The Threat Landscape of IP Leasing in the Post-RPKI Era

Abstract—**Short-term IPv4 leasing is on the rise, allowing address owners (lessors) to rent out spare address blocks to lessees who rely on them for critical operations. Yet under existing RPKI practices, the lessor remains the recognized authority, retaining full control over the ROAs needed to validate BGP announcements.**

This paper uncovers how such arrangements fundamentally clash with the assumptions of route origin validation: even after leasing out an address block, the lessor can unilaterally invalidate the lessee's announcements, causing RPKI-enforcing ASes to drop or redirect traffic. We show that a malicious lessor can leverage RPKI to covertly hijack a leased prefix by feeding "lease-compliant" ROAs to select relying parties while presenting "rogue" ROAs to the rest of the Internet.

Through experiments on two major cloud platforms and the PEERING testbed, spanning multiple continents, we confirm that these attacks can reroute leased-prefix traffic with little visibility to the lessee or standard monitoring tools. We further illustrate scenarios in which a rogue lessor intercepts TLS certificate validation or executes region-specific hijacks, highlighting the severity of such threats. Finally, we propose practical mitigations, including multi-RP ROA verification, delegating ROA authority to neutral brokers, and adopting partial delegation in RIR portals.

By exposing the interplay between IP leasing and RPKI, we aim to spur both policy reforms and technical advancements that strengthen routing security in the face of ever-growing address shortages.

1. Introduction

The IPv4 address space has been nearing depletion for over a decade [64], prompting the Regional Internet Registries (RIRs) to impose allocation constraints and encourage the adoption of IPv6. Yet, despite these measures and the continued growth of IPv6, market demand for IPv4 has not subsided. In fact, it has accelerated the emergence of a *leasing economy*, where addresses are temporarily rented rather than permanently transferred [19]. Such leases range from small blocks for experimental projects to large address pools critical for hosting or content delivery operations.

Under conventional RIR policy, the named owner of a prefix is assumed to both *hold* and *use* it; however, today's short-term leasing departs from that premise: the lessor remains the official owner in RIR records, while an unrelated lessee operates the address space. For the lessee, this can be economical and convenient compared to a formal transfer. Yet, with Resource Public Key Infrastructure (RPKI) [7] in place, the lessor still wields ultimate authority over ROAs, which declare the legitimate origin AS of a prefix. That power can be benign or damaging: a well-intentioned lessor might inadvertently fail to update ROAs on time, disrupting the lessee's connectivity; a hostile one could revoke or override the lessee's ROA at will, causing networks that enforce ROV [6] to drop or reroute traffic.

Some view leasing contracts as a safeguard: they argue a lessor, contractually bound to lease a prefix, would not risk legal trouble by sabotaging it. In practice, however, such protection varies widely by jurisdiction. Many short-term or "micro-lease" deals operate under thin margins, through third-party brokers, and enforcement is neither consistent nor immediate. A malicious or obscure lessor might lie in wait until the lessee's enterprise becomes lucrative—e.g., a cryptocurrency service—then deliberately hijack traffic at a pivotal moment to steal assets or tarnish the lessee's reputation. Publishing a rogue ROA does leave behind a cryptographic trace, but identifying or resolving the incident in real time can prove difficult, and the damage often unfolds long before any legal recourse.

Worsening the problem is RPKI's hierarchical design, which allows lessors to run their own publication points and present inconsistent ROAs globally. A lessor could display "lease-compliant" ROAs to some RPs, while showing "rogue" ROAs to the broader Internet, enabling targeted hijacks that go undetected by the lessee's limited vantage points. As ROV deployment expands, an invalid prefix can lose reachability for large segments of the Internet, underscoring the severity of these risks.

In this paper, we show why short-term IP leasing has become a fertile ground for subtle but serious routing security failures. Our main contributions are:

- We demonstrate how leasing fundamentally clashes with route origin validation: even when a prefix is rented out, the official owner continues to control ROAs, giving them the power to disrupt or hijack the lessee's traffic.
- We explain how a malicious lessor can perform stealthy hijacks by feeding "lease-compliant" ROAs to certain relying parties, while distributing conflicting "rogue" ROAs elsewhere—bypassing typical BGP/RPKI monitoring and even multi-vantage-point checks.
- We confirm these attacks in live RPKI-enabled environments spanning two cloud platforms and the PEERING testbed across four continents, showing that real-world networks are susceptible.
- We propose mitigations: stricter global ROA consistency checks, shifting ROA authority to neutral intermediaries

(brokers), and enabling partial delegation at RIRs so owners can lease out sub-blocks without endangering the entire prefix.

In essence, while ROV improves security for legitimate owners, it also places dangerous leverage in the hands of lessors when the operational user (lessee) differs from the official titleholder. By analyzing prevalent leasing models, describing concrete hijacks, and proposing pragmatic fixes, we call for rethinking RPKI authority so that routine short-term rentals do not undermine the resilience of the global routing ecosystem.

2. Background and Related Work

2.1. BGP and RPKI

BGP is the de facto protocol for exchanging routing information among ASes on the Internet. It operates as a path-vector protocol, where each AS advertises available routes along with the list of ASes a route traverses, forming a path. This mechanism helps construct a global routing table for selecting the best route to any destination. BGP's decision process typically prioritizes more specific routes (longer prefixes) over less specific ones; for example, an AS may receive announcements for 45.3.0.0/16 (origin AS40220) and 45.3.0.0/24 (origin AS13527):

```
45.3.0.0/16 AS_PATH: AS174   AS40220
45.3.0.0/24 AS_PATH: AS20473 AS13527
```

Because the /24 is more specific, BGP selects 45.3.0.0/24 route to forward traffic.

However, BGP lacks inherent security mechanisms, leading to critical vulnerabilities. In particular, routers usually trust incoming routing advertisements without verifying authenticity, making it possible for attackers to hijack prefixes they do not own. This can divert traffic to the attacker's network.

RPKI addresses these weaknesses by providing a cryptographic framework to map IP prefixes to legitimate origin ASes and filter non-authenticated BGP announcements. Its design involves: (1) enabling IP address holders to create Route Origin Authorizations (ROAs) that declare which ASes are authorized to announce their prefixes, and (2) using those ROAs to validate and discard invalid routes through a process called Route Origin Validation (ROV).

2.1.1. Creating ROAs. The first step of using RPKI is for IP address space holders to create ROAs. A ROA is a cryptographically signed object that associates an IP prefix with an authorized ASN. It specifies the ASN permitted to originate BGP announcements for a prefix, along with optional constraints such as maximum prefix length. Although it is common for the IP owner's ASN to appear in a ROA, other ASes can also be listed, for example in scenarios involving DDoS protection [31].

ROAs are published through RPKI CAs, which are generally operated by RIRs or delegated bodies like National Internet Registries (NIRs) and Local Internet Registries (LIRs). Once registered, ROAs are incorporated into the global RPKI publication points (PPs), allowing network operators to retrieve and validate them.

2.1.2. ROA Management and Distribution. There are two primary methods to publish ROA objects, each with distinct operational and security trade-offs:

- Hosted RPKI services: RIRs offer hosted services, which are generally accessed through the operator's account on the RIR's website such as ARIN [63]. This approach shifts the responsibility for certificate and repository management to the RIR, alleviating the burden on network operators by handling key management, certificate rotation, and publication processes on their behalf.
- Delegated RPKI: Network operators retain full control over their keys, certificates, and publication points. They independently create and sign ROAs and coordinate with the RIRs to ensure the prefixes in ROAs match the IP resources listed in the CA certificates [25], and that ROAs appear in the RPKI manifest [35]. This manifest is signed and hosted by resource owners, rather than by RIRs. The operator's publication point URI is included in the RPKI CA certificate, signed by the parent CA (an RIR or NIR) and published under the parent's repository.

2.1.3. Deploying ROV and its Impact. RPKI validation software, or Relying Party (RP) software, starts by retrieving data from all five RIR repositories. It then follows references to any additional publication points listed in RPKI CA certificates, ensuring it collects ROAs from the entire RPKI hierarchy rather than relying solely on RIR-operated repositories. Once collected, each ROA is distilled into a Validated ROA Payload (VRP), a tuple that usually includes an ASN, a prefix, and a maximum prefix length. These VRPs are then provided to routers using the RPKI to Router (RTR) protocol [7], enabling ROV [36].

During ROV, the router checks whether the IP prefix in an incoming BGP announcement is *covered* by any VRP. If so, the router further checks whether the VRP exactly matches the announcement: the announced prefix must fall within the VRP prefix, the originating ASN must match the VRP, and the announced prefix length must not exceed the VRP's maximum length.

A BGP announcement that passes both the coverage and exact match checks is deemed *Valid*. An announcement is *Invalid* if it is covered by a VRP's prefix range but fails the exact match (e.g., the ASN or prefix length do not align). Finally, an announcement is *Unknown* if it is not covered by any VRP at all.

When a BGP announcement becomes RPKI-invalid, it is dropped by ROV-deployed routers and removed from the Forwarding Information Base (FIB). As a result, the route can become unreachable in the data-plane. Past works have explored this connectivity impact [14], [46], [47], [61]; a measurement study [50], conducted via online advertisements, found that 21.4% of clients on the Internet are unable to reach RPKI-invalid prefixes lacking alternative routes.

2.1.4. Security Risks in RPKI. RPKI empowers CA operators to manage publication points with little restriction, while relying parties must regularly retrieve RPKI objects from *all* such publication points. This structure creates an attractive target for compromised or misbehaving repositories.

Cooper et al. [13] initially considered how a malicious RPKI publication point might revoke or overwrite ROAs permitted by the CA certificate. However, they focused on an owner abusing its ROAs globally—a scenario with weak incentives and changes that would be evident to every relying party. Subsequent research by Hlavacek et al. [27], [28] revealed how adversaries can degrade or even disable RPKI validation by feeding corrupted objects through controlled publication points, thus undermining ROV's protections against BGP hijacking.

