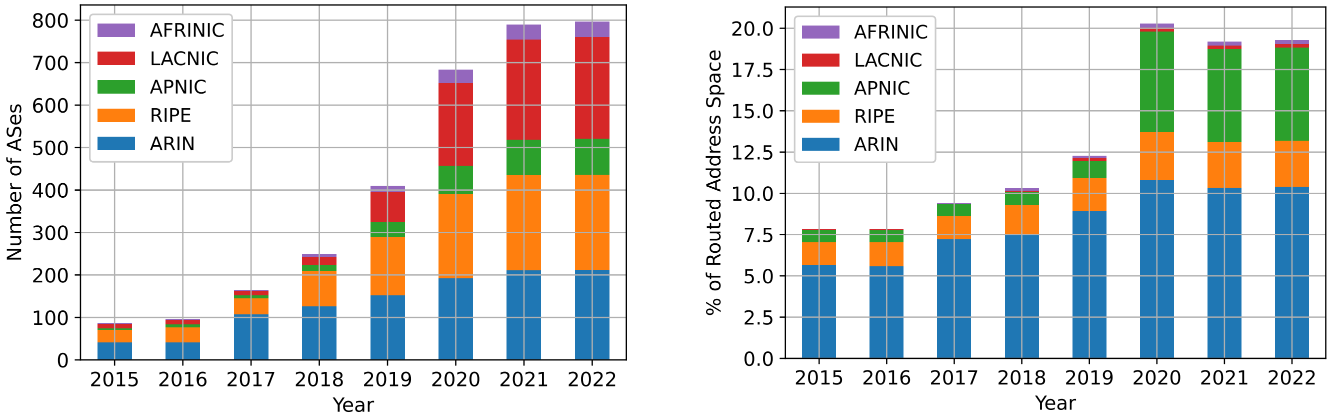
$$\{PO_k : H_{AS1}^{MANRS} \cdots H_{ASm}^{MANRS}, H_{AS1}^{XMANRS} \cdots H_{ASn}^{XMANRS}\}$$

Each AS hegemony value represents how likely an AS is to be on the paths towards PO_k. Equation 9 defines a *MANRS preference score* PS_k^{MANRS} for PO_k, which represents how much more (less) likely PO_k is to go through MANRS transit ASes. PO_k is more likely to propagate through MANRS networks if PS_k^{MANRS} has a value greater than 0. We compare the distribution of *MANRS preference scores* for RPKI Invalid, Valid, and NotFound prefix origin pairs.

$$PS_k^{MANRS} = \sum_{i=1}^{m} AS_i^{MANRS} - \sum_{j=1}^{n} AS_j^{XMANRS} \qquad (9)$$

6.6 Ethical Considerations

All data used in our work is collected from publicly available sources. The Menlo Report [6, 19] states "Researchers have a special obligation to inform individuals or organizations whose resources and welfare may be harmed by information and communication technology research." The results from our work may impact the reputation of



(a) MANRS ASes over time. Brazil (in LACNIC region) added 90 small ASes in 2020 due to local outreach efforts.

(b) Percentage of MANRS routed IPv4 address space. MANRS ASes in the ARIN region announce the most address space.

Figure 4: MANRS ASes and share of routed IPv4 address space over time. The excessive jump in LACNIC ASes was caused by a strong outreach effort by NIC.br in Brazil (184 of the 239 LACNIC ASes are registered in Brazil), but those ASes contributed little additional (0.24%) routed IPv4 address space. The large jump in address space (b) was caused by China Telecom (AS4134, 4.0% of routed v4 address space) joining MANRS. Most large networks (transit providers, CDNs) are from the ARIN region.

companies that provide Internet services. We anonymize the organizations whose reputation could be negatively impacted by our case studies in the paper. We have published our analysis code in a public repository (https://github.com/CAIDA/MANRS_Data_Analysis) for people who might be interested in the details of our case studies. We have disclosed the results of our analysis to the companies we found non-conformant with MANRS, and had voice conversations, email, or text exchanges with all but one.

7 MANRS ECOSYSTEM CHARACTERISTICS

We previously mentioned the steady growth of MANRS membership (Figure 2); in this section we analyze the growth by geographic region, in terms of member ASes (Figure 4a) and address space originated by those ASes (Figure 4b).

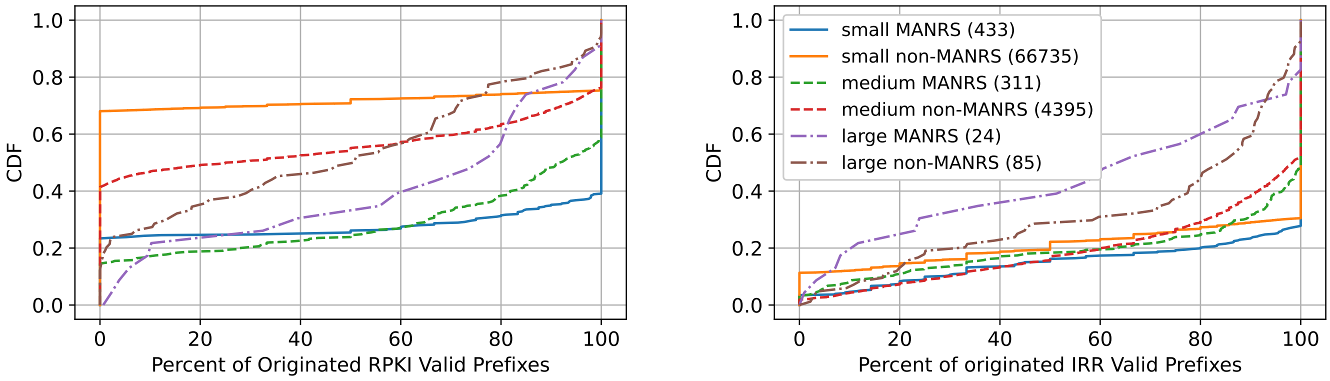
Some anomalies in figures 4a and 4b merit further explanation. The significant jump in LACNIC ASes was caused by a strong outreach effort by Brazil’s national Internet registrar (NIC.br) [53], but those ASes contributed little additional IPv4 address space. In contrast, the large jump in APNIC address space was due mostly to a single ISP – China Telecom – joining MANRS in 2020. Also in 2020, the increase in ARIN routed IPv4 address space was caused by the introduction of the MANRS CDN and Cloud Provider Program, where Amazon (AS16509) represented 1.3% of routed IPv4 address space. In 2021, Level3 (AS3356, now Lumen Technologies) and China Telecom (AS4134) announced fewer prefixes than in 2020, causing a drop in routed address space for those regions (Figure 4b).

