UNIVERSITY OF AMSTERDAM

MASTER THESIS

A quantitative analysis of the Resource Public Key Infrastructure adoption of authoritative Domain Name System servers

Authors:
Sander POST
and
Brice HABETS

Supervisors:
Tom CARPAY
and
Willem TOOROP

A thesis submitted in fulfillment of the requirements for the degree of Master of Science

October 3, 2022

UNIVERSITEIT VAN AMSTERDAM

UNIVERSITY OF AMSTERDAM

Abstract

Master of Science

A quantitative analysis of the Resource Public Key Infrastructure adoption of authoritative Domain Name System servers

by Sander POST
and
Brice HABETS

The Border Gateway Protocol (BGP) was not designed with security in mind. The Resource Public Key Infrastructure (RPKI) aims to add integrity to BGP. This enables autonomous system (AS) operators to cryptographically sign their IP prefixes. With a Route Origin Authorisation (ROA) operators can establish from what AS a prefix may originate. By verifying the ROA, operators can perform Route Origin Validation (ROV). This prevents signed prefixes from being hijacked. This research tries to answer the question "What is the state of RPKI adoption on authoritative name servers?" as, to the best of our knowledge, this has not been done before.

To test this, there are three entities. One entity announces a valid prefix, one an invalid (more specific) prefix, and a querier. The entities announcing prefixes collect DNS replies.

Data sets from OpenINTEL are acquired. These data sets contain a list of authoritative DNS servers and their IPv4 and IPv6 addresses, as well as how many domains they serve. These servers are queried every hour for a total of 8 days; 4 days with a sorted list of IP addresses and 4 days with a randomized list of IP addresses. The responses are then correlated with the data sets acquired earlier and with a list of Validated ROA Payloads (VRP).

This study shows that 42.87% of the IPv4 reachable authoritative name servers are protected by ROV, and 75.06% are covered by a ROA. For IPv6, this is 39.20% and 79.76% respectively. It is also shown that, in proportion, IPv6 reachable domains are better protected than IPv4 reachable domains. 73.14% for IPv6 and 62.48% for IPv4 respectively.

With the environment used in this research, we can not precisely determine which AS does ROV. This is because paths on the Internet are dynamic as shown by our results. It is shown that an average of 0.89% IPv4 and 0.55% IPv6 of the total DNS responses arrive at different collectors during the day. Therefore, every intermediary hop needs to implement RPKI and ROV. It is only possible to assume that the AS does ROV, as currently there is no way to measure if every hop in the path does ROV.

Acknowledgements

This research was made possible by NLnet Labs. They have a huge interest in DNS as well as BGP, they're knowledgeable and it is great to chat with them. We would especially like to thank Tom Carpay and Willem Toorop for their enthusiasm and supervision of this project.

We would like to thank our classmates for a fun and interesting year at the University of Amsterdam. And we would also like to thank our families for the continuous support in the journey toward a Master of Science.

Contents

List of Figures

List of Abbreviations

DNS	Domain Name System
BGP	Border Gateway Protocol
AS	Autonomous System
IP	Internet Protocol
DNSSEC	Domain Name System Security Extensions
RPKI	Resource Public Key Infrastructure
ROA	Route Origin Authorization
ROV	Route Origin Validation
IPV4	Internet Protocol version 4
IPV6	Internet Protocol version 6
UDP	User Datagram Protocol
IANA	Internet Assigned Numbers Authority
BGPsec	Border Gateway Protocol security
PKI	Public Key Infrastructure
INR	Internet Number Resources
RIR	Regional Internet Registry
CA	Certificate Authority
NIR	National Internet Registry
LIR	Local Internet Registry
ISP	Internet Service Provider
EE certificate	End-Entity certificate
RRDP	RPKI Repository Delta Protocol
CDN	Content Delivery Network
RTR	RPKI to Router protocol
RIPE NCC	Réseaux IP Européens Network Coordination Centre
VRP	Validated ROA Payload
TLD	Top Level Domain
ccTLD	country code Top Level Domain
gTLD	generic Top Level Domain

Chapter 1

Introduction

The Domain Name System (DNS) and the Border Gateway Protocol (BGP) are two fundamental building blocks of the Internet. These protocols were not designed with security in mind. In the past, this caused outages, such as the one seen on the 24th of April 2018. On this day Amazon's Route 53 DNS service was hijacked. Attackers were able to announce a more specific prefix into BGP and redirect DNS traffic to their malicious server. They targeted a crypto wallet app and reports indicated that over $\$150,000$ in cryptocurrency was stolen [1]. A year later, on the fifteenth of May, 2019, the Taiwanese Quad101 public DNS system was hijacked [2]. For three and a half minutes an Autonomous System (AS) in Brazil was announcing that Internet Protocol (IP) space, that could have resulted in severe damage.

With the rising demand for security, different additions are proposed [3], [4]. For DNS, the Domain Name System Security Extensions (DNSSEC) is specified. It enables, for example, the cryptographical verification of DNS responses. For BGP, a proposed security building block is called the Resource Public Key Infrastructure (RPKI). This enables AS operators to cryptographically sign their IP prefixes. With a Route Origin Authorisation (ROA) operators can establish from what AS a prefix may originate. By verifying the ROA, operators can perform Route Origin Validation (ROV). This prevents signed prefixes from being hijacked.

There has been research into the adoption of RPKI on the Internet by Chung, Aben, Bruijnzeels, *et al.* [5] and on public DNS resolvers and their adoption of RPKI by Brouwer and Dekker [6]. However, to the best of our knowledge, no research has been done into authoritative name servers and their ROV adoption.

This study envisioned that this can be measured by simulating a BGP hijack by announcing a self-owned more specific prefix for both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). Then, a querier sends DNS queries to an authoritative name server. This can be done by querying addresses from a list containing IPv4 and IPv6 addresses of authoritative name servers. Two collectors listen for query responses. One collector resides in a valid prefix, the other collector in an invalid prefix. As the response will nominally show up in either collector, it is possible to measure the ROV state of a specific authoritative name server. However, a response may end up at a different collector depending on the moment of collection.

Using the environment described above, this study aims to answer the main research question:

"What is the state of RPKI adoption on authoritative name servers?"

In order to better answer that question, the following sub-questions are defined:

- How many authoritative name servers reside in an AS that does ROV?
- How many domains are protected?
- How many authoritative name servers have ROAs?

To aid reproducibility and future research, the code used during this research is publicly available at:

https://gitlab.com/spost-os3-nl/dns-rpk-why

The rest of this paper is organized as follows. In section 2 relevant information on systems such as RPKI and ROV are given. Section 3 presents the current state of research into relevant topics. Chapter 4 shows an overview of the methods used, how these are applied using the experimental setup, and what experiments are done. More importantly, it shows how readers can reproduce the experiments. Chapter 5 presents the analyzed measurements and findings. The chapters 6, 7, and 8 discuss what can be done to possibly improve measurements, discuss future work, and finally conclude the report.

Chapter 2

Background

This chapter describes the relevant background needed for this study. It starts with a very brief introduction of DNS and BGP and security protocols that are added on top in subsections 2.1 and 2.2. Subsection 2.3 describes the autonomy of BGP route hijacks to then explain RPKI in subsection 2.4 and ROV in subsection 2.5.