Although these studies examined misbehaving publication points, our work highlights a *new* dimension in the context of IP leasing. The boom in leasing markets, concurrent with RPKI's adoption, creates a situation where rogue lessors can exploit RPKI's hierarchical model to hijack a lessee's prefix. By selectively distributing conflicting ROAs to different relying parties, a malicious lessor can covertly invalidate a lessee's announcements, evade standard monitors, and circumvent existing defenses.

2.2. The Evolving IPv4 Leasing Landscape

2.2.1. How IP Leasing Works. IP leasing typically involves three parties: a *lessor* (the RIR-recognized owner of IPv4 prefixes), a *broker* (the intermediary who arranges the lease), and a *lessee* (the renter of the address space). Unlike formal transfers through RIRs, leases rarely modify the registry's ownership records to reflect the lessee. Instead, the lessor grants permission—often via a simple contract—for the lessee to announce the prefix, leaving the RIR database to still list the lessor as the official holder.

In theory, reassigning (or sub-allocating) a block through the RIR portal is possible [15], but it typically assumes an upstream ISP-customer relationship, something rarely found in these commercial leasing deals. To circumvent that, brokers often register themselves as maintainers or technical contacts for the leased sub-block without formally reallocating it [51]. This allows quick, short-term leases in a largely informal setting, and does not necessarily violate the practices of RIRs that bar sub-allocations specifically for leasing purposes.

For a lessee, the leasing route is attractive: it can be cheaper and more flexible than seeking a dedicated RIR allocation. The lessee simply pays recurring fees for the duration of usage, gaining a block of IPv4 addresses with minimal administrative overhead. Meanwhile, *ultimate authority remains with the lessor*, who can reclaim the prefix or modify the lease terms at any time.

Such a lightly regulated marketplace leaves multiple points of uncertainty. Lessees rely on address space they do not legally own, brokers focus on short-term rentals without changing RIR databases, and the lessor retains near-absolute power. Some lessors carve large pools into numerous small leases, amplifying operational complexity and security risks. While this flexibility addresses escalating demand for IPv4 resources, it also creates a "gray market" that can leave lessees exposed to abrupt policy shifts, broken contracts, and sudden revocations.

2.2.2. ROA Management in IP Leasing. Since a lease is not an official transfer, *ROA management typically remains under the control of the lessor.* Thus, the lessee or broker must directly coordinate with the lessor (over email or phone communication) to update the ROAs. However, certain arrangements allow brokers or lessees to manage ROAs directly:

- Reassignment with ROA Control: The lessor formally reassigns the prefix to the broker or lessee, allowing the lessee to create and manage ROAs independently. In most RIRs, this process effectively removes the lessor's ability to alter ROAs. However, reassignment practices vary across RIRs and may include notable restrictions; for example, ARIN does not provide the reassignment receiver with direct ROA control, leaving ownership and management with the original lessor [15]. In contrast, other RIRs grant full ROA access to the reassignment receiver (i.e., broker).[1]
- RIR Access Delegation: The lessor grants the broker direct access (e.g., maintainer roles, API credentials) to its RIR account, allowing the broker to manage ROAs and registry data on the lessor's behalf. Although this streamlines updates, the lessor can still change or revoke ROAs at any time without notifying the broker or lessee.
- RPKI CA Delegation: Rather than sharing credentials, the lessor can formally delegate ROA management authority to the broker by creating an RPKI CA certificate for specific prefixes and ASNs. The broker then operates its own publication point and manages its own keys. We identify three possible delegation approaches:
  (a) RIR-Level (Complete) Delegation: The lessor uses the RIR's RPKI portal to generate a child request [5], handing over *all* IP prefixes under the account to the broker. This effectively makes the broker the sole CA for the entire address block. The lessor can only regain control by revoking the broker's CA certificate, which disrupts ROAs for all prefixes in that RIR account.
  (b) Subordinate CA Delegation: The lessor runs its own RPKI CA (including publication infrastructure) and issues a subordinate CA certificate to the broker that covers only a designated subset of prefixes—typically those being leased. This setup allows the broker to manage ROAs solely for the delegated prefixes,

[1]However, RIRs typically restricts reassignments to cases involving *transit provider–customer relationships* (e.g., APNIC [42], AFRINIC [29]); thus, using reassignment solely for leasing purposes may violate policy.

while the lessor retains direct control of the rest. The lessor can still create additional ROAs or revoke the subordinate certificate entirely, but must maintain the required RPKI systems (e.g., RRDP/RSYNC publication servers, CRLs). So far, only one broker supports this model for a small set of prefixes (§3.4).

(c) Hybrid (Hosted + Delegated) Model: Ideally, an RIR could allow some prefixes to remain under its hosted RPKI service while simultaneously delegating specific sub-blocks to a broker. However, *no RIR currently supports this arrangement through their standard user portals*, forcing lessors to choose between full hosting or a complete delegation model.

In most cases—except for specific RIR reassignments or complete RIR-level delegations—lessors retain the ability to modify or remove ROAs without notifying lessees. Even subordinate CA delegations do not prevent lessors from revoking certificates and reclaiming control. Therefore, unless the leasing framework protects lessees from the lessor's authority, unilateral or hidden changes to ROAs are possible.

Prior research has not addressed the risks posed by lessors. Instead, it has focused on other aspects of the IP leasing market, such as the functioning of IP transfer markets [33], [34], methods for identifying leased prefixes using WHOIS logs [19], and the prevalence of malicious activities from leased IP addresses [24], [32], [41]. Furthermore, the specific mechanics of ROA management across lessors, brokers, and RIRs-especially the capacity of the original owner to override or selectively distribute ROAs remain largely unexplored.

3. Leased Prefixes and Their ROAs

To understand leased IP spaces, we identify actively leased prefixes on the Internet and analyze their ROAs.

3.1. Leased Prefixes in the Wild

We begin by identifying leased prefixes through their reallocation patterns in WHOIS and IRR records, following the methodology of prior work [19]. The key insight is twofold: (1) leased prefixes are typically more specific sub-prefixes delegated to different organizations, while the parent prefixes remain managed by the original owner and continue to appear in the global routing table; and (2) leasing brokers usually update the `mnt-by` field in WHOIS and IRR records, transferring maintenance responsibilities to themselves. This allows brokers to handle abuse reports and other operational tasks related to the leased prefixes.

We apply this method to the four years of longitudinal datasets from 2021 to 2024:

- **BGP Datasets:** We use RouteViews [54] and RIPE RIS [49] BGP table dumps from January 1, 2022, to December 31, 2024, collected every four hours from all vantage points.
- **Routing registry Datasets:** We gather WHOIS and IRRs from all five RIRs and RADb on a daily basis from January 1, 2022, to December 31, 2024.

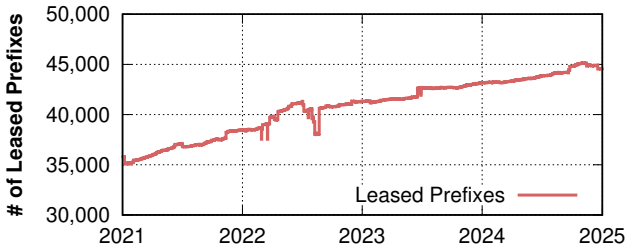

Figure 1. The number of inferred leased prefixes; 44,591 observed in the latest snapshot.

Figure 1 illustrates our finding: As of December 31, 2024, we observe 44,591 leased prefixes, comprising 4.8% of the global routing table. This is a 28.1% increase from 34,809 on January 1, 2022, highlighting the rapid expansion of IP leasing.

3.2. Internet Resources on Leased Prefixes

The growing adoption of leased addresses now underpins an increasingly diverse set of critical Internet resources. To appreciate their real-world impact, we analyzed how many such services reside in the 44,591 leased prefixes identified in our measurement dataset.

Web Servers: Leased IP space is home to a surprising number of popular websites. By cross-referencing the Cisco Umbrella Top 1M domains [2], we found that 54,903 (5.5%) domains resolve to leased prefixes. Noteworthy examples include:

- High-level Chinese government portals such as the Supreme People's Court (`chinacourt.org`), Xinhua News Agency (`xinhuanet.com`), and the main government portal (`www.gov.cn`).
- `vbet.am`, a large Armenian betting platform.
- `webmoney.com`, a globally used digital payments platform.

These domains show that leasing extends well beyond small-scale or disposable addresses: even high-profile government, media, finance, and educational services increasingly rely on leased blocks.

DNS Resolvers: Core DNS infrastructures also gravitate toward leased addresses. Out of 21,430 open DNS resolvers surveyed [62], 1,110 (5.2%) ran on leased prefixes. In a larger DNS scan of 6,496,730 servers [44], 3.2% (206,850) were found in leased space, underscoring the role these addresses play in critical naming services.

NTP Servers: Similarly, time synchronization services hosted under the Network Time Protocol (NTP) have begun shifting to leased prefixes. Among 1,030 public NTP servers listed in the NTxMon dataset [4], 37 (3.6%) resided on leased IPs.

These observations demonstrate the expanding importance of leased blocks in the modern Internet. When essen-

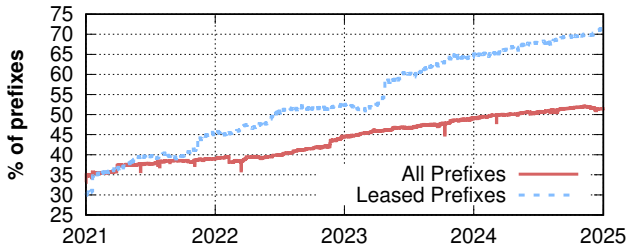

Figure 2. ROA coverage of the leased prefixes has increased rapidly, reaching 71% in our latest snapshot.

tial services—from DNS and NTP to mainstream websites—run on leased addresses, any disruption or hijack can produce widespread consequences, threatening not only the immediate leaseholder but also the broader Internet community that depends on these resources.