Finding 7.0: As of May 2022, 70% MANRS organizations registered all their ASes in MANRS and 82% announced all their address space in BGP through registered ASes.

Many ISPs own more than one AS number, and MANRS allows each organization to specify which of their AS numbers will become MANRS members and thus subject to the MANRS requirements. We used the *as2org dataset*, the *MANRS ISP dataset*, and the *MANRS CDN dataset* to identify sibling ASes (i.e., owned by the same organization) of registered MANRS ASes. We then used the *IHR prefix origin dataset* and estimated that, as of May 2022, 463 (70%) organizations registered all of their AS numbers in MANRS, and 543 (82%) announced IPv4 address space *only* through registered ASes. We found that, as of May 2022, 117 MANRS organizations announced some of their IP address space from ASes that were not MANRS members, and, 8 of these 117 only announced their IP address space from non-MANRS ASes. This means that for those organizations, MANRS conformance could not accurately reflect their routing security practices because some of their originated prefixes were not under MANRS scrutiny. On the contrary, we found 80 organizations that did not register all of their ASes in MANRS but only announced IP address space from the MANRS ASes, indicating that they did not register their quiescent ASes in MANRS. Some examples include cloud hosting companies that only provided services to their customers through their main AS.

8 ACTION 4: PREFIX ORIGINATION BEHAVIOR

MANRS Action 4 in the ISP and CDN programs requires participating ASes to originate prefixes that are either RPKI Valid or IRR Valid (§2.4). In this section, we quantify the validity of prefixes originated by MANRS ASes, compare to that of non-MANRS ASes, and separately check the conformance of ISPs and CDNs to their corresponding action. The MANRS ISP program states that its members must originate at least 90% IRR/RPKI Valid prefixes, while the MANRS CDN program requires 100%.



(a) MANRS ASes were more likely than non-MANRS ASes of the same type to originate RPKI Valid prefixes.

(b) Large MANRS ASes were less likely to originate IRR Valid prefixes than large non-MANRS ASes.

Figure 5: Prefixes originated by MANRS and non-MANRS ASes (shared legend). Large MANRS ASes were more likely to originate RPKI Valid prefixes than IRR Valid prefixes in May 2022.

8.1 RPKI Prefix Validity

Finding 8.1: MANRS ASes were more likely to originate RPKI Valid prefixes compared to non-MANRS ASes in May 2022.

Figure 5 depicts the distribution of the overall percentage of valid prefixes originated by small, medium and large MANRS and non-MANRS ASes. Figure 5a shows that for small networks, RPKI validity distribution was bimodal: in May 2022, prefixes originated by most ASes were either entirely valid or entirely invalid. The bimodal distribution was due to small networks generally originating few prefixes - the 75th percentile of small networks originated only 5 prefixes, and thus could more easily maintain RPKI registration.

Small MANRS ASes were about 2.5 times more likely to register ROAs for their prefixes. Indeed, in May 2022, of 433 small MANRS ASes that originated prefixes, 264 (60.1%) originated only RPKI Valid prefixes while 102 (23.6%) originated only RPKI Invalid/NotFound prefixes. In contrast, of 66,735 small non-MANRS ASes, 45419 (68.1%) ASes originated only RPKI Invalid/NotFound prefixes while 16,492 (24.7%) ASes originated only RPKI Valid prefixes.

The RPKI validity difference between medium MANRS and non-MANRS ASes was similar to that of the small networks, with medium MANRS ASes almost twice as likely to originate only RPKI Valid prefixes. In May 2022, of 311 and 4,395 medium MANRS and non-MANRS ASes, 129 (41.5%) and 1,044 (23.8%) originated only RPKI Valid prefixes, while 46 (14.8%) and 1,818 (41.4%) originated only RPKI Invalid/NotFound prefixes. This also shows a positive impact of MANRS for medium networks.

The validity distribution for large networks was less polarized than that of small and medium networks. However, while all large MANRS ASes originated some RPKI Valid prefixes, we found that 10 (11.8%) non-MANRS ASes did not register ROAs for any prefix they announced and thus originated only RPKI NotFound prefixes. Additionally, another large network (AS23947, an Indonesian ISP) did not originate any RPKI Valid prefix and originated 2 RPKI Invalid prefixes. We further studied this case below. On the other end, 3 (12.5%) out of 24 large MANRS ASes and 5 (5.9%) out of 85 large non-MANRS ASes originated only RPKI Valid prefixes.

We further studied the ASes that originated RPKI Invalid prefixes, since ROV-deploying networks will drop those routes while allowing RPKI NotFound announcements to pass. We found that, in May 2022, no small MANRS AS originated RPKI Invalid prefixes while 489 (0.7%) small non-MANRS ASes originated 1,097 RPKI Invalid prefixes. 9 (2.8%) medium MANRS ASes originated 14 RPKI Invalid prefixes and 198 (4.5%) medium non-MANRS ASes originated 1,401 RPKI Invalid prefixes. We also found that 5 (20.8%) large MANRS ASes originated 13 RPKI Invalid prefixes, while 28 (32.9%) of large non-MANRS ASes originated 724 RPKI Invalid prefixes, showing that MANRS networks were less likely to originate RPKI Invalid announcements.

We note that ASes may originate RPKI Invalid prefixes for legitimate reasons, such as routing misconfigurations. We further analyzed the Indonesian ISP (AS23947) that originated 2 RPKI Invalid prefixes and found that the prefixes were registered under `AS0` in RPKI. Since both prefixes were registered under AS23947 in RADB and have been announced consistently since May 2019, we speculate that this ISP misconfigured its ROA.

8.2 IRR Prefix Validity

Finding 8.2: Large MANRS ASes were less likely to originate IRR Valid prefixes than large non-MANRS ASes in May 2022.