2.1 DNS

The Domain Name System (DNS) is one of the fundamental building blocks of the Internet. It translates domain names to IP addresses. The protocol was first specified in the early 80's [7] and later standardized [8], [9]. In this research, authoritative name servers are queried using the User Datagram Protocol (UDP). These servers are the authority for specific domains, and serve the DNS records for that domain. From here on an authoritative name server will be referred to as an authoritative.

In its basic form, DNS has no security. However, because it is an operational part of the Internet [4] security protocols were added on top. In the late 90's DNSSEC was specified [4]. DNSSEC enables cryptographical verification of DNS responses. In 2010 the first cryptographical key was prepared for worldwide use by the Internet Assigned Numbers Authority (IANA) [10].

2.2 BGP

The Border Gateway Protocol (BGP) has its origins in the late 80's and is also one of the fundamental building blocks of the Internet [11], [12]. The Internet consists of a set of ASes hosting a part of the Internet. These ASes are interconnected to each other. BGP exchanges network connectivity information between the ASes. Hosts participating in BGP are called BGP speakers. The initial protocol specifies authentication of peers. However, it does not provide confidentiality to the transmission of data.

Because of the rising demand for security [13], early 90's the community proposed several techniques to secure BGP [14]. Smith and Garcia-Luna-Aceves [15], propose cryptographically verifying the second-to-last hop in the `AS_PATH`. Another verification method was proposed by Li, Bush, Rekhter, *et al.* [16]. In the proposed protocol, received prefixes should be consistent with their allocation in an Internet Registry system. The verification relied on DNS to provide a repository with information on address space allocation.

In 2006 the Secure Inter-Domain Routing (SIDR) Working Group (WG) started at the Internet Engineering Task Force (IETF) [14]. Over the years RPKI was developed and is being deployed [5], [17]. It is explained in more detail in section 2.4. Later, the *BGPsec Protocol Specification* by Lepinski and Sriram [18] was published. BGPSec can cryptographically verify hops originating `UPDATE` messages. If all hops in an `AS_PATH` implement BGPSec, the complete path can be verified.

2.3 BGP route hijacks

BGP route hijacks happen when an AS announces an IP range that it is not authorized to. As stated by Birge-Lee, Sun, Edmundson, *et al.* [19], there are multiple types of BGP route hijacks:

- **Traditional sub-prefix attack:** an attacker makes an announcement for a more specific prefix than the victim. Due to IP routing preferring the more specific prefix, the traffic will be routed toward the attacker.
- **Traditional equally-specific-prefix attack:** an attacker announces an equally specific prefix. With this attack, only ASes closer (keeping in mind local preferences and `AS_PATH` lengths) to the attacker will route traffic to the attacker. This means some of the traffic still ends up in the victim AS.
- **Prepended sub-prefix attack:** the attacker claims to be able to reach a more specific prefix with a non-existing connection. With this attack, the attacker prepends the victim's AS number to the path, followed by its own AS number. With this attack, the attacker AS no longer claims to be the origin for the prefix. This aims to increase the invisibility of the original attack.
- **Prepended equally-specific-prefix attack:** the attacker claims to be able to reach a more specific prefix with a non-existing connection. Again, in this attack the victim's AS is prepended to the path, followed by the attacker's AS. Here, the prefix length is kept the same as the original prefix.
- **AS-path poisoning attack:** an attacker announces a valid route to a more specific prefix in order to intercept the traffic en route to the victim. Here, the attacker acts as a man-in-the-middle.

For this research, only the traditional sub-prefix attack will be considered. The available resources include a /23 IPv4 prefix that can be hijacked with a /24 and a /47 IPv6 prefix that can be hijacked with a /48. Usually, such a hijack triggers monitoring systems, as a prefix suddenly originates from a different AS [19]. For this experiment, that does not matter. Furthermore, the only interest is if the AS where the queried authoritative resides implements ROV.

2.4 RPKI

An Infrastructure to Support Secure Internet Routing [20], or also known as RPKI, is an out of band verification mechanism to validate received BGP route advertisements. The system is a hierarchical Public Key Infrastructure (PKI) containing objects and certificates. The end owner of the Internet Number Resources (INRs) is the IANA. Therefore, being the root of RPKI. The IANA then delegates trust and resources to the five Regional Internet Registries (RIRs). Each RIR, being a trust anchor and operating its own Certificate Authority (CA), can delegate trust and resources. These

delegations might include National Internet Registries (NIRs), Local Internet Registries (LIRs), or Internet Service Providers (ISPs) such that a chain of trust is created. This can be seen in figure 2.1.

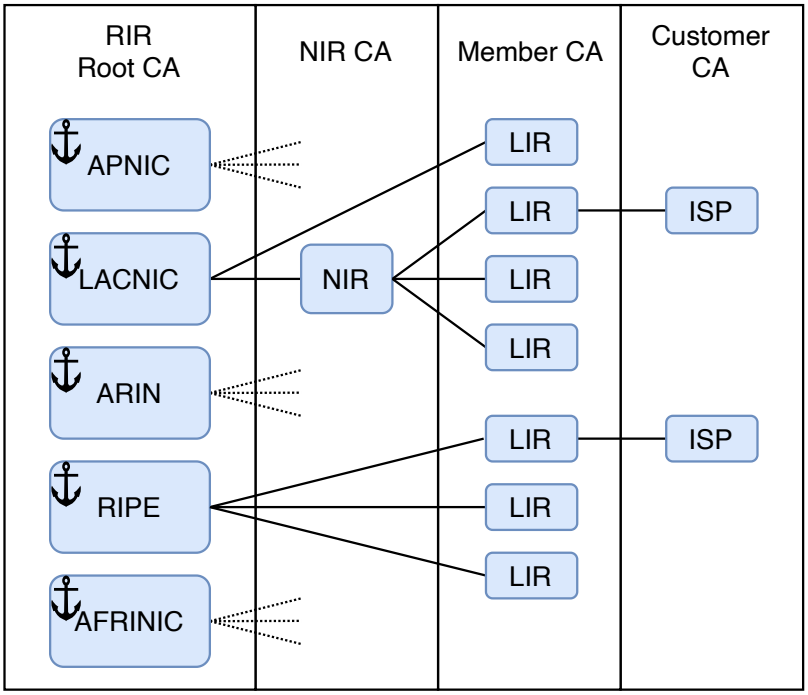

FIGURE 2.1: Certificate hierarchy of RPKI. Adapted from *RPKI Documentation* [21].

The architecture enables an entity to verifiably assert that an entity is the legitimate owner of a set of IP addresses or ASes [20]. To be able to cryptographically verify the allocation of the resources, resource certificates can be issued. By binding a public key (contained in an End Entity (EE) certificate) to the IP or AS [20], these certificates prove who is allowed to make decisions about a range of IP addresses e.g. creating ROAs.

EE certificates sign resource records, they cannot sign other certificates. Owners of a prefix can create ROAs. These identify that a prefix is authorized to originate from a given AS. Such a ROA is signed by an EE certificate.

2.5 ROV

Interaction with RPKI is most often done with specialized software. It is referred to as the relying party. The relying party has four responsibilities: fetching and caching RPKI repository objects, certificate and certificate revocation lists processing, processing RPKI repository signed objects, and distributing the validated cache.