3.3. Leased Prefixes with ROAs

Having identified a set of leased prefixes, we next assess how many of them are associated with ROAs. Specifically, we collect daily ROA data from all five RIRs and their delegated publication points, then validate each ROA using Routinator [55]. We cross-reference those validations with our BGP datasets to determine the extent of RPKI coverage among leased prefixes.

As shown in Figure 2, on Jan. 1st, 2021, 33.1% of the global routing table had ROAs, whereas only 29.9% of leased prefixes were covered. Over the subsequent four years, ROA coverage among leased prefixes grew dramatically, reaching 71.0% by Dec. 31st, 2024—outpacing the global table's coverage rate of 51.5% by nearly twenty percentage points; one likely factor behind this accelerated adoption is the *Bring Your Own IP Addresses* (BYOIP) practice now required by many cloud providers (e.g., AWS [11], Google [12]); thus, lessees risk service penalties and potential termination [43] if their prefixes become RPKI-invalid.

3.4. ROA Management of Leased Prefixes

We now examine how ROAs are managed for leased IP prefixes. As discussed in §2.2.2, ROAs can be administered either by the prefix owner or by brokers. When ROAs are set up through direct communication or credential sharing with brokers, they are hosted in RIR or NIR RPKI repositories. In these cases, owners can modify ROAs without notifying brokers unless brokers continuously monitor the ROA status of leased prefixes. Conversely, with RPKI CA delegation, ROAs are managed under the broker's RPKI CA, identifiable via the URI field in the CA certificate.

Out of 31,659 leased prefixes in our latest snapshot covered with ROAs, we analyze *where* each ROA is served. Table 1 summarizes the publication point types and the number of leased prefixes they host; we note that most leased prefixes (98.4%) have ROAs served by RIRs or NIRs, indicating that RPKI CA delegation is rarely used.

TABLE 1. RPKI PUBLICATION POINTS OF LEASED IP PREFIXES.

Publication Point	# of prefixes
RIRs	31,160 (98.4%)
NIRs	35 (0.1%)
Others:	464 (1.5%)
ipxo.com (IPXO)	370 (1.2%)
roa.net (xTom)	34 (0.1%)
rpki.app (Cloudie)	20 (0.1%)
accuristechnologies.ca (Accuris)	16 (0.1%)
0.sb (xTom)	16 (0.1%)
owl.net (Owlnet)	8 (0.0%)

The remaining 1.5% (464 prefixes) are hosted on six RPKI publication points managed by five companies: IPXO, xTom, Cloudie, Accuris, and Owlnet where only IPXO operates as a leasing broker; the others are hosting providers offering direct IP leasing. Despite over 162 brokers registered with RIRs [19], only one broker (i.e., IPXO) utilizes RPKI CA delegation, highlighting its limited adoption. This could be due to the absence of a *Hybrid Model*, which allows lessors to transfer RPKI authority solely for leased prefixes while retaining control over others; currently, lessors must either run their own publication points or use complete delegation, which hands over all IP prefixes under their account to the broker, as described in §2.2.2.

Consequently, even at IPXO—managing over 3,900 leased prefixes—only 370 (9.4%) employ full RPKI CA delegation, reflecting the technical and operational hurdles to widespread adoption.

4. Threats from a Rogue Lessor

Leasing an IP prefix ostensibly grants the lessee freedom to announce and use that block independently, much like a transit customer might advertise a provider-allocated prefix. In practice, however, the fundamental RIR-based ownership remains with the *lessor*, who retains key privileges and can override ROAs for the leased space. Unlike a typical provider–customer setup in which the provider also routes the customer's traffic, lessors in commercial lease arrangements provide *no* network connectivity to the lessee, relying on separate ISPs to carry traffic. As such, they normally have no control over the lessee's traffic paths—unless they leverage RPKI to invalidate the lessee's announcements and hijack that traffic elsewhere.

Below, we define our threat model, the attacker's capabilities and goals, and the assumptions that underlie these attacks.

4.1. Threat Model

Adversary: The Rogue Lessor. We consider a *rogue lessor* that owns one or more IP prefixes recognized by an RIR; it subdivides and leases these addresses to unrelated parties (the lessees). The lessor may work directly with lessees or through a broker who arranges short-term rentals.

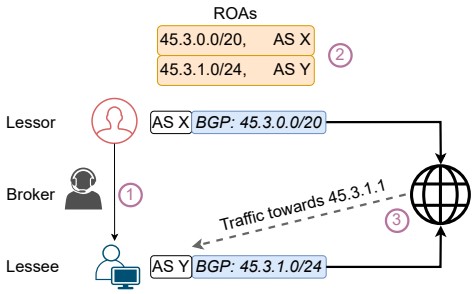

Figure 3. A rogue lessor (AS X) leases a more specific prefix to a lessee (AS Y) and creates two ROAs: one covering its own announcement (e.g., /20) and one lease-compliant ROA authorizing the lessee's prefix.

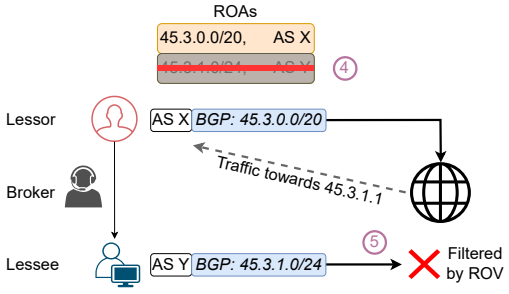

Figure 4. By withdrawing the lease-compliant ROA for the lessee's route, the rogue lessor invalidates the lessee's more specific prefix, causing ROV-enabled networks to favor the lessor's route.

The rogue lessor's incentives could range from monetizing hijacked traffic (e.g., by injecting ads or stealing credentials) to sabotaging services hosted on its leased blocks.

Motivation and Goals. Since the lessor is not a transit provider, it ordinarily has no traffic visibility for the leased sub-prefix. Nonetheless, the lessor *retains control* over the RPKI certificates and ROAs for that address space. By manipulating or revoking ROAs, the lessor aims to:

- *Hijack or intercept traffic* destined for the leased prefix, enabling man-in-the-middle (MITM) attacks or impersonation of the lessee's services.
- *Remain undetected* by the lessee or broker, who may perform only basic checks to confirm the RPKI validity of the leased sub-prefix.

Capabilities. The rogue lessor can:

- *Create, delete, or modify ROAs* in the RIR portal or via a delegated RPKI CA. This includes updating covering prefixes (like a `/20`) so that a lessee's more specific prefix (like a `/24`) becomes RPKI-invalid.
- *Announce legitimate covering routes* for which it is the authoritative owner. Such announcements comply with interdomain routing norms and would not appear as classical "unauthorized" hijacks in many detection systems.
- *Distribute divergent ROAs*, showing one set of objects to specific relying parties (e.g., the lessee's or broker's RPs) and a different set to the rest of the Internet.
- *Monitor public-facing services* under the leased prefix (e.g., via scanning or passive observation) to identify active domains or applications worth targeting.

Limitations. While the lessor can manipulate RPKI data and originate covering prefixes, it does *not* automatically have physical access to the lessee's networks or hosts. Moreover, if the lessee or broker monitors global routing tables or multiple RPKI vantage points, signs of an attack (e.g., disappearance of the sub-prefix from certain BGP collectors) may become apparent. However, most brokers and lessees are not running such intensive monitoring (§7), leaving ample room for covert hijacks.

4.2. Leasing Scenario

Figure 3 illustrates an initial leasing scenario. A rogue lessor owns and announces the prefix `45.3.0.0/20` (AS X) with an existing ROA. The lessor leases a sub-prefix `45.3.1.0/24` to a lessee (AS Y)—either directly or through a broker (①)—and creates a lease-compliant ROA authorizing AS Y to announce it (②). After leasing, lessor continues announcing `45.3.0.0/20`, while the lessee announces `45.3.1.0/24`. Since BGP prefers more specific prefixes (`/24` over `/20`), traffic to `45.3.1.1` routes to the lessee's network (③).

4.3. Global Hijacking Through ROA Manipulation

A rogue lessor can hijack a lessee's sub-prefix *without* altering its own BGP advertisements simply by modifying ROAs to invalidate the lessee's route; this may involve deleting, updating, or revoking the previously valid lease-compliant ROA. Figure 4 illustrates one scenario: by withdrawing the lease-compliant ROA for `45.3.1.0/24` (origin AS Y)(④), the lessee's route immediately becomes RPKI-invalid. Networks that enforce ROV discard the /24, causing traffic to revert to the valid, less-specific prefix `45.3.0.0/20` announced by AS X (⑤). Because the lessor's less-specific prefix remains RPKI-valid, the lessor effectively handles both inbound and outbound traffic for `45.3.1.0/24`, impersonating the lessee's services. Common hijack detection systems(like [3], [16], [45]) and source-address validation approaches (e.g., ACLs [40] or feasible-path uRPF [58]) often fail to detect this hijack because the lessor's less-specific prefix is still recognized as legitimate.

In cases where the leased prefix does not have a ROA at all, the lessor can invalidate the lessee's announcement by simply creating a valid ROA for the less-specific prefix (e.g., `45.3.0.0/20` with origin AS X). During ROV, the router sees no exact-match ROA for the sub-prefix, so the covering ROA applies instead, rendering the lessee's more-specific route RPKI-invalid.