Figure 5b shows that the median large MANRS network originated 63.5% IRR Valid prefixes of all prefixes the network originated, which was lower than the 84.0% median for the non-MANRS counterpart. We speculate this difference is due to (1) IRR being more widely adopted than RPKI and (2) networks that adopt RPKI (especially MANRS networks with high RPKI registration rates) leaving IRR records unmaintained, causing BGP announcements to become IRR Invalid and creating inconsistency between IRR and RPKI records [20].

In contrast, MANRS and non-MANRS ASes in the small and medium classes had similar likelihood in originating IRR Valid prefixes. In May 2022, the percentage of networks that only originated IRR Valid prefixes was 72.3% for small MANRS, 70.0% for small non-MANRS, 52.1% for medium MANRS, and 48.0% for medium non-MANRS.

We also found that non-MANRS networks were more likely to register only in IRR but not RPKI compared to MANRS networks. In May 2022, 23.6% (102) small MANRS ASes versus 65.4% (43,659) small non-MANRS ASes only registered in IRR. Similarly, 14.8% (46) medium MANRS compared to 41.0% (1,803) non-MANRS ASes, and 0% (0) large MANRS ASes compared to 11.8% (10) large non-MANRS ASes, registered only in IRR. Registering only in IRR is less optimal than registering in RPKI, since IRR may contain inaccurate records due to looser validation standards compared to RPKI [20]. The lower fractions of IRR-only MANRS ASes suggests MANRS participants were more likely to adopt RPKI than their non-MANRS counterparts.

8.3 AS Level Conformance to Action 4

After looking at the prefix validity levels of ASes, we looked at how conformant were MANRS ISPs and CDN program participants to required validity levels.

> Finding 8.3: In May 2022, 18 out of 21 (86%) MANRS CDNs were conformant to MANRS Action 4.

We first looked at how conformant MANRS CDN participants were to the Action 4 requirements in the MANRS CDN program, which requires CDNs to originate all prefixes as either RPKI or IRR Valid. We discovered one MANRS CDN AS did not originate any prefix. In the May 1^{st} snapshot of the *IHR prefix origin dataset*, we found that the AS belonged to a company that registered two ASes in MANRS but was only using one AS to originate address space in BGP (similar to other cases mentioned in §7). We considered that AS to be trivially conformant. We found that 17 out of 20 CDN ASes were conformant, i.e., 100% of the prefixes they originated were either RPKI Valid or IRR Valid. The other three ASes still originated more than 98% of their prefixes as either IRR or RPKI Valid. These three ASes were the among the top 5 MANRS CDN ASes who originated the most prefixes, two of which originated more than 3,500 prefixes in BGP. For ASes that originate so many BGP announcements, it is reasonable that a small fraction of them were neither RPKI Valid nor IRR Valid due to their complicated relationship with business customers. We provide case studies on those three CDNs (§8.4).

> Finding 8.4: In May 2022, 810 out of 849 (95%) MANRS ISPs were conformant to MANRS Action 4.

We then analyzed the conformance of MANRS ISP participants to the MANRS ISP program Action 4 requirements, which requires ISPs to have over 90% of the prefixes they originate in BGP to be either IRR or RPKI valid. In the same *IHR prefix origin dataset* snapshot from May 2022, we found 95 ASes that did not originate any prefix and considered them trivially conformant. We then found that only 39 out of 754 ASes were unconformant, where fewer than 90% of the prefixes they originated were IRR or RPKI valid. The 39 ASes belonged to 15 organizations total: 24 ASes were from one large ISP (ISP1), 2 ASes belonged to ISP2, and the remaining 13 organizations each had one AS. The percentages of IRR/RPKI Valid prefixes originated by those 39 ASes ranged from 0% to 89%. We manually inspected some of those ASes with no IRR/RPKI Valid prefixes and found they were stub ASes of large networks who originated fewer than 3 prefixes. We reached out to some of those non-conformant networks and discuss their behavior next.

8.4 Analyzing Unconformant ASes

We manually analyzed 3 unconformant ISPs and 3 unconformant CDNs to shed light on the reasons for their unconformance.

> Finding 8.5: In the 6 unconformant organizations we analyzed, 1% of invalid prefixes were RPKI Invalid. More than 50% mismatching origin ASes between BGP and RPKI/IRR belonged to the same organization or had customer-provider relationships with that organization.

We conducted case studies for all three unconformant CDNs and the three largest unconformant ISPs. Table 1 provides an overview of the prefix-origins that were not MANRS-conformant. The RPKI Invalid and IRR Invalid columns contain the number of prefix-origins with those statuses (prefix-origins in the IRR Invalid column were all RPKI NotFound), which combined is a subset of the total non-MANRS-conformant prefixes of the network (excluded prefix-origins that were both RPKI NotFound and IRR NotFound). The Sibling/C-P columns denote the number of prefix-origins whose BGP origin AS and mismatching RPKI/IRR origin AS belonged to the same organization (i.e., siblings according to the *as2org dataset*) or had a customer-provider relationship (C-P, according to the *as2org dataset*). The Unrelated columns denote the number of remaining prefix-origins whose origin ASes had no relationship.

Most prefix-origins that were not conformant were IRR invalid instead of RPKI Invalid. Since RPKI Invalid prefix-origins suffer more visibility reduction in the global routing table (due to ROV filtering) than RPKI NotFound or IRR Invalid ones, networks who originated IRR Invalid prefixes due to temporary traffic engineering efforts or misconfigurations are less likely to have their services negatively impacted. In addition, in almost all cases, the majority of the RPKI Invalid/IRR Invalid prefix-origins were under the Sibling/C-P category, meaning the lack of compliance was likely due to internal misconfigurations or business dynamics, and thus could be easily corrected.

> Finding 8.6: Five organizations had non-MANRS member ASes that were still MANRS-conformant in May 2022.