The first interaction with RPKI is usually a connection to a database operated by a RIR. As previously discussed, the next interactions can be with a NIR, LIR, or ISP. This is shown in figure 2.2. The synchronization of the database can be performed by leveraging rsync or *The RPKI Repository Delta Protocol (RRDP)* [22]. RRDP was introduced to be more scalable and enables the use of Content Delivery Networks (CDNs) or other caching mechanisms.

Using the validated cache filters can be generated that can be applied to BGP speakers. The relying party uses the RPKI to Router (RTR) protocol to communicate with its BGP speakers.

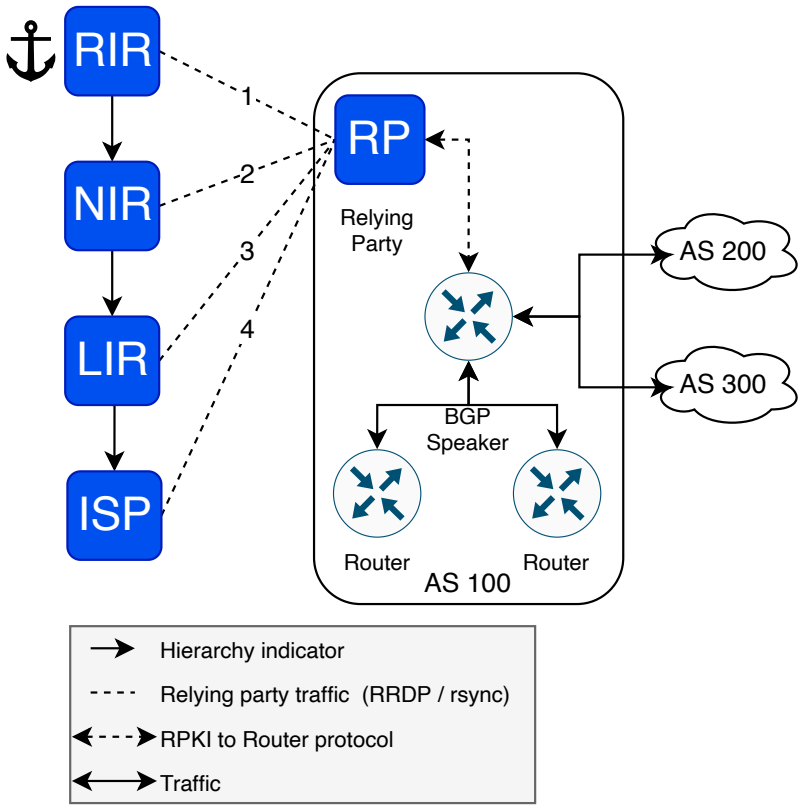

FIGURE 2.2: Relying party interaction with RPKI and BGP speakers

Chapter 3

Related Work

This chapter presents four related studies that have been done in the past. The topics of the first two works are measurements in BGP, RPKI, and ROV. The following two works combine that with DNS.

In 2018 Reuter, Bush, Cunha, *et al.* [17] researched how to measure the adoption of RPKI route validation and filtering. The research showed an uncontrolled measurement method and proposed a controlled method instead. Using the PEERING BGP Testbed [23] they were able to control valid and invalid prefix advertisements. Because of the high degree of peering relations, they were able to identify if operators implemented ROV. [17].

A year later Chung, Aben, Bruijnzeels, *et al.* [5] performed a comprehensive study on the deployment, coverage, and quality of RPKI. The researchers used a data set covering eight years of RPKI data and came to the conclusion that in late 2019 globally 12.1% of the IPv4 address space was covered by ROAs. They mentioned that RPKI was designed to filter out unauthorized BGP announcements. Furthermore, over the years the quality of RPKI improved and the researchers concluded that it was "ready for the big screen" [5]. The researchers also concluded that operators such as AT&T already dropped invalid routes. [5]

In 2020, Brouwer and Dekker [6], from the University of Amsterdam, surveyed the state of RPKI protected public DNS resolvers. During their research, they used the Réseaux IP Européens (RIPE) Atlas probes [24]. They instructed these probes to query authoritatives that contained resource records for both an RPKI valid and invalid prefix. On the third of February 2020, they concluded that 11.5% of the used probes were fully protected.

In the same year, Linssen researched the protection of eleven Top Level Domains (TLDs), including the ".com" zone. That research showed that 45% of the DNS servers resided in a protected prefix [25].

Chapter 4

Method

This chapter explains the approach of the different experiments involved in this research. The tooling and in what context it needs to operate is explained under the subsection environment 4.1. In the following subsection, the experiments are explained.

4.1 Environment

The method used in this research works towards testing which authoritative DNS servers are protected by ROV. To be flexible, the environment is abstracted. The environment contains three entities. Two entities are "collectors". In this paper, the term collector is used to describe a piece of software that catches DNS replies. The collector listens on a specified port, and the replies can be matched based on their queried domain name. Of the replies, the domain name, timestamp, and IP address are written to a file for later analysis. These collectors are located in two separate ASes with a different upstream provider and are geographically separated. Both announce an overlapping prefix into BGP. The invalid announcement is more specific than the valid announcement. It is important to note that the upstream AS for the invalid announcement should not perform ROV. If the AS does ROV, the announcement will never propagate. The exact BGP announcements can be seen in figure 4.1.

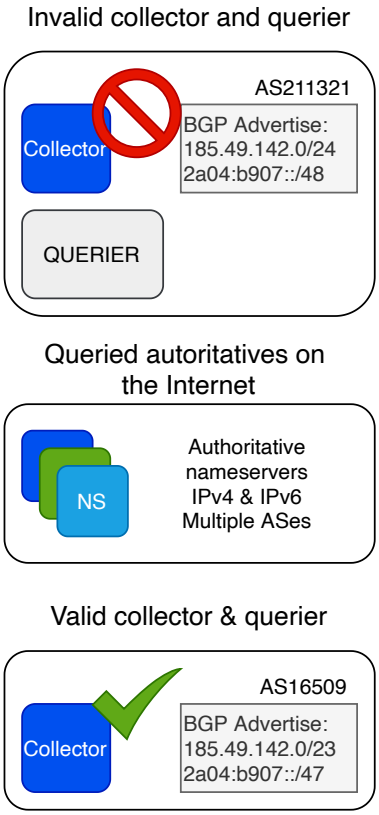

FIGURE 4.1: Overview of the experiment setup. The abstracted parts are shown: the querier, the valid and invalid collector, and the specific BGP advertisements.

To query the authoritatives, a querier is needed. This is the third entity. The querier can reside on one of the machines containing the valid or invalid collector, as long as it has the same source address that is present on both the valid and invalid collectors. It also has to be able to query authoritatives through feeding a list of IPv4 or IPv6 addresses. The purpose of this script is to send thousands of queries in orders of minutes and be able to set a specific source address, port, interface, and queried domain name. The responses can either arrive at the valid collector as shown in figure 4.2 or at the invalid collector as shown in figure 4.3. There is also the possibility that the query or response gets lost.