However, this global hijacking is obvious to any entity actively monitoring ROA status, such as brokers [51], cloud

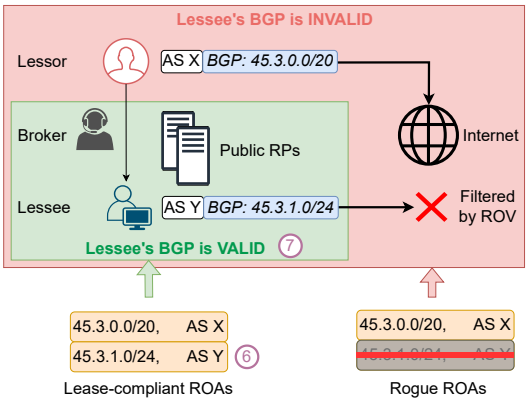

Figure 5. The rogue lessor selectively returns lease-compliant ROAs to RPs used by the broker and lessee, but distributes rogue ROAs elsewhere, enabling a covert hijack that goes undetected from the lessee.

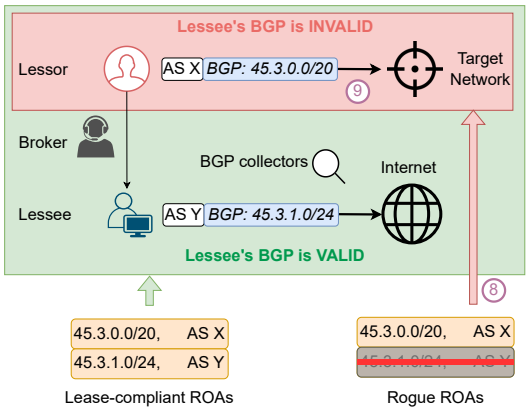

Figure 6. Alternatively, the rogue lessor may send rogue ROAs only to specific networks, hijacking their traffic while preserving the lessee's visibility in most of the Internet—thereby reducing the likelihood of detection.

providers [1], [43], and ISPs [30], many of whom now track the RPKI-status of leased or onboarded prefixes.

4.4. Covert Attacks via Divergent ROA Publication

To conceal these attacks from the lessee or broker—even if they actively monitor ROA status—a rogue lessor can exploit the fact that *RPKI does not guarantee global consistency of ROAs and other objects*. Thus, By managing the publication point, the lessor can distribute different ROAs to different sets of RPs, each with a corresponding valid manifest. Specifically:

- *Lease-compliant* ROAs, which are only provided to the broker and lessee's RPs, ensuring that `45.3.1.0/24` remains RPKI-valid for AS Y.
- *Rogue ROAs*, which omit the ROA for `45.3.1.0/24` when presented to the Internet, causing AS X's `45.3.0.0/20` announcement to be the only valid route.

This tactic is particularly effective when the lessee has onboarded their prefixes with cloud providers that periodically validate RPKI status and enforce ROV policies such as AWS [43], Azure [18], OCI [39], and Vultr [1]. If these cloud providers detect an onboarded prefix has become invalid, they halt the customer's announcements; by feeding lease-compliant ROAs to the RPs used by lessees or brokers while distributing rogue ROAs elsewhere, the hijack proceeds covertly while keeping the victim unaware of the attack.

4.4.1. Identifying the RPs Used by Brokers and Lessees. A rogue lessor's first challenge is determining which RP servers the broker and lessee relies on. One approach involves monitoring the lessor's own RPKI publication point logs to see which IP addresses fetch the repository data. By introducing small, controlled ROA changes only to certain RPs—for instance, briefly invalidating a prefix that is being actively announced—the lessor can send simple probes (e.g., ICMP echo) to observe whether the lessee's prefix becomes unreachable from certain vantage points; if a given vantage point drops the route after the ROA change, the lessor can infer that vantage point is using an RP that recognized the new (malicious) object.

This divide-and-conquer technique can be repeated to pinpoint the exact RP servers used by each major ISP, broker, or cloud provider. Notably, some providers (e.g., AWS, IPXO) provide ROA dashboards listing which prefixes are marked valid; by watching how these dashboards update in response to staged ROA changes, the lessor can confirm whether they are "seen" by the targeted provider's RPs—even without actively probing data-plane reachability.

Such selective publication strategies have already been deployed in measurement studies of RPKI and DNSSEC [26], underscoring how an actor with control over the repository can provide divergent ROA objects for different requesters. In §5.2.2, we show how a rogue lessor can exploit these same techniques to launch and sustain covert hijacks.

4.4.2. Publishing Divergent ROA Sets. Once the lessor identifies the RPs used by the broker and lessee, it delivers the lease-compliant ROAs exclusively to those RPs, while distributing rogue ROAs to all others. As depicted in Figure 5, the new ROAs (⑥) invalidates `45.3.1.0/24` for most of the Internet, redirecting traffic to the supernet `45.3.0.0/20` via AS X. Meanwhile, the lessee and broker see the lease-compliant ROA (⑦) and believe everything remains operational and secure. This divergent publication strategy hides the hijack from any local ROA monitors or dashboards that rely on the broker's or lessee's RP.

4.5. Localized Hijacks to Evade Global Detection

While the introduced hijacks can effectively redirect traffic, they often cause a noticeable drop in the prefix's overall BGP visibility in public BGP collectors like Routeviews [54]

and RIPE RIS [49]. If the lessee or broker monitors routing across multiple vantage points, they may detect the sudden disappearance of the leased prefix, exposing the hijack attempt.

To evade this detection, a rogue lessor can selectively distribute rogue ROAs *only to the RPs used by specific target networks* (⑧), as illustrated in Figure 6. This manipulation causes those networks to treat the lessee's `/24` as RPKI-invalid, defaulting instead to the lessor's valid `/20`. Meanwhile, all other networks continue to see lease-compliant ROAs, maintaining the lessee's `/24` visibility globally and reducing suspicion.

To ensure traffic from the targeted networks flows toward its own infrastructure, the lessor must strategically position its servers; hosting within or near the targeted networks prevents intermediate ASes from overriding the rogue route with the lessee's still-valid `/24` elsewhere (⑨). Establishing direct peering or leveraging regional upstream providers further strengthens the attack.

While this approach requires reconnaissance, identifying the RPs used by specific networks and placing infrastructure accordingly, it is far from impractical; many regional networks rely on a small set of upstream ISPs that enforce ROV, meaning that manipulating just a few key ISPs can capture a significant volume of traffic.

In §5.2.3, we demonstrate how targeting only four ASes in Australia allows the lessor to intercept 57.9% of regional traffic while preserving the lessee's global BGP visibility, making the attack highly effective and difficult to detect.

4.6. Identifying Leased Prefixes Vulnerable to Rogue Lessor Attacks

We now assess how many of the 44,591 leased prefixes in our latest snapshot (§3.1) could be compromised by a rogue lessor. The essential criterion is whether the lessor can invalidate the lessee's announcement by adding, modifying, or revoking ROAs at will. Our analysis identifies three primary conditions enabling such unilateral attacks:

(1) *Reassigned Prefixes with ARIN-Specific Caveats*: If a prefix has been formally "reassigned", the lessee (or broker) gains full ROA control and the lessor no longer holds unilateral authority—*except* in ARIN's registry, where the original owner can still manage ROAs (see §2.2.2). By examining the RIR information of the leased prefixes, we find 12,732 ARIN-based leased prefixes that remain exposed to rogue modifications despite reassignment.

(2) *Lack of RPKI CA Delegation:* In many cases, the lessor keeps official ownership in the RIR database (i.e., no "reassignment" to the broker or lessee). A broker might implement RPKI CA delegation, forcing the lessor to relinquish ROA authority for the leased portion. Yet we uncover additional 14,508 prefixes with no evidence of CA delegation—often signaled by a `mnt-by` or `abuse-contact` change to the broker without an updated CA certificate. Here, the lessor can still create or revoke ROAs arbitrarily, posing a direct hijack threat.

(3) *Leased Prefixes Lacking ROAs Altogether:* If no ROA covers the lessee's prefix, the lessor can publish a valid *covering* ROA and render the more-specific announcement RPKI-invalid—regardless of whether the prefix is reassigned to a broker or lessee via an RIR that grants the transferee direct ROA control. Because a valid less-specific prefix overrides the lessee's route in those networks, traffic shifts to the lessor's advertisement. We identify additional 6,928 reassigned prefixes in this category, all vulnerable if the lessor broadcasts a covering route and maintains a valid ROA.

In total, 34,618 out of 44,591 leased prefixes (76.6%) remain at risk.

4.7. Real-world Practice

In this section, we analyze whether the existing leasing IP spaces are already exposed to security risks. We only focus on the global attack scenario where the leased prefixes are globally RPKI-invalid.

4.7.1. RPKI-invalid in vulnerable prefixes. We first analyze how many of these vulnerable leased prefixes are already RPKI-invalid, while covering with a RPKI-valid less-specific prefix announced from the lessor. For the 34,618 vulnerable prefixes we identified previously, we find 1,392 (4.0%) prefixes are RPKI-invalid using VRPs of the same date. Among these RPKI-invalid prefixes, a majority of them (1,023) we find are covered by a less-specific RPKI-valid prefixes announced by the lessor (the lessor ASN is inferred using the same methodology as in [19]).

4.7.2. Existing Man-in-the-middle. We further analyze these RPKI-invalid leased prefixes in the data plane, to see *whether traffic are already re-directed to the lessors*. Firstly, we use ZMap [21] to find hosts responding to ICMP echo requests under these 1,392 prefixes, obtaining 98,928 responding hosts covering 418 of these prefixes. To minimize the traffic toward each prefix, we only pick one representative host for each prefix. We then run ICMP traceroute toward these hosts and collect the paths.

To determine whether traffic traverses lessors, we first map each hop from traceroute results to ASN. We do not consider the last hop IP address, since the last hop IP is the target host, we cannot tell whether the last hop is the lessor or lessee. We first check whether the remaining last hop AS is the lessor AS, if so, we consider the traffic is traversing the lessor. Then we also use the same methodology as [37], [65], examining the penultimate hop AS in the traceroute responses; if the penultimate hop AS is never listed in any AS_PATH of that prefix in our BGP datasets, but is listed in the AS_PATH of the lessor's less-specific prefix, we consider the traffic is traversing the lessor ([19] already filter potential lessors which are transit upstreams of the lessees.).