All six organizations in our case study were partial MANRS participants according to our analysis using the *as2org dataset*. We also manually checked the AS numbers belonging to those organizations and contacted their networks operators to confirm that they did not register all AS numbers in MANRS. ISP2 mentioned that they intended to register all AS numbers in MANRS but might have missed some newer AS numbers. CDN1 listed only one AS number in MANRS, with 98.7% MANRS-conformant prefix-origins,

	RPKI Invalid (NotFound)	Sibling/C-P	Unrelated	IRR Invalid & RPKI NotFound	Sibling/C-P	Unrelated
CDN1	3	3 (100%)	0	48	38 (79.2%)	10 (20.8%)
CDN2	(1)	0	1 (100%)	0	0	0
CDN3	0	0	0	5	5 (100%)	0
ISP1	1	0	1 (100%)	302	154 (51.0%)	148 (49.0%)
ISP2	8	6 (75.0%)	2 (25.0%)	272	152 (55.9%)	120 (44.1%)
ISP3	1	1 (100%)	0	486	359 (73.9%)	127 (26.1%)

Table 1: Non-conformant prefix origins from the MANRS networks we contacted. CDN2 had no Invalid prefixes and only one RPKI-NotFound prefix. Prefixes in Sibling/C-P were originated by a sibling or customer AS, and no relationship was found for prefixes in the Unrelated column. The RPKI Invalid and IRR Invalid columns each sums the 2 subsequent columns.

but had 11 out of 12 unlisted ASes with 100% conformant prefixes. Similarly for CDN2, CDN3, and ISP1, 75%, 100%, and 100% of their unlisted ASes had 100% conformant prefixes. Compared to the MANRS AS, all unlisted ASes originated fewer prefixes, which agrees with Finding 7.0.

8.5 Conformance Stability

Finding 8.7: Between February 2022 and May 2022, 18 out of 21 MANRS CDNs and 803 out of 849 MANRS ISPs were consistently conformant.

We next looked at MANRS conformance over time. We took 12 weekly snapshots from the *IHR prefix origin dataset* between February 1st, 2022 and May 1st, 2022 (1 snapshot was removed due to missing data) to analyze the conformance stability of MANRS ASes. We found that 17 out of 20 CDNs stayed in conformance for all 12 snapshots, and the 3 CDNs stayed unconformant for 12 weeks. For MANRS ISPs, we found 46 ASes were not conformant in some of the 12 snapshots, where 35 ASes were unconformant consistently across all snapshots. The remaining 11 ASes that were unconformant for fewer than 12 snapshots belonged to 10 organizations. We also found one AS had fluctuating conformance status where its MANRS-conformant prefix-origins dropped below 90% in early February and again in late March. Overall, most ASes were stable in their conformance and consistently stayed either conformant or unconformant.

We looked at the 3 CDNs to study prefix-level conformance stability. For CDN1, we found that between February and May 2022, it stopped announcing 80 prefixes and announced 141 new prefixes, while the active 3,822 prefixes remained conformant. Similarly for CDN2, no prefix changed conformance status over the 3-month period, and for CDN3, only 2 out of 902 prefixes changed conformance status. Overall, prefixes were also likely to have stable conformance status, possibly due to infrequent changes in RPKI and IRR registration.

8.6 Presence in RPKI of MANRS ASes

Finding 8.8: In May 2022, MANRS ASes overall had signed 58% of their routed address space and thus had higher presence in RPKI than non-MANRS ASes.

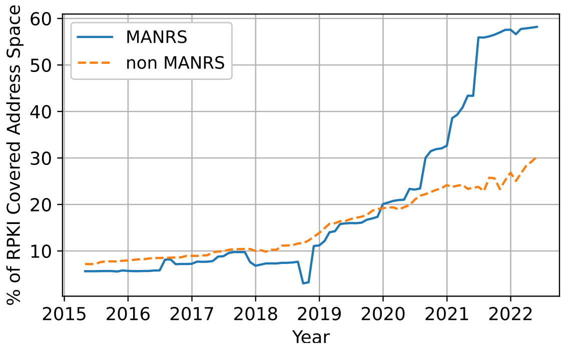


Figure 6: Percentage of RPKI covered address space for MANRS and non-MANRS networks. RPKI covered address space of MANRS networks grew faster in recent years.

We found that in May 2022, 64.8% of the routed IPv4 address space was not covered by RPKI VRPs, while only 5.3% was not covered by IRR route objects. This shows that the RPKI has significant room for growth. We found that MANRS ASes had higher RPKI Saturation than non-MANRS networks.

Figure 6 shows that in May 2022, MANRS networks had reached an RPKI Saturation level of 58.2% (*i.e.,* that fraction of their collective address space had been RPKI signed), greater than 30.2% for non-MANRS networks. Although there is still room for MANRS RPKI Saturation to grow, it is unlikely to reach 100% due to the barriers in RPKI registration of legacy IPv4 address space [21]. We discovered that the significant increase of MANRS RPKI Saturation after 2020 was due to the introduction of the MANRS CDN program, where large CDNs and cloud providers such as Amazon (AS16509) and Cloudflare (AS13335) registered more than 1, 700 prefixes in RPKI. We correlated this change to the increase of ARIN MANRS address space shown in Figure 4b. Similarly, 95.0% of MANRS address space was covered by IRR and 97.6% was MANRS-conformant; 84.6% of non-MANRS address space was covered by IRR and 87.2% was MANRS-conformant.

9 ROUTE FILTERING BEHAVIOR

In addition to requirements on prefix origination, MANRS requires networks to ensure the correctness of customer announcements. In this section, we quantify the RPKI/IRR Invalid prefixes propagated through MANRS networks and originated by their customers, compare to that of the non-MANRS networks, and analyze conformance to the Action 1 requirements.

9.1 RPKI filtering

> Finding 9.1: Large MANRS ASes were less likely to propagate RPKI Invalid announcements compared to non-MANRS ASes in May 2022.

Figure 7a shows the distribution of the percentage of valid prefixes forwarded by networks for small, medium and large, MANRS and non-MANRS networks. It shows that a distinct difference in large networks between MANRS and non-MANRS ones. 11 (45.9%) out of 24 large MANRS networks propagated no RPKI Invalid prefixes compared to 31 (36.0%) out of 86 for large non-MANRS. On the other end, large MANRS networks propagated at most 1.1% of their received announcements that were RPKI Invalid, while large non-MANRS networks propagated at most 6.4%.