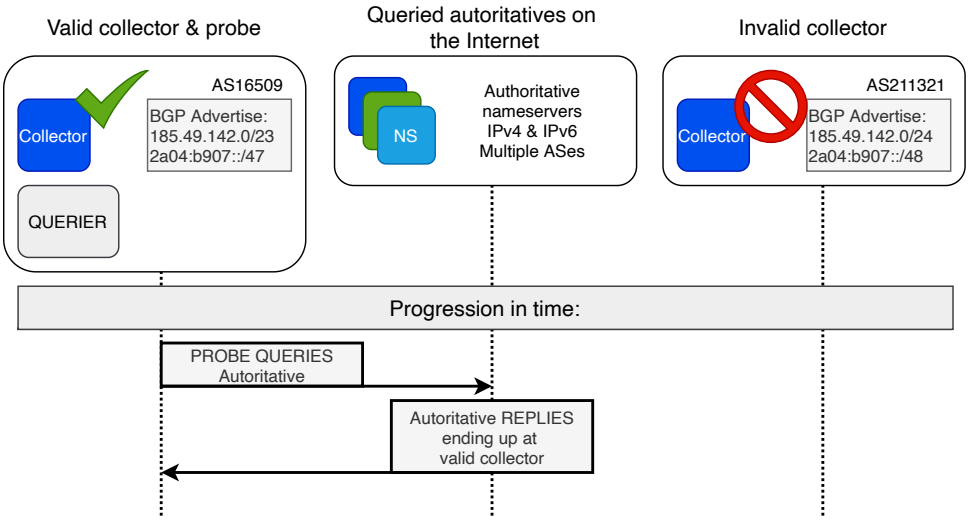

FIGURE 4.2: Overview of query and response progression in time. Here a query is sent to an authoritative. The response is sent to the IP address the query came from. In the shown progression the response arrives at the valid collector

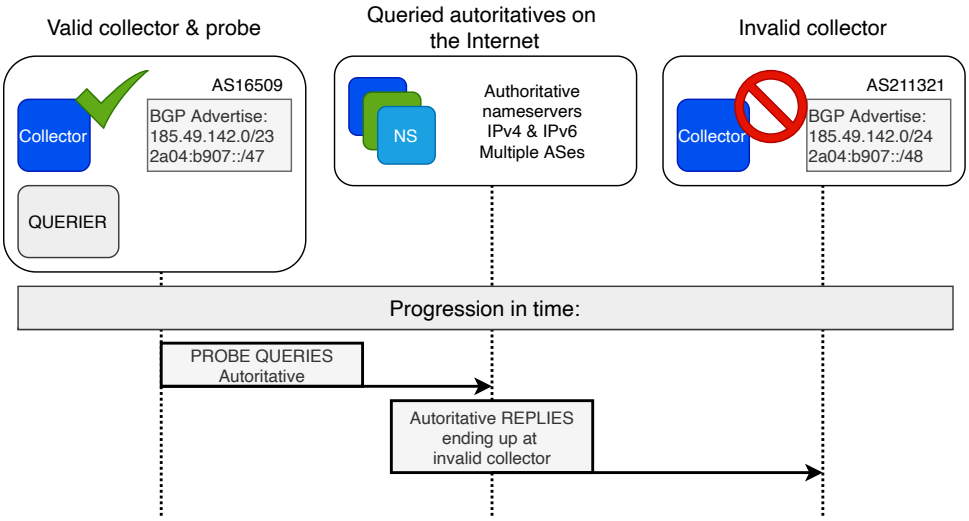

FIGURE 4.3: Overview of the query and response progression in time. On the contrary to figure 4.2, this figure shows the response arriving on the invalid collector.

4.2 Experiments

The experiments use data from the OpenINTEL Active DNS Measurements Joint Project [26]. From this platform, a data set of authoritatives is obtained. The data set contains IPv4 and IPv6 addresses and their respective A and AAAA resource records. The sets contain many country code TLDs (ccTLDs), generic TLDs (gTLDs), data from the Alexa top 1 million, and data from the Cisco Umbrella top 1 million [26].

The first two experiments are trivial for this research. All other experiments conducted have the first two experiments' resulting data sets as their basis. These two experiments applied two different strategies to how the authoritatives are queried. In the first experiment, the lists of addresses are ordered. In the second experiment, this list is randomized. The second experiment has been chosen to circumvent possible rate limiting techniques possibly implemented by DNS operators. In both experiments, the list from OpenINTEL is used to query the authoritatives every hour. Due to time constraints linked to this project, both experiments gather data for four days.

The collected DNS responses on the collectors yield a list of both IPv4 and IPv6 addresses. These responses are written to files by the hour. To display the collected responses more clearly, the measurements of each hour are grouped per day. Then all unique addresses are filtered leaving the distinct data per day. This is done separately for the valid and invalid collectors as well as IPv4 and IPv6 addresses.

When multiple responses from the same authoritative arrive at both valid and invalid collectors during different hours of querying during the day, it is called a duplicate. To check if there are any duplicates in the resulting responses, a comparison between the collected responses per hour is performed. This way, this experiment can show that DNS responses can take different paths on the Internet during the day.

From OpenINTEL, a different data set is acquired. This data set contains a list of authoritatives and the number of domains they serve. This is then correlated with the gathered responses from the first two experiments. This experiment gains insight into how many domains are served by an authoritative that presumably resides in an AS that either does or does not do ROV.

A list containing ROAs that has been validated by a relying party is acquired. The list with the Validated ROA Payloads (VRPs) is correlated with gathered data from the first two experiments. This experiment gains insight into how many authoritatives are covered by a ROA.

Chapter 5

Results

In the following section, the results of the conducted experiments are presented. All results are based on the main data set gathered from the first two experiments. As only the order of queries of these experiments differentiates, the graphs presented in this section visualize a total of eight days. In total 731,113 IPv4 and 79,701 IPv6 addresses are queried every hour.

5.1 General overview

Figure 5.1 shows an overview of authoritative responses per day. In green, the responses collected at the valid collector are shown. In blue, the responses collected at the invalid collector are shown. Furthermore, IPv4-related statistics are shown in the top graph, and IPv6 is shown in the bottom graph. What is immediately apparent, is that the data set for IPv4 is nine times larger than the IPv6 data set. For IPv4 on average 339,179.13 responses arrive at the valid collector, for IPv6 that average is 31,239.75. On the invalid collector, on average, 375,096 IPv4 responses arrive. For IPv6 that average is 33,090.63.

Over the eight days combined, 42.87% of the IPv4 responses arrived at the valid collector and 47.41% at the invalid collector. For IPv6, this is 39.20% and 41.52% respectively. The percentages that can be found in the graph indicate the percentage of the total amount of IP addresses queried. The non-responsive queries are not shown. Therefore, the percentages shown do not add up to 100.