After all, we confirm 387 (27.8%) of the 1,392 RPKI-invalid prefixes are traversing the lessor ASes. Although

there is no evidence whether these lessors are intentionally hijacking the leased prefixes, or just because of misconfiguration, the fact that these lessors are already become the man-in-the-middle of the leased prefixes is alarming.

5. Empirical Evaluation of Lessor-Led Attacks

The effectiveness of our attack depends on the deployment of ROV. In this section, we conduct experiments with a diverse set of rogue lessor and lessee network pairs to evaluate its practical impact. Through these experiments, we demonstrate how attackers can exploit RPKI by selectively manipulating ROAs to hijack leased prefixes, redirecting traffic while minimizing detection.

5.1. Experiment setup

5.1.1. The Lessor and Lessee Networks. We emulate a lessor announcing a prefix while a lessee announces a more specific sub-prefix. Our experiments involve two cloud providers (Vultr and Amazon AWS), plus three nodes in the PEERING testbed spread across four continents:

- Cloud Providers: `Vultr` (Sydney) and `AWS` (Atlanta)
- PEERING Testbed: `ufmg01` (upstream AS1916), `isi01`, (upstream AS2914), and `amsterdam01` (AMS-IX)

We exclude any scenario where the rogue lessor and lessee reside within the same cloud environment or network to avoid trivial conflicts, lead us to 20 lessor-lessee pairs. In each pair, the lessor's network announces a /47 IPv6 prefix, while the lessee network announces the more specific /48. We then host the ROAs for these prefixes on our own RPKI publication point servers.

To launch the covert attack, we operate two PP servers behind a gateway capable of serving different ROAs based on the incoming IP address of each RRDP or RSYNC request, allowing selective manipulation of ROAs.

5.1.2. Measuring Hijack Impact. We measure how much traffic actually diverts to the rogue lessor after attack. By employing RIPE Atlas [48] vantage points, we send ICMP echo to our experimental prefixes. The recipient of each connection attempt reveals whether traffic is routed to the lessor or the lessee. Over the course of our experiments, 16,273 active vantage points from 1,676 ASes in 176 countries participated. For each lessor-lessee pair, the *attack success rate* is the fraction of Atlas probes reaching the lessor instead of the lessee.

5.2. Attack Scenarios

5.2.1. Global Attack. We start with a basic attack scenario in which the lessor removes the ROAs for the leased prefixes, causing ROV-enforced routers to reject the lessee's route. However, cloud providers such as Vultr and AWS immediately withdraw customer announcements upon detecting customer prefixes have become RPKI-invalid. To ensure continued reachability in these environments, lease-compliant ROAs must still be served selectively; thus, we limit our global attack experiments to configurations where the lessee operates on the three PEERING nodes, while the adversary can be any of the five vantage points (including three PEERING nodes and two cloud nodes). This setup results in a total of 12 adversary-victim experiment pairs.

5.2.2. Covert Attack. In typical leasing scenarios, the lessee should operate its own RPKI RP servers (recommended by RFC 7115 [6]) or rely on public RP services (e.g., Cloudflare's RP [17]). Meanwhile, a broker can also monitor the ROA status of leased prefixes. The rogue lessor must therefore *identify* which RPs the lessee and broker use and then return lease-compliant ROAs to those RPs while distributing rogue ROAs to others.

Following the methods of §4.4.1, we locate:

- Victim RPs: For Vultr and AWS, we leverage each provider's RPKI dashboards which public the validation results for customers prefixes. By assigning distinct, random ASNs in each rogue ROA and detecting which VRPs are listed on the dashboard, we infer the IP addresses of the underlying RPs. For PEERING testbed, we perform selective route tests as outlined in §4.4 to identify its RPs.
- Broker RPs: We include one RP used by a popular IP leasing broker, IPXO, which maintains a public VRP dashboard. Observing changes there allows us to pinpoint their RPs.
- Public RPs: Some lessees or brokers may rely on well-known public RP services rather than deploying in-house solutions. We focus on three such RPs (Cloudflare [17], RIPE [52], and OpenBSD [38]). Each of these publishes its VRPs on a web server, enabling us to detect their RPs through a process similar to the one described for Vultr and AWS.

5.2.3. Targeted Attack. To evaluate the feasibility of a targeted attack, we focus on Australia—an island continent with relatively concentrated network interconnections. This geographical characteristic allows an adversary to influence a significant portion of local traffic by manipulating a small set of key upstream providers.

For our experiment, we position the lessor at Vultr's Sydney while the lessee operates from two PEERING testbed vantage points (`ufmg01` and `amsterdam01`). We selectively distribute rogue ROAs only to the RPs used by four top-ranked Australian networks that enforce ROV (AS4826, AS1221, AS38195, and AS4764), as well as to the lessor's own AS (Vultr). These RPs are identified through the methodology outlined in §4.4.1.

To evaluate the success of this targeted attack against Australia, we use all 232 RIPE Atlas probes located within Australia and send `ICMP echo` to the lessee's prefix. We then examine whether the replies originate from the lessor's vantage point—indicating successful traffic interception. Simultaneously, we monitor the BGP visibility of the lessee's prefix using RouteViews, ensuring that its announcements

TABLE 2. HIJACK SUCCESS RATE (%) ACROSS DIFFERENT ATTACK SCENARIOS. V, B, AND P REPRESENT SCENARIOS WHERE THE ADVERSARY (I.E., ROGUE LESSOR) SERVES LEASE-COMPLIANT ROAS TO RPS USED BY THE VICTIM (V), THE VICTIM AND BROKERS (B), AND THE VICTIM, BROKERS, AND PUBLIC RPS (P), RESPECTIVELY. NOTE THAT INCLUDING A BROKER'S RP DOES NOT AFFECT THE SUCCESS RATE, AS BROKERS USE RPS SOLELY FOR MONITORING PURPOSES AND DO NOT TRANSIT TRAFFIC.

Adversary	Victim	Attack Scenarios				
		Global	Covert			Targeted
			V	V+B	V+B+P	
Atlanta	Sydney	-	82.1	82.1	79.5	-
	UFMG	100	89.6	89.6	85.0	-
	AMS	100	79.4	79.4	74.0	-
	ISI	100	85.9	85.9	81.8	-
Sydney	Atlanta	-	79.8	79.8	76.2	42.3
	UFMG	100	87.2	87.2	85.8	68.9
	AMS	100	77.3	77.3	73.1	57.8
	ISI	100	85.1	85.1	82.0	62.5
UFMG	Atlanta	-	72.9	72.9	70.2	-
	Sydney	-	71.4	71.4	69.5	-
	AMS	100	74.0	74.0	70.7	-
	ISI	100	76.9	76.9	74.8	-
AMS	Atlanta	-	83.2	83.2	80.4	-
	Sydney	-	85.5	85.5	81.9	-
	UFMG	100	89.1	89.1	87.0	-
	ISI	100	87.3	87.3	85.2	-
ISI	Atlanta	-	75.8	75.8	73.9	-
	Sydney	-	77.0	77.0	74.0	-
	UFMG	100	79.4	79.4	78.2	-
	AMS	100	74.1	74.1	70.5	-
Average		100	80.7	80.7	77.8	57.9

remain unaffected outside Australia while localized traffic is quietly redirected to the lessor.

5.3. Results

Table 2 presents the hijack success rates across different attack scenarios.

5.3.1. Global Attack. When the lessor marks the lessee's prefix as RPKI-invalid while keeping its own announcement RPKI-valid, transit providers enforcing ROV will drop the lessee's route, redirecting all traffic to the lessor. As soon as the lessor changes the ROA status of the lessee's prefix to invalid, ROV-compliant ASes reject the announcement, preventing further propagation and resulting in a complete hijack with a 100% success rate.

However, global hijacks are not always feasible; cloud providers such as Vultr and AWS block invalid BGP announcements *at the source*. When the lessee resides at these providers, any RPKI-invalid advertisement triggers an immediate shutdown of the lessee's route, alerting both the lessee and the broker as mentioned in §5.2.1.

5.3.2. Covert Attack. Since many major ASes have already adopted ROV, the covert attack remains highly effective, hijacking on average 80.7% of traffic and reaching 89.6%

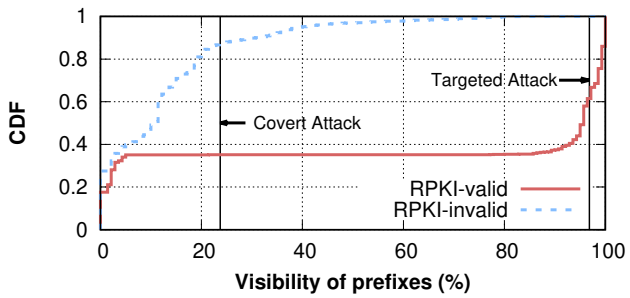

Figure 7. CDF of BGP visibility for all RPKI-valid and RPKI-invalid prefixes in our latest snapshot, compared to lessee prefixes under covert and targeted attacks. In covert attacks, visibility drops sharply to 23.7%, making detection more likely. In contrast, targeted attacks maintain 95.8% visibility, closely mirroring normal RPKI-valid behavior, making detection significantly harder.

in certain configurations (e.g., lessor at AWS, lessee at UFMG). If a leasing broker monitors the prefix's ROA status, the lessor must provide lease-compliant ROAs to that broker's RP. Doing so has no impact on the hijack rate, since brokers typically do not themselves carry transit traffic.

In contrast, masking the attack from well-known public RPs (e.g., Cloudflare, RIPE, OpenBSD) does reduce success rate slightly—from 80.7% to 77.8% on average—because certain transit providers rely on those public RPs for validation. Keeping such providers unaware of the rogue ROAs allows them to continue forwarding traffic to the lessee.