In contrast, there was no such difference between MANRS and non-MANRS for small and medium networks. Indeed, small networks propagated almost no RPKI Invalid announcements. Of 118 small MANRS ASes that propagated some prefix, 117 (99.2%) propagated no RPKI Invalid prefixes while 1 (0.8%) propagated only 1 RPKI Invalid prefix. Of 6,140 small non-MANRS networks, 6,083 (99.1%) ASes propagated no RPKI Invalid prefixes. This similarity was because small networks are mostly edge ASes where they have almost no customers and therefore propagate very few prefixes in general: the 75th percentile of small networks propagated only 5 prefixes. Since RPKI Invalid announcements occupied less than 1% of the routing table, it is very unlikely for small networks to encounter RPKI Invalid announcements.

Similarly, Medium MANRS and non-MANRS networks were almost indistinguishable with respect to the percentage of propagated RPKI Invalid announcements. Of 310 and 4,405 medium MANRS and non-MANRS networks, 283 (91.3%) and 4,072 (92.4%), respectively, propagated no RPKI Invalid prefixes.

9.2 IRR filtering

> Finding 9.2: In May 2022, small MANRS ASes were less likely to propagate IRR Invalid announcements compared to small non-MANRS ASes. Large MANRS ASes were less likely to propagate more than 9% of IRR Invalid announcements, but were more likely to propagate more than 7% of IRR Invalid announcements.

Figure 7b shows small MANRS networks were less likely to propagate IRR Invalid prefixes than small non-MANRS networks. However, Medium MANRS and non-MANRS networks had similar likelihood of propagating IRR Valid prefixes. In May 2022, the percentage of networks that only originated IRR Valid prefixes was 94.1% for small MANRS, 85.5% for small non-MANRS, 59.4% for medium MANRS, and 63.0% for medium non-MANRS. Large MANRS networks propagated at most 25.5% IRR Invalid announcements of all its received announcements, which was lower than the 74.5% of its non-MANRS counterpart. We speculate this difference was due to inconsistent IRR adoption and filtering among ISPs [54], and especially among non-MANRS networks without standard filtering procedures. We further calculated that the variance of the percentages of propagated IRR Invalid announcements for large MANRS networks was 39, while it was 134 for large non-MANRS networks, which was consistent with our speculation.

9.3 AS Level Conformance to Action 1

> Finding 9.3: Over 83% of MANRS ASes were fully conformant to MANRS Action 1.

To assess networks' level of conformance to the filtering requirement, we combined members of MANRS ISPs and CDNs programs and calculated their fractions of propagated MANRS-unconformant announcements from their *direct customers*. Since the MANRS ISP program Action 1 does not provide a threshold, and the MANRS CDN program Action 1 only describes a validation flow in its recommended additional requirements, a MANRS AS is *fully* Action 1 conformant if *none* of the announcements they propagate are MANRS-unconformant. MANRS ASes that did not propagate any announcements are considered trivially conformant

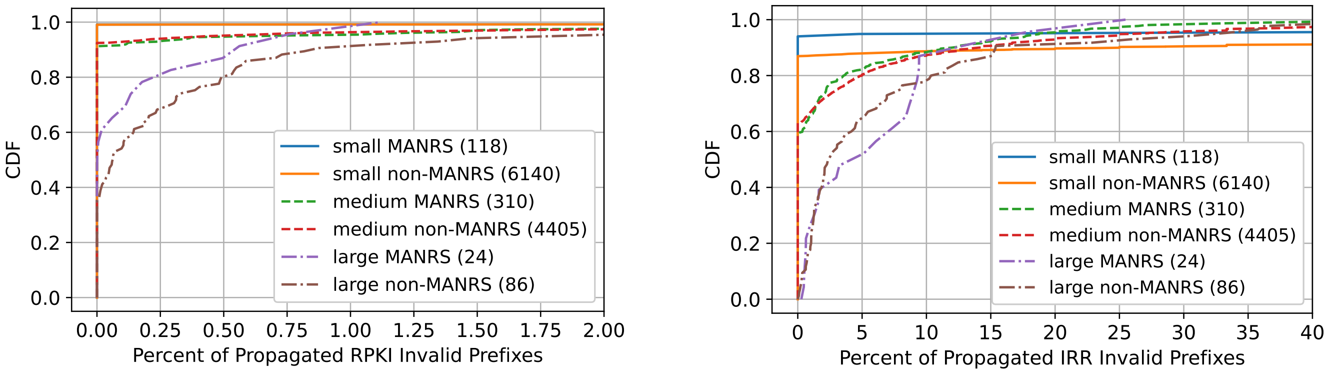
Figure 8 shows that in May 2022, all types of MANRS ASes were more likely to be Action 1 conformant than their non-MANRS counterpart. All large MANRS ASes propagated less than 15% MANRS-unconformant prefixes, while the highest percentage of MANRS-unconformant prefixes propagated by large non-MANRS ASes was 41.4%. The long tails for small and medium non-MANRS ASes both end at 100%, where we found one medium non-MANRS AS propagated more than 800 RPKI or IRR Invalid prefixes. To emphasize, those announcements were received from the direct customers of the ASes, hence the fewer ASes per category (Figure 8 legend vs. Figure 7b).

Table 2 lists the number of fully conformant MANRS ASes. The Total Transit column shows the number of MANRS ASes that actually propagated some announcement. The remaining MANRS ASes that did not propagate any announcements we considered trivially conformant. We obtain the Total Conformant values by adding the number of trivially conformant ASes to the number of Transit Conformant ASes. We found that 347 out of 451 small MANRS ASes did not provide transit to any prefixes at all. Overall, all categories of MANRS ASes were more than 93% conformant to Action 1.

9.4 MANRS RPKI Filtering Effectiveness

> Finding 9.4: RPKI Invalid BGP announcements were more likely to propagate through non-MANRS networks than MANRS networks.

To measure whether RPKI Invalid announcements were more likely to propagate through MANRS transit networks, we first estimated how likely BGP announcements were to propagate through MANRS networks by calculating the *MANRS preference scores* for RPKI Valid and RPKI NotFound announcements. Figure 9 depicts



(a) Percent of RPKI Invalid prefixes propagated by MANRS and non-MANRS networks by type. Large MANRS networks propagated limited RPKI Invalid announcements, no more than 1.1% of their total.