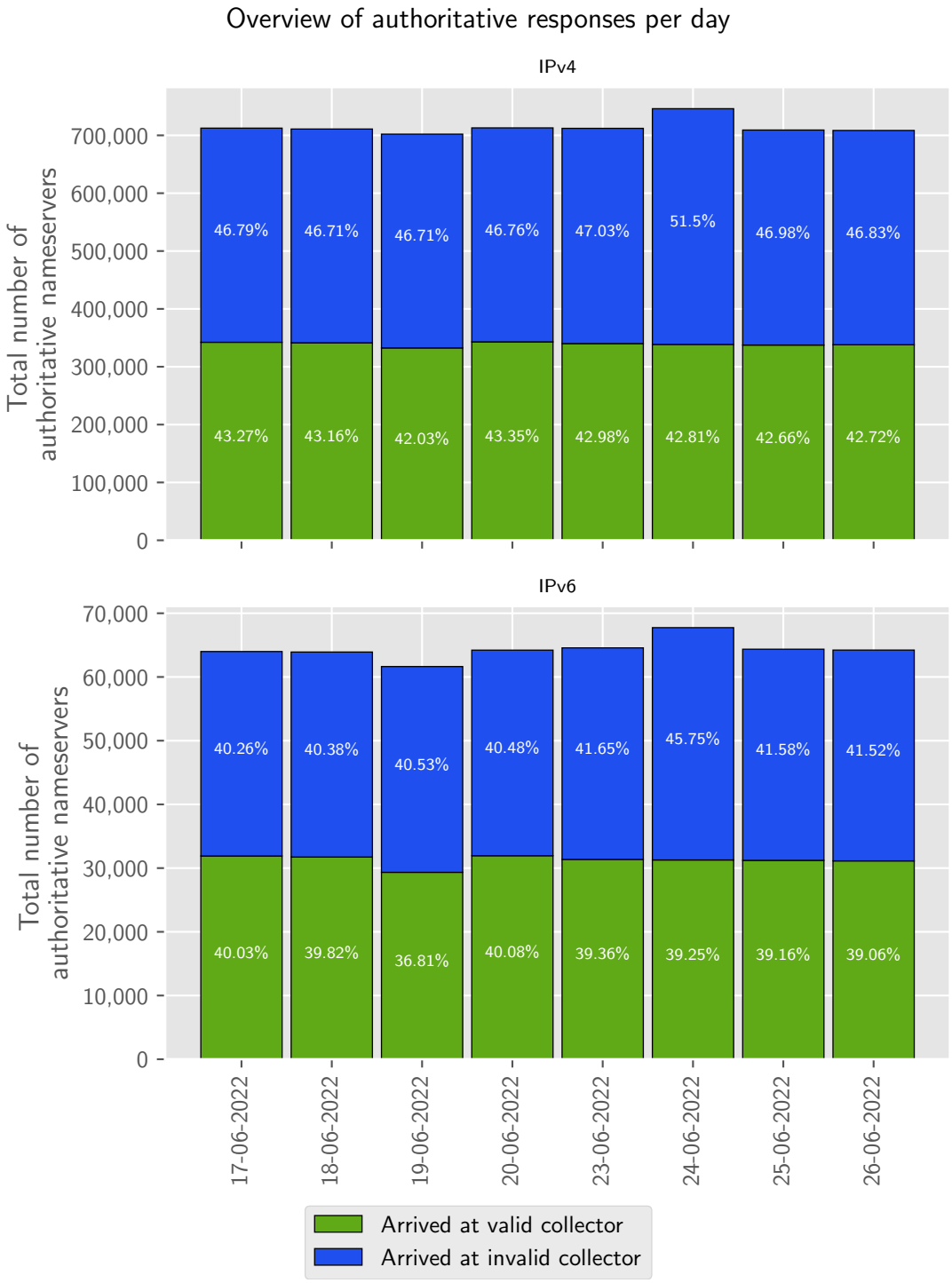

FIGURE 5.1: Overview of experiment results per day. On the y-axis, the total amount of DNS responses can be seen. Shown in the graph are the responses collected on the valid and invalid collector. There are 9 times more IPv4 responses than IPv6 responses.

5.2 Overview of protected domains

How many domains are served per authoritative and what their ROV state is, is shown in figure 5.2. In the top graph, the IPv4 reachable domains are shown. The bottom graph does this for IPv6. Green represents the domains that are protected by ROV and blue the unprotected. It should be noted that the amount of IPv4 reachable domains is larger than the number of IPv6 reachable domains. However, in percentages, on average the IPv6 reachable domains are slightly better protected. On average 73.14% of the IPv6 reachable domains are protected by ROV. For IPv4 that average is lower: 62.48%. On average, 31.52% of the IPv4 reachable domains are unprotected. For IPv6 that average is 24.02%.

The percentages shown are based on the total amount of domains in the data set. Like in figure 5.1, the results shown in figure 5.2 also exclude non-responsive queries.

On average, 186, 442, 390.25 IPv4 reachable domains and 176, 386, 002.75 IPv6 reachable domains are served by an authoritative that is presumably protected by ROV. For the unprotected domains that average is 94, 066, 720.63 for IPv4 and 57, 920, 887.75 for IPv6.

The results vary significantly due to duplicates throughout the day.