5.3.3. Targeted Attack. In our experiment, we target four major Australian ASes that enforce ROV by supplying them with malicious ROAs, while showing the lease-compliant versions to every other RP; as a result, the hijack succeeds for 57.9% of traffic originating in Australia (since those four ASes reject the lessee's prefix) yet leaves the prefix fully visible elsewhere, drastically reducing the likelihood of detection.

Figure 7 compares how this targeted strategy affects visibility relative to a covert attack on all RPs; it measures visibility as the percentage of RouteViews [54] and RIPE RIS [49] peers that observe the prefix. Under a full covert attack, the lessee's prefix loses substantial global coverage (down to 23.7%), whereas in the targeted scenario, it retains 95.8% visibility. In other words, from a global vantage, the prefix appears nearly identical to a normal RPKI-valid route. Only the regional traffic in Australia is silently redirected to the lessor.

If the adversary wishes to hide the covering announcement from public BGP collectors, it can incorporate other well-known hijack techniques that limit route propagation (e.g., NO_EXPORT communities [8], [10]). Such localized hijacks become especially difficult to detect in practice, given that most lessees and brokers do not systematically monitor broader routing state (§7); our data shows only 5 out of 16 lessees and 1 out of 7 brokers keep track of BGP visibility, implying that even partial hijacks may go unnoticed for extended periods.

5.4. Case Study: Obtaining TLS Certificates via Covert Attack

TLS certificates authenticate a server's identity to clients. One of the most common ways to obtain such certificates is via the HTTP-01 ACME challenge, popularized by Let's Encrypt. In this section, we show how a rogue lessor can leverage a selective (covert) hijack to fraudulently acquire a valid TLS certificate for a lessee's domain.

5.4.1. TLS Certificate Acquisition Process. The HTTP-01 challenge is a domain-validation mechanism that requires the requester to serve a unique token at a predefined URL. A Certificate Authority (CA) then sends HTTP requests to that URL from multiple vantage points to confirm domain ownership. If the retrieved token matches the one issued, the domain is deemed valid, and a TLS certificate is granted.

To mitigate simple BGP hijacks, Let's Encrypt employs *Multi-Vantage-Point Domain Validation* [9], distributing its ACME servers across multiple locations. The aim is to prevent a BGP hijacker from successfully hijacking routes to a single validation server. However, if these diverse vantage points rely on a common or easily identifiable RP infrastructure, a rogue lessor can still perform a *covert hijack* by selectively invalidating the lessee's prefix for those vantage points while presenting lease-compliant ROAs to the lessee's vantage points.

5.4.2. Attack Overview. Figure 8 illustrates how a rogue lessor can impersonate `lessee.com`, which operates on the leased IP `45.3.1.1`:

(a) Domain Setup: The lessor configures a web server to mimic `lessee.com`, hosting any content or services needed to pass domain validation.

(b) Challenge Initiation: The lessor requests a certificate for `lessee.com` (or another domain pointing to `45.3.1.1`) from a CA that supports ACME, receiving a unique challenge token (①).

(c) Covert Hijack: The lessor supplies lease-compliant ROAs to the lessee's RPs, maintaining a valid route from the lessee's perspective, but distributes rogue ROAs elsewhere. These rogue ROAs invalidate the lessee's more-specific prefix for most of the Internet, causing BGP to favor the lessor's route.

(d) Validation and Certificate Issuance: The CA's globally distributed validation servers query the IP address of `lessee.com` from the lessee's DNS server (②), then attempt to retrieve the challenge token at `45.3.1.1`. Due to the covert hijack, these requests reach the lessor's server, which supplies the correct token (③). Finally, the CA issues a valid TLS certificate.

5.4.3. Experiments and Results. We tested this attack on the same set of 20 lessor–lessee pairs as presented in Table 2. We observed that Let's Encrypt dispatches validation requests from multiple vantage points, including its own server hosted on AS13649 (Flexential) and four distinct

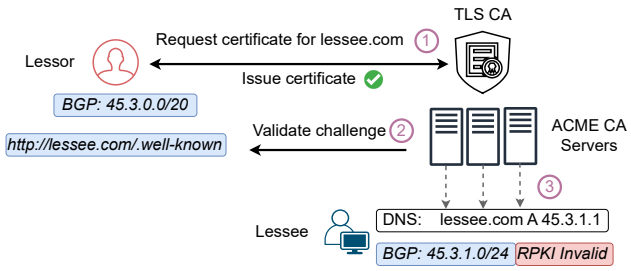

Figure 8. A rogue lessor uses selective RPKI invalidation to divert ACME validation traffic, ultimately obtaining a TLS certificate for `lessee.com`

AWS locations. Both AS13649 and AWS enforce ROV, making it straightforward for the rogue lessor to hijack these validation flows by invalidating the lessee's prefix *except* where the lessee's RPs are located.

Overall, 16 of the 20 lessor–lessee pairs managed to obtain legitimate TLS certificates for the lessee domain. The remaining 4 pairs failed due to additional AWS-based checks that could not be bypassed without triggering detection. Nevertheless, these results demonstrate that a rogue lessor, equipped with selective RPKI hijacking, can frequently secure valid TLS certificates tied to a leased IP block; crucially, while major cloud providers implement ROV, the lessor's selective route invalidation can still redirect enough of the ACME validation traffic to achieve domain validation under most circumstances.

6. Locating Anonymized RPs

In principle, one can impede our proposed attacks by *obscuring or anonymizing RP servers*. However, as we show below, existing anonymity tactics remain vulnerable to fingerprinting methods rooted in the RPKI synchronization protocol itself.

6.1. Defenses Against Covert Attacks

In order to know which specific RPs the lessee use, the lessor can monitor RP queries at its publication point or test short-lived ROA changes to discover which vantage points adopt those changes.

Prior work on misbehaving RPKI publication points has primarily suggested scaling up the number of RPs or dispersing them geographically for increased resilience. For example, ByzRP [22] proposes using many RPs along with a consensus-based voting mechanism; OpenBSD operates five separate servers [38] to reduce single points of failure. However, *merely having more RPs* does not inherently block a determined attacker: if the adversary can learn *all* of the relevant RP endpoints, it can deliver malicious ROAs to each one.

One proposed mitigation is to *anonymize* RP servers; for example, RPs might frequently rotate their IP addresses or route traffic via Tor [20] to conceal their true location [57].

If the rogue lessor cannot determine which requests come from the victim's RPs, it cannot tailor a malicious ROA feed for those vantage points.

6.2. Breaking RP Anonymity via RRDP

6.2.1. RRDP Basics. Most RP implements the RPKI Repository Delta Protocol (RRDP) [60]; RRDP allows an RP to download only the incremental "delta" of newly published objects (e.g., ROAs) rather than fetching the entire repository every time.

Each publication point maintains a *notification file* that tracks the current serial number and lists older serials along with the changed objects. Upon connecting, an RP only download the corresponding delta based on the last serial it has seen. While this design improves efficiency, it also creates an observable *fingerprint* of how an RP moves through repository updates.

6.2.2. Fingerprinting RPs Using Deltas. Figure 9 illustrates how a malicious lessor can exploit RRDP's versioning to de-anonymize RPs, even if they connect from shifting or proxy IPs. Suppose two RPs, labeled RP1 and RP2, each connect multiple times under different addresses. The publication point can artificially increment the repository's serial number for each request:

(a) *Initial Sync.* RP1 first fetches all files at serial-01, while RP2 later fetches them at serial-02.

(b) *Differential Updates.* When RP1 returns, it requests only the delta from its *previous* serial (01) to the *current* serial (e.g., 03). This reveals that the RP making this request must be the same one that had previously synchronized at serial-01. By contrast, if a new request attempts to move from serial-02 to serial-04, the server learns it is *RP 2* again, merely re-appearing from a different IP.

By embedding small updates or innocuous ROA changes each time, the adversary can correlate repeated fetch patterns with unique RP "identities". In this way, even large IP address pools or proxies cannot mask which physical (or virtual) server is continuing a specific RRDP session. This is also applicable to `rsync`-based repositories as well as they also support delta-based partial updates that can expose an RP's synchronization history.

6.2.3. Trade-Offs for True Anonymity. The only foolproof workaround would require an RP to *always* fetch the entire repository from scratch, never revealing continuity via delta fetching. However, this approach is resource-intensive, leading to slower updates and greater bandwidth use. Even then, subtle timing correlations or repeated patterns in fetched objects might still de-facto fingerprint the RP.

As a result, purely technical methods of anonymizing RPs remain incomplete. Substantial overhead and operational complexities often dissuade defenders from implementing full repository fetches, particularly as RPKI adoption grows. Instead, it may be more effective to address the underlying security gap in the IP leasing system ensuring that malicious lessors cannot exploit delegated ROA authority in the first place (see §8).

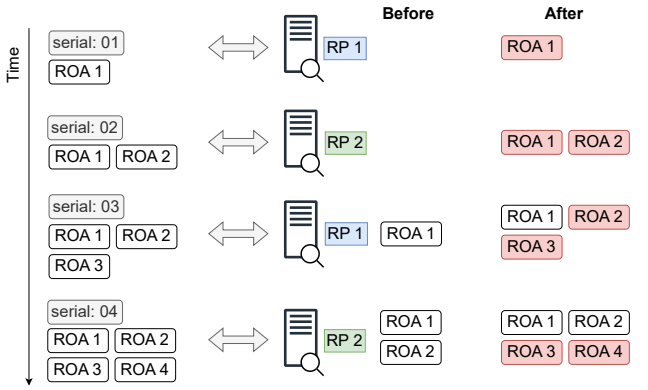

Figure 9. Two RPs, each changing IP addresses, still reveal their identities through RRDP's versioned deltas.