(b) Percent of IRR Invalid prefixes propagated by MANRS and non-MANRS networks by type. Large MANRS networks propagated less than 25% IRR Invalid prefixes.

Figure 7: RPKI and IRR Invalid prefixes propagated by MANRS and non-MANRS networks in May 2022.

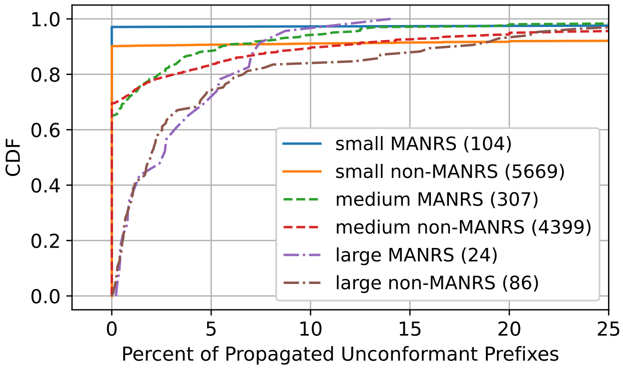


Figure 8: Unconformant prefixes propagated by MANRS and non-MANRS networks by network type. The median large MANRS AS propagated only 2.5% MANRS-unconformant prefixes.

	Transit Conformant	Total Transit	Total Conformant	Total MANRS
Small	101 (97.1%)	104	448 (99.3%)	451
Medium	200 (65.1%)	307	212 (66.4%)	319
Large	0 (0%)	24	0 (0%)	24

Table 2: Action 1 (filtering) conformance. ASes with no customers are conformant by default and included in right side columns. Results for transit ASes are shown in left side columns. Only 23% of small MANRS ASes provided transit and 97.1% of them were conformant.

their distribution and shows that 34% of RPKI Valid prefix origin pairs preferred to transit via MANRS networks (*MANRS preference scores* greater than 0). Similarly for RPKI NotFound announcements,

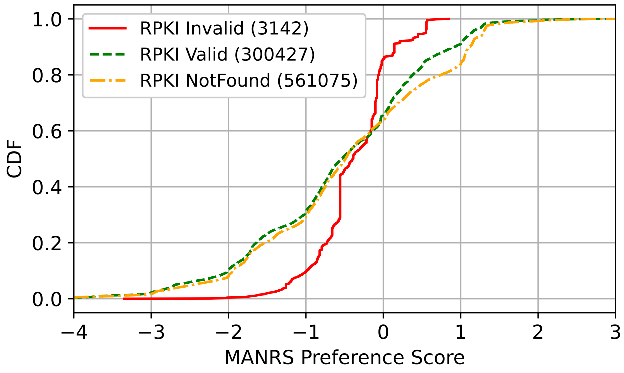


Figure 9: Prefix preference for MANRS transit by RPKI status (0 means no preference). RPKI Invalid BGP announcements were less likely to propagate through MANRS networks than non-MANRS networks.

36% preferred MANRS transit networks. The similarity between these *MANRS preference scores* is expected as networks propagate RPKI Valid and NotFound in the same way, even if they implement ROV. In contrast, only 14% of RPKI Invalid prefix origin pairs preferred MANRS networks, showing that MANRS networks collectively were more effective in filtering RPKI Invalid announcements than non-MANRS networks, and therefore suggesting better routing security.

10 DISCUSSION

MANRS aims to improve Internet routing security by promoting security best practices to network operators and our findings confirm that MANRS participant are more likely to follow best practices than other similar networks in the Internet. However, within MANRS, not all networks take the MANRS mandate with the same rigour. For instance, we reported our findings to operators at six large network operators to inform them about their unconformant announcements. We got replies from five of them. Two networks responded that they had discovered the cause of the unconformant prefix and would fix it. We were able to confirm that they have corrected the unconformant announcements at the time of writing. The remaining 3 networks used our findings to investigate the problem.

In addition, we also surveyed these 6 networks regarding their opinions on the helpfulness of the monthly MANRS conformance reports and we received varying responses. Three networks reported that they read the conformance reports, but needed more actionable information. The remaining two networks were not aware of such reports; likely we reached someone besides the MANRS POC for that network.

We hope to use our work to help MANRS provide more detailed information to their participants and help network operators address routing issues in a timely manner. In addition, two operators told us that it was hard to meet the MANRS Actions requirements due to complicated business relationships and outdated equipment. We hope our work can help the MANRS program optimize its utility for different types of networks.

In the future, MANRS can increase its positive influence on routing security by being a forum to build consensus on the appropriate direction and next steps for routing security and support the operationalization of security protocols and training of networks operators.

11 LIMITATIONS

Limited routing table visibility We used public BGP data collected by Routeviews and RIPE RIS, which are known to have limited number of vantage points and limited visibility of the Internet. Our analysis of the MANRS routing ecosystem was bound by such limitations. For example, we may have overestimated the conformance of a MANRS network if we were unable to observe some unconformant prefix origins (§8).

Incomplete route filtering inference Our analysis in §9 may have underestimated the propagation of RPKI/IRR Invalid prefixes for each AS. Since we cannot directly infer whether an AS is deploying route filtering, we observe whether invalid prefix origins traverse that AS. However, if any other AS along the AS-path filtered out the invalid prefix origin, our methodology will assume the AS in question performed route filtering.

12 SUMMARY AND FUTURE WORK

This paper provides a first look into the MANRS networks' conformance to routing security practices. We investigated the geographical and address space distribution of MANRS members, and found the presence of very large networks as part of MANRS and a large proportion of MANRS members in Brazil. Our analysis of routing registry data (IRR and RPKI) revealed that MANRS members were more likely to register and maintain routing objects than non-MANRS members. The analysis on route filtering showed that MANRS members were likely to have better routing practices than non-MANRS members. We inferred that, as of May 2022, the vast majority of, but not all, MANRS members were conformant with MANRS actions, and found that conformance for very large networks is difficult to achieve.