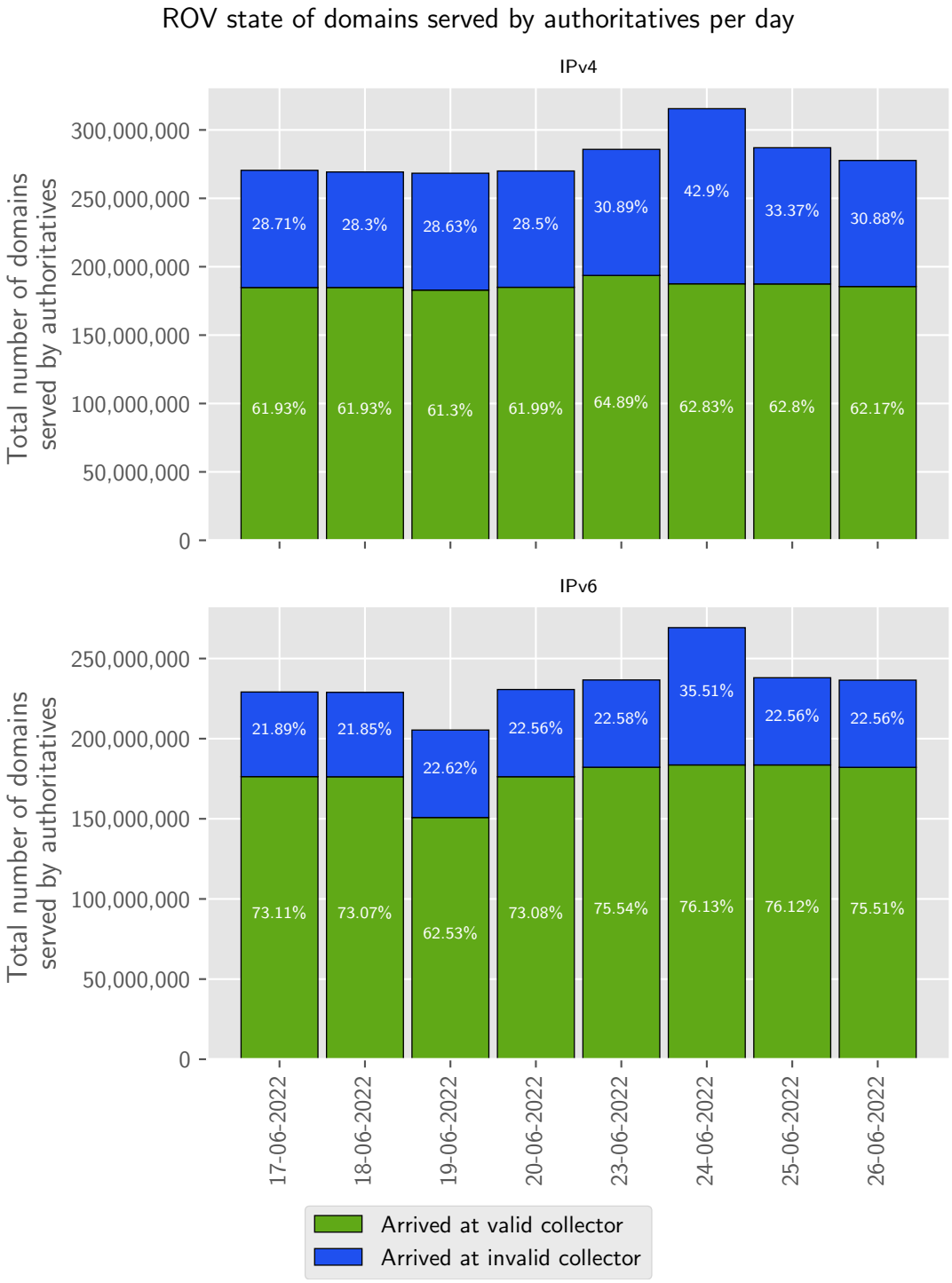

FIGURE 5.2: General overview of the amount of domains served by authoritatives. On the y-axis the amount of domains is shown. Shown on the graph are validating and non-validating domains. There are more domains reachable over IPv4 then over IPv6.

5.3 Duplicates

The third result, shown in figure 5.3, shows responses that are seen on both the valid and invalid collectors. As described in previous results, the top graph shows the IPv4 space and the bottom graph shows the IPv6 space. At the bottom of each bar, the proportional amount of the total responses is shown in percentages. The graph shows that throughout the day, different paths to and from the authoritative can be taken. Outliers can be observed for both the IPv4 and IPv6 reachable authoritatives on the 24^{th} of June. That day was good for a total of $38,137$ IPv4 and $2,486$ IPv6 responses seen on both collectors. In percentages, that is 4.82% for IPv4 and 3.12% for IPv6 of the total responses.

In summary, an average of $9,977.13$ IPv4 and 436.25 IPv6 duplicates are seen. These make up for an average of 0.89% and 0.55% of the total amount of responses.

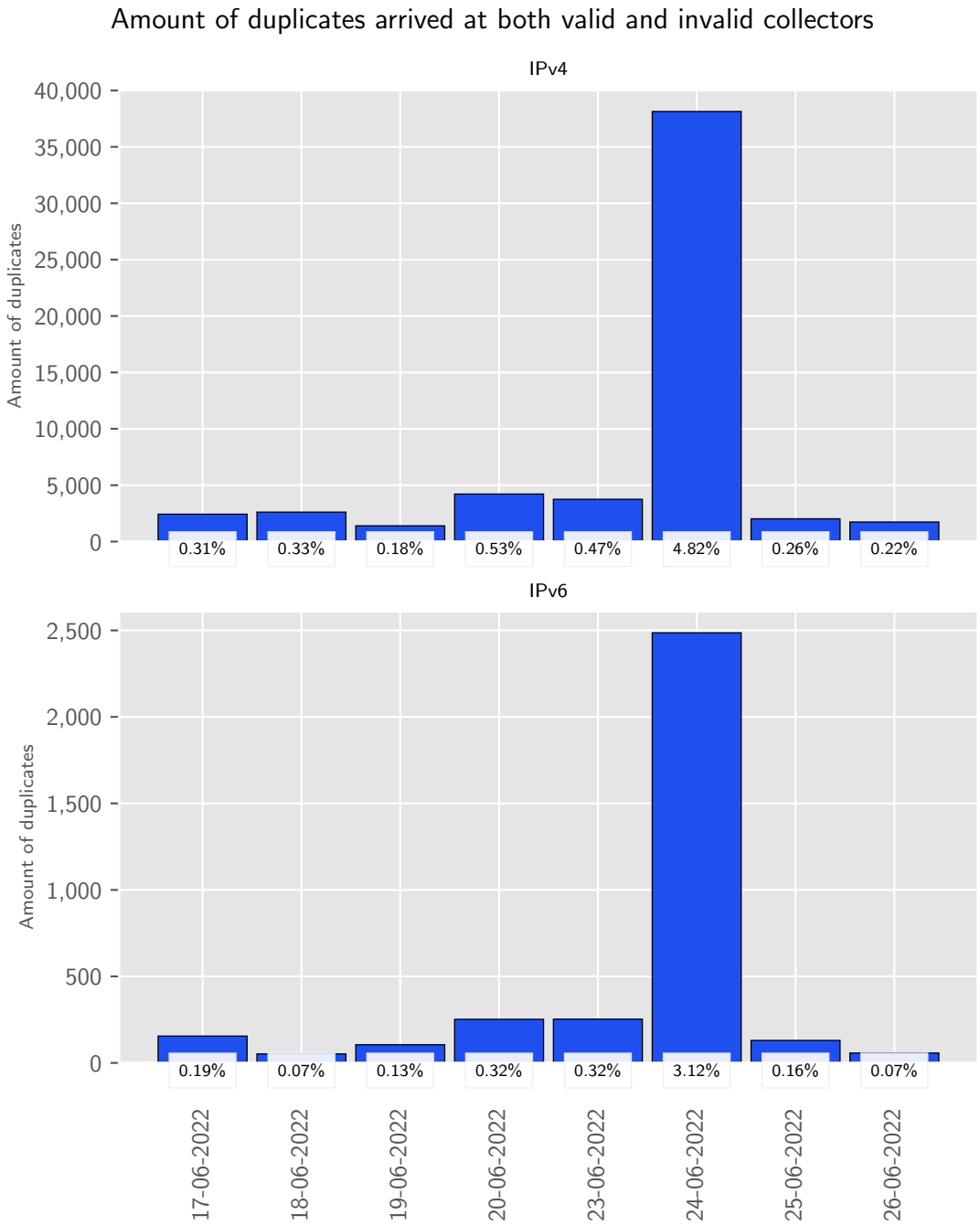

FIGURE 5.3: This figure shows the total amount of duplicates. These are responses from authoritatives seen on both valid and invalid collectors during different hours. Below the bars, the percentage of the total queried authoritatives can be seen.

5.4 Overview of authoritatives and their ROAs

The responses collected are correlated against a list of VRPs as described in section 4.2. In figure 5.4, the overview of authoritatives IP addresses covered is shown. In the top graph, the IPv4 results are shown. In the bottom graph, the IPv6 results are shown. Green represents the responses collected at the valid collector of which IP addresses are covered by a ROA. Blue represents responses collected at the invalid collector of which IP addresses are covered by a ROA.

It can be seen that, on average, 322,096.63 of the IPv4 authoritative responses collected on a valid collector are covered by a ROA. That is an average of 40.71% of the total average responses. For IPv6 reachable authoritatives, this average is 39,963.13. That is an average of 50.14% of the total average responses. Authoritatives' addresses seen on the valid collector are signed and covered by a ROA and are presumably protected by ROV.

There are also responses collected on the invalid collector that are covered by a ROA. For IPv4, this is an average of 271,660.38. That is 34.35% of the average total amount of responses. For IPv6 the averages lie at 23,605.63 and therefore 29.62% of the average total amount of responses. The total proportional average of IPv4 authoritatives covered by a ROA is 75.06% and 79.76% for IPv6 reachable authoritatives covered by a ROA.