7. Survey on ROA Management in IP Leasing

To gain deeper insights into how ROAs are managed in the context of IP leasing, we conducted a survey of lessors, brokers, and lessees between December 2024 and January 2025. We gathered 16 responses from lessees and 10 from lessors via community mailing lists and Discord channels. For the broker survey, emails were sent to all 47 registered brokers listed by ARIN [23] and APNIC [53], yielding 8 responses; the questions addressed ROA configuration, ongoing maintenance, and any obstacles or challenges specific to leased IPs. Full questionnaires are provided in Appendix §A.

7.1. Operational Leasing Practices and RPKI

Brokers. All 8 brokers stated they support ROA publication, usually completing setup in under 48 hours. However, the specifics varied: (1) four brokers required the lessor to delegate full control of their RIR account for ROA changes, (2) three relied on manual, case-by-case communication with lessors, and (3) Only one used RPKI CA delegation.

Meanwhile, 7 brokers reported actively monitoring the ROA status of leased prefixes, but each broker relied on a single RP server (self-operated or publicly hosted). Only 1 broker also tracked BGP visibility. Because these brokers each uses just one source of route origin data, discrepancies between lease-compliant and rogue ROAs would be difficult to catch, making covert hijacks potentially elusive.

Lessors. All 10 lessors confirmed that brokers request ROA configuration for leased prefixes. Most of these lessors said they update or create ROAs *manually* in response to broker instructions. Only 1 lessor had adopted a fully delegated RPKI CA model, suggesting that the additional complexity and operational burden of delegated RPKI deter most from pursuing it. 6 surveyed lessors admitted they

do not monitor the RPKI status of their leased prefixes; among the four who did, three had previously encountered incidents where a leased prefix became RPKI-invalid due to misconfiguration, leading to manual corrective actions.

These practices indicate that if a malicious lessor intentionally invalidates a leased prefix, neither the lessee nor the broker may detect it—particularly if neither side systematically monitors ROA status or consults multiple vantage points.

Lessees. Of the 16 lessee respondents: (1) 6 lease prefixes directly from owners, (2) 9 operate through brokers, (3) 1 uses both methods. Among the 9 broker-oriented lessees, most rely on manual coordination for ROA updates, contrary to some brokers' claims of relying on RIR account or CA delegation. Only 3 lessees track ROA status themselves (via public or self-hosted RPs), and 4 keep an eye on BGP visibility; in cases where these checks are absent, a rogue lessor could easily enact a covert hijack by presenting lease-compliant ROAs to the lessee's chosen RP while distributing rogue ROAs elsewhere—leaving the lessee clueless about changes in external routing environments.

7.2. Takeaways

The survey findings reveal several noteworthy points:

- Heavy Reliance on Manual Processes: Both lessors and brokers frequently resort to ad-hoc communication and manual ROA updates. This opens the door to misconfigurations and delays, which can inadvertently invalidate leased prefixes—disrupting lessees' operations.
- Single-RP Monitoring is the Norm: Brokers and many lessors use just one RP source to track ROA status, which fails to capture divergences across publication points. In stealth hijacks, a malicious lessor can craft lease-compliant ROAs for that single RP while serving rogue ROAs to the rest of the Internet.
- Lessee Vulnerability: Lessees typically lack direct control over ROA, leaving them dependent on brokers or lessors for updates. With many not monitoring RPKI or BGP visibility, they remain unaware if their prefixes become invalid or hijacked in remote portions of the Internet.

Overall, these patterns highlight a lack of robust safeguards in the IP leasing ecosystem and underline the inherent security risks revealed in our broader study.

8. Concluding Discussion

Our work highlights a key vulnerability in the current IP leasing ecosystem: RPKI intrinsically defers authority over ROAs to whoever is listed as the owner in RIR records, even when that party no longer uses the prefix. This mismatch, combined with RPKI's hierarchical design and the ability to selectively manipulate RPs, enables covert or partial hijacks that are difficult for lessees to detect or prevent.

Although these attacks cannot be fully eliminated under current RPKI structures, they can be made more transparent and much harder to carry out. Below, we summarize actionable recommendations for each stakeholder group, followed by closing thoughts on the path forward.

- **For Lessees:**
  - *Publish and Maintain ROAs for Leased Prefixes.* If the leased block has no explicit ROA, a lessor can trivially invalidate it by creating a covering prefix ROA. Lessees should actively confirm that ROAs exist for sub-prefixes they announce. Monitoring these ROAs ensures they remain aligned with the correct origin ASN and prefix length.
  - *Use Multiple RP Sources for Validation.* Relying on a single feed (or dashboard) can be misleading, especially if the lessor selectively presents different ROAs to different RPs. Lessees should compare data from several independent RP services. Tools such as `rtrmon` [59], `ByzRP` [22] or public looking-glass sites [66] help catch discrepancies across vantage points.
- **For Brokers:**
  - *Monitor ROAs Actively and From Multiple Perspectives.* Brokers are in a strong position to detect malicious behavior early. By polling multiple RPs, a broker can see if a lessor issues conflicting ROAs. When anomalies arise, brokers can alert the lessee or require corrective action from the lessor.
  - *Offer RPKI CA Delegation Services.* Providing a delegated RPKI platform allows the broker (rather than the lessor alone) to manage ROAs. This reduces the risk that a lessor can covertly alter or revoke them.
- **For Lessors:**
  - *Adopt Partial Delegation Where Possible.* If a lessor wishes to lease out only certain sub-prefixes, a delegated RPKI setup (potentially via a broker) can isolate leased blocks without granting universal control over the lessor's entire address range.
- **For RIRs and the Broader Community:**
  - *Enable a Hybrid RPKI Model.* Current RIR portals rarely allow partial or hybrid delegation (splitting resources between hosted RPKI and delegated RPKI). Enabling this feature would let lessors delegate exactly the leased portion, reducing the risk that a single party controls ROAs for all their address space.

Final Remarks Achieving a robust fix will require both technical and policy changes: on the policy side, RIRs need to allow more nuanced delegation mechanisms that reflect actual usage, and on the technical side, multi-vantage-point checks and delegated CA authority can limit the lessor's unilateral power. Strengthening collaboration among RIRs, brokers, and network operators is crucial; only by introducing partial delegation, improving transparency across publication points, and encouraging proactive multi-source monitoring can the community ensure the growing IP leasing market does not unintentionally weaken global routing security.

References

[1] About Resource Public Key Infrastructure (RPKI) at Vultr. https://docs.vultr.com/rpki.

[2] Cisco Umbrella Top 1M Domain List. https://umbrella-static.s3-us-west-1.amazonaws.com/index.html.

[3] GRIP - Global Routing Intelligence Platform. https://grip.inetintel.cc.gatech.edu.

[4] NTxMon. https://ntxmon.com/.

[5] R. Austein. An Out-of-Band Setup Protocol for Resource Public Key Infrastructure (RPKI) Production Services. RFC 8183, IETF, 2017.

[6] R. Bush. Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI). RFC 7115, IETF, 2014.

[7] R. Bush and R. Austein. The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1. RFC 8210, IETF, 2017.

[8] H. Birge-Lee, M. Apostolaki, and J. Rexford. Global bgp attacks that evade route monitoring. *PAM*, 2025.

[9] H. Birge-Lee, L. Wang, D. McCarney, R. Shoemaker, J. Rexford, and P. Mittal. Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt. *USENIX Security*, 2021.

[10] H. Birge-Lee, L. Wang, J. Rexford, and P. Mittal. Sico: Surgical interception attacks by manipulating bgp communities. *CCS*, 2019.

[11] Bring your own IP addresses (BYOIP) to Amazon EC2. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-byoip.html.

[12] Bring your own IP addresses in Google Cloud. https://cloud.google.com/vpc/docs/bring-your-own-ip.

[13] D. Cooper, E. Heilman, K. Brogle, L. Reyzin, and S. Goldberg. On the risk of misbehaving RPKI authorities. *HotNets*, 2013.

[14] B. Cartwright-Cox. Measuring RPKI Adoption via the data-plane. NLNOG Day 2018. https://nlnog.net/static/nlnogday2018/8_Measuring_RPKI_ben_NLNOG_2018.pdf.

[15] Can I create a ROA for a network prefix that has been reassigned or reallocated to my OrgID? https://www.arin.net/resources/manage/rpki/byoip/.

[16] Cloudflare Radar. https://radar.cloudflare.com/routing.

[17] Cloudflare's RPKI Toolkit. https://rpki.cloudflare.com/rpki.json.

[18] Azure Custom IP address prefix (BYOIP). https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/custom-ip-address-prefix.

[19] B. Du, R. Fontugne, C. Testart, A. C. Snoeren, and k. claffy. Sublet Your Subnet: Inferring IP Leasing in the Wild. *IMC*, 2024.

[20] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. *USENIX Security*, 2004.

[21] Z. Durumeric, E. Wustrow, and J. A. Halderman. ZMap: Fast Internet-Wide Scanning and its Security Applications. *USENIX Security*, 2013.

[22] J. Friess, D. Mirdita, H. Schulmann, and M. Waidner. Byzantine-secure relying party for resilient RPKI. *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2024.

[23] Find a Qualified Facilitator. https://www.arin.net/resources/registry/transfers/facilitators/qualifiedfacilitators/.

[24] V. Giotsas, I. Livadariu, and P. Gigis. A First Look at the Misuse and Abuse of the IPv4 Transfer Market. *PAM*, 2020.

[25] G. Huston, G. G. Michaelson, C. M. Martínez, T. Bruijnzeels, A. Newton, and D. Shaw. Resource Public Key Infrastructure (RPKI) Validation Reconsidered. RFC 8360, IETF, 2018.

[26] T. Hlavacek, P. Jeitner, D. Mirdita, H. Shulman, and M. Waidner. Behind the scenes of RPKI. *CCS*, 2022.

[27] T. Hlavacek, P. Jeitner, D. Mirdita, H. Shulman, and M. Waidner. Stalloris: RPKI Downgrade Attack. *USENIX Security*, 2022.