This study demonstrates the need to continually assess the conformance of members for the prosperity of the MANRS initiative, and the difficulties to automate such conformance checks. In future work, we plan to further study the impact of MANRS by comparing the number of routing incidents before and after the launch of MANRS. We also plan to extend this study to actions that are not related to routing and to another MANRS program, such as the IXP Program. We will make our analysis code available to network operators to help them monitor their state of routing security and to non-MANRS networks for checking if they meet the requirements to join MANRS.

ACKNOWLEDGMENTS

This work is based on research sponsored by U.S. NSF grants CNS-2120399, OAC-2131987, and OAC-1724853. The views and conclusions are those of the authors and do not necessarily represent endorsements, either expressed or implied, of the sponsors. We thank our shepherd Italo Cunha for providing valuable feedback on our paper. We also thank the network operators from various organizations who shared their practical experience in improving routing security.

REFERENCES

[1] 2022. MANRS Observatory. (2022). https://observatory.manrs.org/#/overview
[2] 2022. Mutually Agreed Norms for Routing Security. (2022). https://www.manrs.org
[3] 2022. Peering with Google. (2022). https://peering.google.com/#/options/peering
[4] 2022. SIX IRR Tutorial. (2022). https://www.seattleix.net/irr-tutorial
[5] Cengiz Alaettinoglu, Curtis Villamizar, Elise Gerich, David Kessens, David Meyer, Tony Bates, Daniel Karrenberg, and Marten Terpstra. 1999. *Routing Policy Specification Language (RPSL)*. RFC 2622.
[6] Michael Bailey, David Dittrich, Erin Kenneally, and Douglas Maughan. 2012-03. The Menlo Report. *IEEE Security & Privacy* 10 (2012-03), 71–75.
[7] Jay Borkenhagen. 2019. AT&T/AS7018 now drops invalid prefixes from peers. (2019). https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html
[8] CAIDA. 2022. AS Rank. (2022). https://asrank.caida.org
[9] CAIDA. 2022. AS Relationships. (2022). https://www.caida.org/catalog/datasets/as-relationships
[10] CAIDA. 2022. Inferred AS to Organization Mapping Dataset. (2022). https://www.caida.org/catalog/datasets/as-organizations
[11] CAIDA. 2022. Routeviews Prefix to AS mappings Dataset (pfx2as) for IPv4 and IPv6. (2022). https://www.caida.org/catalog/datasets/routeviews-prefix2as
[12] Massimo Candela. 2022. A One-Year Review of RPKI Operations, RIPE 84. (May 2022). https://ripe84.ripe.net/archives/video/741/
[13] Ben Cartwright-Cox. 2019. The Year of RPKI on the Control Plane. (2019). https://blog.benjojo.co.uk/post/the-year-of-rpki-on-the-control-plane
[14] Wenqi Chen, Zhiliang Wang, Dongqi Han, Chenxin Duan, Xia Yin, Jiahai Yang, and Xingang Shi. 2022. ROV-MI: Large-Scale, Accurate and Efficient Measurement of ROV Deployment. In *Network and Distributed System Security Symposium.*
[15] Taejoong Chung, Emile Aben, Tim Bruijnzeels, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, Roland van Rijswijk-Deij, John Rula, and Nick Sullivan. 2019. RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. In *Proceedings of the Internet Measurement Conference (IMC '19).* Association for Computing Machinery, New York, NY, USA, 406–419.
[16] Luca Cittadini, Wolfgang Mühlbauer, Steve Uhlig, Randy Bush, Pierre Francois, and Olaf Maennel. 2010. Evolution of internet address space deaggregation: myths and reality. *IEEE Journal on Selected Areas in Communications* 28, 8 (2010), 1238–1249.
[17] Federal Communications Commission. 2022. FCC Launches Inquiry into Internet Routing Vulnerabilities. (2022). https://www.fcc.gov/document/fcc-launches-inquiry-internet-routing-vulnerabilities
[18] Amogh Dhamdhere and Constantine Dovrolis. 2011. Twelve Years in the Evolution of the Internet Ecosystem. *IEEE/ACM Transactions on Networking* 19, 5 (Oct 2011), 1420–1433.
[19] David Dittrich, Michael Bailey, and Erin Kenneally. 2013-10. *Applying Ethical Principles to Information and Communication Technology Research: A Companion to the Menlo Report.* Technical Report. U.S. Department of Homeland Security.

[20] Ben Du, Gautam Akiwate, Thomas Krenc, Cecilia Testart, Alexander Marder, Bradley Huffaker, Alex C Snoeren, and KC Claffy. 2022. IRR Hygiene in the RPKI Era. In *International Conference on Passive and Active Network Measurement*. Springer, 321–337.

[21] Alain Durand. 2020. *Resource Public Key Infrastructure (RPKI) Technical Analysis*. Technical Report. ICANN. https://www.icann.org/en/system/files/files/octo-014-02sep20-en.pdf

[22] Romain Fontugne, Anant Shah, and Emile Aben. 2018. The (thin) bridges of as connectivity: Measuring dependency using as hegemony. In *International Conference on Passive and Active Network Measurement*. Springer, 216–227.

[23] Takafusa Hori. 2021. *IIJ's Efforts with RPKI*. Technical Report. https://www.iij.ad.jp/en/dev/iir/pdf/iir_vol50_focus1_EN.pdf

[24] Geoff Huston and Joao Damas. 2020. Measuring Route Origin Validation. (2020). https://www.potaroo.net/ispcol/2020-06/rov.html

[25] Geoff Huston, Mattia Rossi, and Grenville Armitage. 2011. Securing BGP — A Literature Survey. *IEEE Communications Surveys Tutorials* 13, 2 (2011), 199–222.

[26] Internet Initiative Japan. 2022. Internet Health Report. (2022). ttps://ihr.iijlab.net/ihr/en-us/rov

[27] Stephen Kent, Charles Lynn, and Karen. Seo. 2000. Secure Border Gateway Protocol (S-BGP). *IEEE Journal on Selected Areas in Communications* 18, 4 (2000), 582–592.

[28] Akmal Khan, Hyun-chul Kim, Taekyoung Kwon, and Yanghee Choi. 2013. A Comparative Study on IP Prefixes and Their Origin Ases in BGP and the IRR. *SIGCOMM Comput. Commun. Rev.* 43, 3 (July 2013), 16–24.