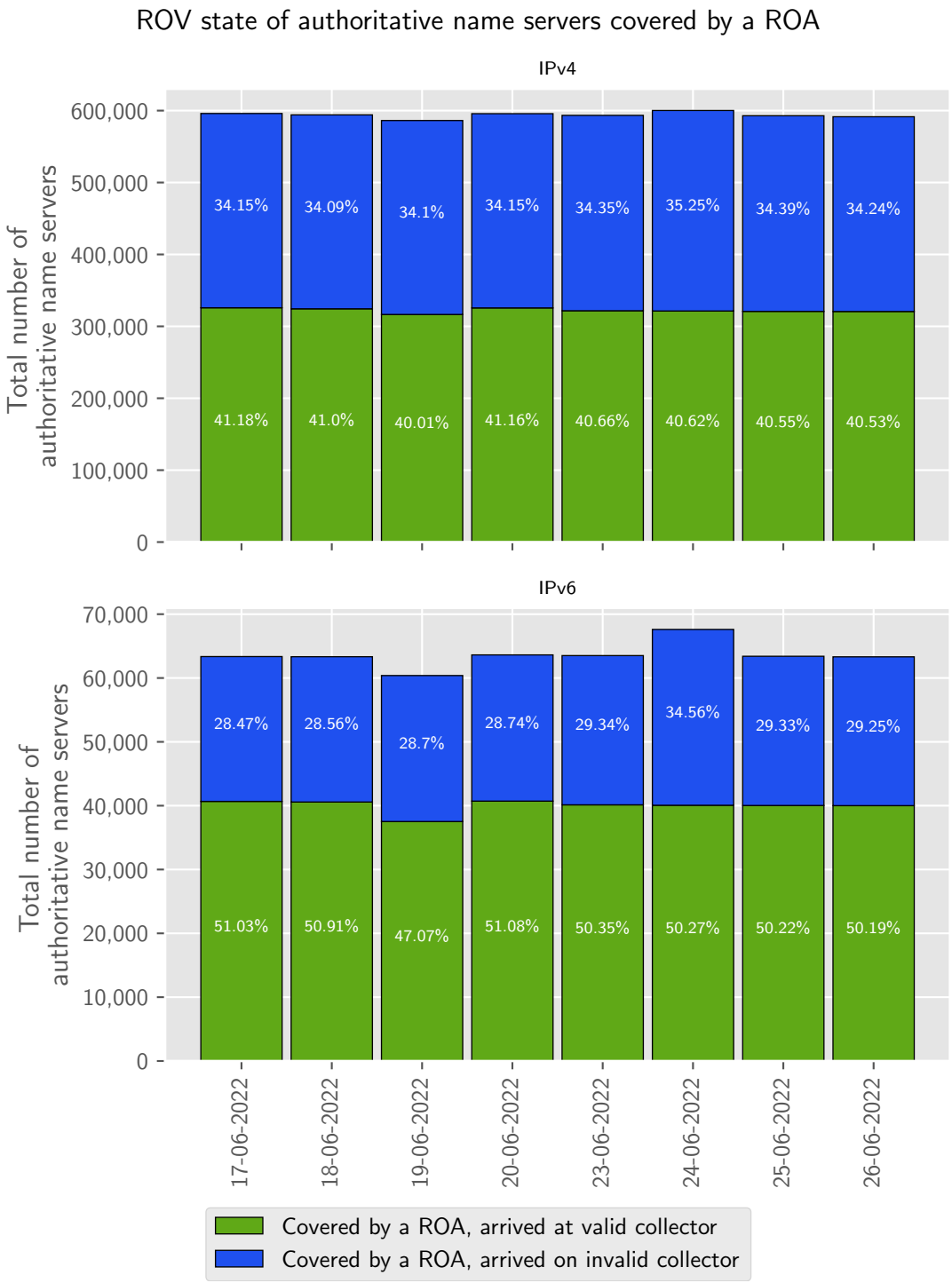

FIGURE 5.4: General overview of authoritatives covered by a ROA. Showing the responses collected and the proportional value of the total send queries. For IPv6 reachable authoritatives that value is a bit higher than for IPv4 reachable authoritatives.

Chapter 6

Discussion

This chapter describes discussion points. It starts with considerations regarding the data set from OpenINTEL. Then it describes what the weakest-link problem is, how it affects the presented results, and how that problem could be circumvented in the future.

The data set from OpenINTEL contains not just public addresses. We hypothesize that primary authoritatives end up in this list but are not publicly reachable. The true cause of this is outside the scope of this research. The list of addresses is first sanitized and leaves only public addresses.

The current results are based on one specific vantage point of the Internet. The IP prefixes for both the valid and invalid collector originate from the same ASes. For a more granular view, the responses should be captured from multiple places on the Internet. Preferably such that the paths towards the authoritatives differ in between experiments. Furthermore, the current list of authoritatives might include anycast addresses [27]. This variable is not considered during the experiments and can therefore give a different view of reality. The variability of anycast routing might also be the reason for the duplicates.

With the results gathered during this experiment, it is not possible to definitively state that the authoritative is protected by ROV (even if the response is captured on the valid collector). This is because the internet is dynamic and ROV needs to be implemented on every intermediary hop. This is due to the weakest-link problem. One of the scenarios with this problem is seen in figure 6.1. Here a validating AS is surrounded by non-validating ASes. In case the route to the validating AS is being hijacked, returning traffic will never arrive. Normal operation in this specific case shows that traffic towards the validating AS will arrive at that specific AS. However, if that route is being hijacked the traffic will never return to the same location.

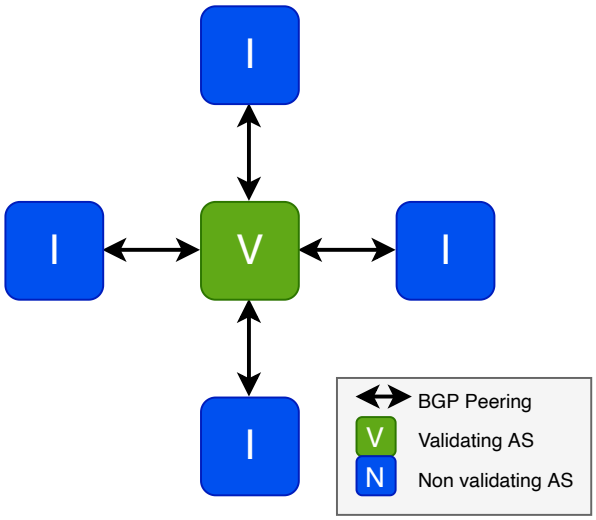

FIGURE 6.1: A validating AS surrounded by non-validating ASes

In both presented paths in figure 6.2, the upstream AS decides where the response will end up. This is even so if the authoritative resides in an AS that does ROV. In the same figure can see that even if most of the chain implements ROV, it can go wrong at the upstream AS. However, on the Internet, multiple networks are interconnected with each other and therefore this is not always the case.