[28] T. Hlavacek, P. Jeitner, D. Mirdita, H. Shulman, and M. Waidner. Beyond limits: How to disable validators in secure networks. *SIGCOMM*, 2023.

[29] IPv4 Allocation Policy. https://www.afrinic.net/library/policies/126-afpub-2005-v4-001.

[30] Improved BGP Routing Security Adds Another Important Layer of Protection to Online Networks. https://corporate.comcast.com/stories/improved-bgp-routing-security-adds-another-layer-of-protection-to-network.

[31] M. Jonker, A. Sperotto, R. van Rijswijk-Deij, R. Sadre, and A. Pras. Measuring the Adoption of DDoS Protection Services. *IMC*, 2016.

[32] T. Krenc and A. Feldmann. BGP Prefix Delegations: A Deep Dive. *IMC*, 2016.

[33] I. Livadariu, A. Elmokashfi, and A. Dhamdhere. On IPv4 transfer markets: Analyzing reported transfers and inferring transfers in the wild. *Computer Communications*, 111, Elsevier, 2017.

[34] I. Livadariu, A. Elmokashfi, A. Dhamdhere, and K. Claffy. A first look at IPv4 transfer markets. *CoNEXT*, 2013.

[35] M. Lepinski, S. Kent, G. Huston, and R. Austein. Manifests for the Resource Public Key Infrastructure (RPKI). RFC 6486, IETF, 2012.

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

[37] S. McQuistin, S. P. Uppu, and M. Flores. Taming Anycast in the Wild Internet. *IMC*, 2019.

[38] OpenBSP RPKI-Client VRP. https://console.rpki-client.org/rpki.json.

[39] OpenDKIM. https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/BYOIP.htm.

[40] F. Paul and S. Daniel. Network ingress filtering: defeating denial of service attacks which employ ip source address spoofing. IETF, 2000. https://datatracker.ietf.org/doc/html/rfc2827.

[41] L. Prehn, F. Lichtblau, and A. Feldmann. When wells run dry: the 2020 IPv4 address market. *CoNEXT*, 2020.

[42] Policies for IPv4 address space management in the Asia Pacific region. https://www.apnic.net/community/policy/drafts/add-manage-policy/#9.7.

[43] Prerequisites for BYOIP in Amazon EC2. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/prepare-for-byoip.html.

[44] Project Sonar. https://www.rapid7.com/research/project-sonar/.

[45] L. Qin, D. Li, R. Li, and K. Wang. Themis: Accelerating the detection of route origin hijacking by distinguishing legitimate and illegitimate MOAS. *USENIX Security*, 2022.

[46] A. Reuter, R. Bush, I. Cunha, E. Katz-Bassett, T. C. Schmidt, and M. Whlisch. Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering. *CCR*, 48(1), 2018.

[47] N. Rodday, I. Cunha, R. Bush, E. Katz-Bassett, G. D. Rodosek, T. C. Schmidt, and M. Wählisch. Revisiting RPKI Route Origin Validation on the Data Plane. *TMA*, 2021.

[48] RIPE NCC Annual Report 2015. https://www.ripe.net/publications/docs/ripe-665.

[49] RIPE Routing Information Service (RIS). http://www.ripe.net/projects/ris/rawdata.html.

[50] RPKI I-Rov Filtering Rate. https://stats.labs.apnic.net.

[51] RPKI Management at IPXO (IP Holder). https://www.ipxo.com/kb/technical-guides/rpki-management-at-ipxo-ip-holder/.

[52] RPKI Validator API. https://rpki-validator.ripe.net/api/export.json.

[53] Registered IPv4 brokers. https://www.apnic.net/manage-ip/manage-resources/transfer-resources/transfer-of-unused-ip-and-as-numbers/transfer-facilitators/.

[54] University of Oregon RouteViews project. http://www.routeviews.org/.

[55] Routinator. https://nlnetlabs.nl/projects/rpki/routinator/.

[56] H. Schulmann and S. Zhao. Insights into SAV Implementations in the Internet. *PAM*, 2024.

[57] J. Snijders. Security and operations of RPKI infrastructure. 2025. Routing Security Workshop 2025.

[58] K. Sriram, D. Montgomery, and J. Haas. Enhanced Feasible-Path Unicast Reverse Path Forwarding. RFC 8704, IETF, 2020.

[59] StayRTR. https://github.com/bgp/stayrtr.

[60] B. Tim, M. Oleg, W. Bryan, and A. Rob. The RPKI repository delta protocol (RRDP). RFC 8182, IETF, 2017.

[61] H. Tomas, H. Amir, S. Haya, and W. Michael. Practical experience: Methodologies for measuring route origin validation. *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2018.

[62] The most exhaustive list of reliable DNS resolvers. https://github.com/trickest/resolvers.

[63] What is Hosted RPKI? https://www.arin.net/resources/manage/rpki/hosted/.

[64] What is IPv4 Run Out? https://www.ripe.net/manage-ips-and-asns/ipv4/ipv4-run-out.

[65] M. Zhou, X. Zhang, S. Hao, X. Yang, J. Zheng, G. Chen, and W. Dou. Regional IP Anycast: Deployments, Performance, and Potentials. *SIGCOMM*, 2023.

[66] rpkiviews. https://www.rpkiviews.org/.

Appendix A.
Full questionnaires

Below are the full questionnaires we used in §7 for understanding the leasing practice of brokers, lessees and lessors.

A.1. Survey for Brokers

Below are the questions we posed to IP-address leasing brokers:

Q1: When leasing prefixes to a lessee, does your company verify their existing Route Origin Authorization (ROA) status?
Q2: What is your company's policy for configuring ROAs on leased prefixes?
Q3: After a prefix is leased, approximately how long does it take your company to complete the ROA configuration?
Q4: Does your company monitor the Resource Public Key Infrastructure (RPKI) status of leased prefixes?
Q5: How does your company monitor RPKI status?
Q6: How many Route Propagation (RP) servers does your company operate?
Q7: Where does your company place its RP servers?
Q8: Which public RP sources does your company use?
Q9: If a leased prefix becomes RPKI-Invalid due to the lessor's action, what steps does your company take?
Q10: Which ROA statuses does your company monitor?
Q11: Does your company monitor the BGP visibility of leased prefixes (i.e., the BGP path to each leased prefix)?

A.2. Survey for Lessors

Below are the questions we posed to organizations that lease out prefixes to brokers or lessees:

Q1: How familiar is your company with RPKI overall?
Q2: What is your company's autonomous system number (ASN)?
Q3: Where does your company lease prefixes?
Q4: Has your company ever been asked to configure ROAs for the prefixes it leases out?
Q5: How does your company configure ROAs?
Q6: Has your company ever experienced a leased prefix becoming RPKI-Invalid?
Q7: Does your company track the RPKI status of the prefixes it leases out?
Q8: How is your company notified when a leased prefix becomes RPKI-Invalid?
Q9: How long does it typically take your company to correct an RPKI-Invalid ROA?

A.3. Survey for Lessees

Below are the questions we posed to organizations that rent prefixes from brokers or lessors:

Q1: How familiar is your company with RPKI overall?
Q2: What is your company's autonomous system number (ASN)?
Q3: Where does your company rent prefixes?
Q4: Has your company ever requested that a broker configure ROAs for leased prefixes so they align with your company's AS?
Q5: How are ROAs configured for those prefixes?
Q6: Does your company also monitor the RPKI status of the rented prefixes?
Q7: How does your company monitor RPKI status?
Q8: Has your company ever experienced a leased prefix becoming RPKI-Invalid?
Q9: How long did it take your company to resolve the RPKI-Invalid status?
Q10: Does your company also monitor BGP visibility for the rented prefixes?
Q11: What challenges has your company encountered during the prefix-leasing process?

Appendix B.
Relaying Hijacked Traffic to the Real Lessee

While a rogue lessor can impersonate the lessee's services by hijacking inbound connections, there may be situations where they need to forward some of that traffic back to the legitimate server—perhaps to quietly extract additional data such as session tokens or user credentials. This is not a straightforward man-in-the-middle (MITM) scenario, however, because ROV-enabled networks discard the lessee's more-specific announcement in favor of the rogue lessor's route.

To circumvent this, the adversary can place a second server in a *non-ROV* network or one that continues to accept the lessee's announcement. Traffic entering via the hijacked route is forwarded from the adversary's main server to this secondary vantage point, which still retains a valid path to the lessee. Alternatively, the adversary might host a node within the same cloud or ISP as the lessee, relaying traffic behind the scenes. This method allows the adversary to covertly maintain a "dual-path" flow: user traffic initially intercepted by the rogue route but ultimately passed along to the lessee's infrastructure, preserving partial functionality for the victim and hiding evidence of interference.

Appendix C.
Attack Feasibility Under Source Address Validation (SAV)

Although these hijack scenarios involve the lessor announcing a covering route for the victim's prefix (thus overriding the lessee's more specific route), this approach does not amount to classic IP "spoofing" that might be stopped by common SAV methods. Techniques such as Access Control Lists (ACLs) and loose or feasible-path uRPF admit traffic if the source IP range is recognized as valid in the routing table. Because the lessor's announcement appears legitimate

from the perspective of RPKI-enabled routers, these SAV configurations do not impede it.

In contrast, *strict* uRPF-where a router discards any packet arriving on an interface that is not the best (or equal-cost) path to the source IP range—can potentially block traffic from hijacked prefixes if the legitimate, more specific route remains preferred. This makes the attack less feasible in environments where strict uRPF is enforced; however, strict uRPF would only reject the adversary's route if the router also receives lease-compliant ROAs and retains the victim's prefix in the routing table. Even in such cases, the adversary could still impersonate the victim's IP addresses for a significant portion of the Internet during global or covert hijacks.

Unfortunately, strict uRPF deployment is extremely limited, with fewer than 1% of ASes implementing it [56]. Thus, the majority of SAV mechanisms in use today provide little to no defense against hijacks orchestrated by a rogue lessor.