[29] Brenden Kuerbis and Milton Mueller. 2017. Internet routing registries, data governance, and security. *Journal of Cyber Policy* 2, 1 (2017), 64–81.

[30] Matt Lepinski and Stephen Kent. 2012. *An Infrastructure to Support Secure Internet Routing*. RFC 6480. http://www.rfc-editor.org/rfc/rfc6480.txt

[31] Matt Lepinski and Kotikalapudi Sriram. 2017. *BGPsec Protocol Specification*. RFC 8205.

[32] Matthew Luckie, Robert Beverly, Ryan Koga, Ken Keys, Joshua A. Kroll, and k claffy. 2019. Network Hygiene, Incentives, and Regulation: Deployment of Source Address Validation in the Internet. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. Association for Computing Machinery, New York, NY, USA, 465–480.

[33] Doug Madory. 2018. BGP Hijack of Amazon DNS to Steal Crypto Currency. (2018). https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/

[34] Doug Madory. 2020. Visulizing Routing Incidents in 3D. (2020). https://ripe80.ripe.net/presentations/14-3dleak_viz_madory_ripe.pdf

[35] Apostolaki Maria, Zohar Aviv, and Vanbever Laurent. 2017. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. In *Security and Privacy (SP), 2017 IEEE Symposium on*. IEEE.

[36] Inc Merit Network. 2018. Internet Routing Registry. (2018). http://www.irr.net

[37] Inc Merit Network. 2022. RADb. (2022). http://www.radb.net

[38] Prodosh Mohapatra, John Scudder, David Ward, Randy Bush, and Rob Austein. 2013. *BGP Prefix Origin Validation*. RFC 6811. http://www.rfc-editor.org/rfc/rfc6811.txt

[39] RIPE NCC. 2008. YouTube Hijacking: A RIPE NCC RIS case study. (2008). https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

[40] RIPE NCC. 2022. Routing Information System (RIS). (2022). https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris

[41] NTT. 2022. Routing Registry - RPKI based BGP Origin Validation. (2022). https://www.gin.ntt.net/support-center/policies-procedures/routing-registry/#RPKI

[42] University of Oregon. 2022. Route Views Project. (2022). http://www.routeviews.org/routeviews

[43] P.C. van Oorschot, Tao Wan, and Evangelos Kranakis. 2007. On Interdomain Routing Security and Pretty Secure BGP (PsBGP). *ACM Trans. Inf. Syst. Secur.* 10, 3 (July 2007), 11–es.

[44] Anirudh Ramachandran and Nick Feamster. 2006. Understanding the Network-Level Behavior of Spammers. In *Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '06)*. Association for Computing Machinery, New York, NY, USA, 291–302.

[45] Andreas Reuter, Randy Bush, Italo Cunha, Ethan Katz-Bassett, Thomas C. Schmidt, and Matthias Wählisch. 2018. Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering. *SIGCOMM Comput. Commun. Rev.* 48, 1 (apr 2018), 19–27.

[46] RIPE NCC. 2022. RPKI Dataset. (2022). https://ftp.ripe.net/ripe/rpki

[47] Andrei Robachevsky. 2020. Improving routing security through concerted action. (2020). https://ripe80.ripe.net/wp-content/uploads/presentations/3-202005-MANRS-RIPE80.pdf

[48] Nils Rodday, Ítalo Cunha, Randy Bush, Ethan Katz-Bassett, Gabi Dreo Rodosek, Thomas C Schmidt, and Matthias Wählisch. 2021. Revisiting RPKI Route Origin Validation on the Data Plane. In *Proc. of Network Traffic Measurement and Analysis Conference (TMA). IFIP. accepted for publication.*

[49] Sojun Ryu. 2022. Post Mortem of KlaySwap Incident through BGP Hijacking. (2022). https://medium.com/s2wblog/post-mortem-of-klayswap-incident-through-bgp-hijacking-en-3ed7e33de600

[50] Pavlos Sermpezis, Vasileios Kotronis, Petros Gigis, Xenofontas Dimitropoulos, Danilo Cicalese, Alistair King, and Alberto Dainotti. 2018. ARTEMIS: Neutralizing BGP Hijacking Within a Minute. *IEEE/ACM Transactions on Networking* 26, 6 (2018), 2471–2486.

[51] Aftab Siddiqui. 2020. Big route leak shows need for routing security. (2020). https://www.manrs.org/2020/07/big-route-leak-shows-need-for-routing-security

[52] Internet Society. 2018. *Routing Security for Policymakers: An Internet Society White Paper*. White Paper. MANRS. https://www.manrs.org/wp-content/uploads/2018/10/Routing-Security-for-Policymakers-EN.pdf

[53] Internet Society. 2020. Making the Most of Our MANRS Partnerships – NIC.br and Brazil Lead the MANRS Pack. (2020). https://www.manrs.org/2020/06/making-the-most-of-our-manrs-partnerships-nic-br-and-brazil-lead-the-manrs-pack

[54] Cecilia Testart. 2018. Reviewing a Historical Internet Vulnerability: Why Isn't BGP More Secure and What Can We Do About it? TPRC.

[55] Cecilia Testart and David Clark. 2021. A Data-Driven Approach to Understanding the State of Internet Routing Security. In *Research Conference on Communications, Information, and Internet Policy (TPRC)*.

[56] Cecilia Testart, Philipp Richter, Alistair King, Alberto Dainotti, and David Clark. 2020. To Filter or not to Filter: Measuring the Benefits of Registering in the RPKI Today. In *International Conference on Passive and Active Network Measurement*. Springer, 71–87.

[57] Pierre-Antoine Vervier, Olivier Thonnard, and Marc Dacier. 2015. Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks.. In *The Network and Distributed System Security Symposium (NDSS)*.

[58] Matthias Wählisch, Robert Schmidt, Thomas C. Schmidt, Olaf Maennel, Steve Uhlig, and Gareth Tyson. 2015. RiPKI: The Tragic Story of RPKI Deployment in the Web Ecosystem. In *Proc. of Fourteenth ACM Workshop on Hot Topics in Networks (HotNets)*. ACM, New York.