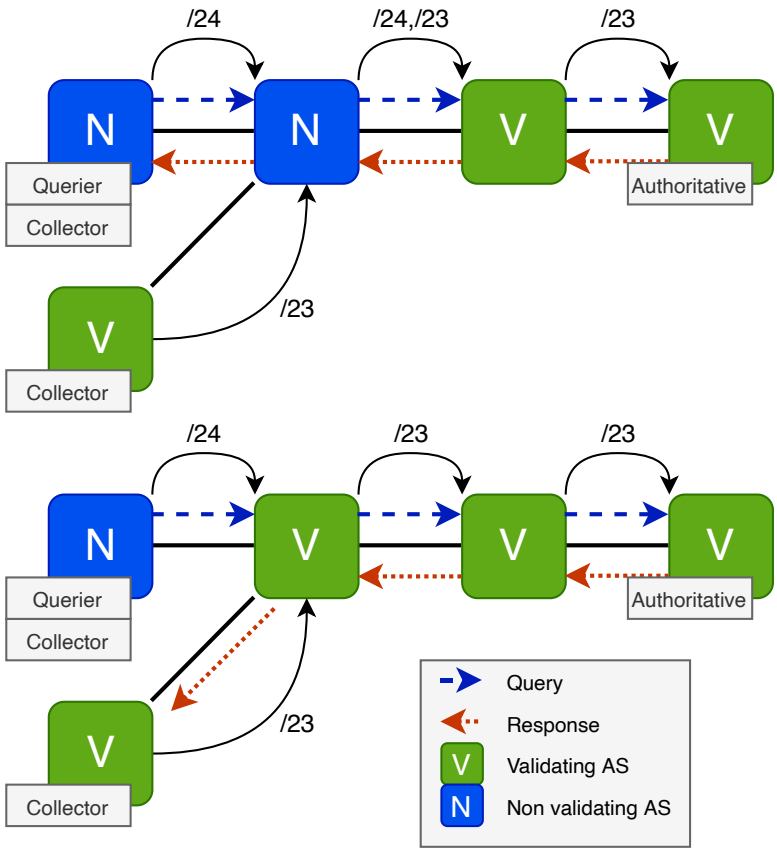

FIGURE 6.2: The difference with a non-validating and validating upstream AS

With the method that the results are collected, it is not possible to say whether the whole path is protected or not. With the current setup, it can only be assumed. The reasoning behind this is illustrated in figure 6.3. Here, the upstream AS validates and does not propagate the invalid advertisement. In this case, the chain is protected even though one of the intermediary hops and the authoritative are not protected by ROV. This also highlights one of the strengths of ROV. If one AS implements ROV, others could be protected as well. However, on the Internet networks are usually interconnected with each other. Therefore, the invalid announcement will presumably still spread through the Internet.

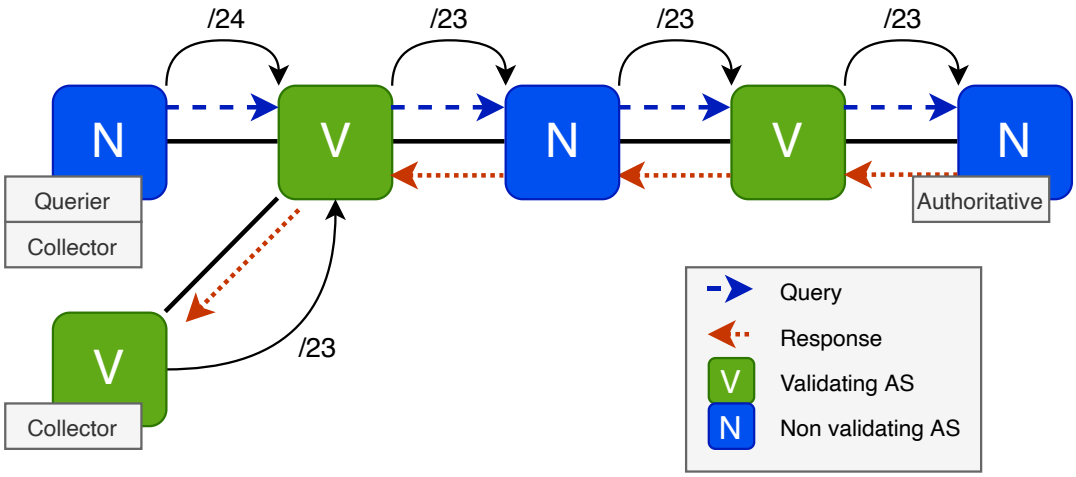

FIGURE 6.3: The authoritative is protected, even though it does not do ROV

The community has seen this limitation in BGP routing [18]. To overcome this issue, BGPsec can be implemented. The protocol lets every AS in a given `AS_PATH` cryptographically verify the `UPDATE` message [18]. However, this method relies on all operators implementing RPKI and BGPsec. It is also computationally expensive because all advertised routes need to be signed and all received BGP announcements need to be validated.

Chapter 7

Future Work

This chapter introduces three new studies that can be done. As previously described, the results in this research are based on one specific vantage point of the Internet. It could be beneficial to run the same experiments in different locations on the Internet. This could produce significantly different results.

As previously described it is assumed that the Internet is dynamic. There is old research [28] done on this topic and it falls outside the scope of this research. This is why further research and development are needed in this specific area. An option to measure how dynamic the Internet is could be done by measuring and comparing the paths specific traffic takes. Measuring from the same source and destination for a specified amount of time could give insights into this problem.

Another interesting area of research is finding the first AS in the chain that does not implement ROV i.e. the first weakest-link. This could be done with a proposed "TraceROV" tool that makes use of the well know tool "Traceroute" and a setup similar to the one described in section 4.1. This TraceROV tool sets the hop limit to minimal to let the next hop generate an "ICMP time exceeded" message and then measures where the response arrives. The hop limit is then increased until the final destination is reached, or the response ends up at the invalid collector. Both collectors should communicate to know when a response arrives at the invalid collector.

Chapter 8

Conclusion

Route hijacks have been seen in recent Internet history. RPKI and ROV offer to make this part of the Internet more secure. 42.87% of IPv4 authoritatives and 39.20% of IPv6 authoritatives are presumed to be protected by ROV. Besides that, 62.48% of IPv4 domains and 73.14% of IPv6 domains are served by authoritatives that presumably are protected by ROV. Next, it is visible that the Internet is very dynamic. Throughout the day, a response can end up at a different collector than before. Especially on the 24th of June a lot of those duplicates are found: 4.82% for IPv4 and 3.12% for IPv6. Finally, 75.06% of the IPv4 addresses and 79.76% of IPv6 addresses are covered by a ROA. Of those, 40.71% of IPv4 reachable authoritatives and 50.14% of IPv6 reachable authoritatives presumably reside in an AS that does ROV.

Assuming the data set used in this research is similar to the one used by Linssen [25], this study shows that RPKI adoption is steadily increasing and thus answers the main research question "What is the state of RPKI adoption on authoritative name servers?". Depending on the path that a response took, it either ended up at a valid collector or invalid collector. This was shown to measurably happen, highlighting the importance that all intermediate hops need to implement RPKI and ROV.

Bibliography

[1] N. Ameet, *Anatomy of a bgp hijack on amazon's route 53 dns service*, 2018. [Online]. Available: https://www.thousandeyes.com/blog/amazon-route-53-dns-and-bgp-hijack.

[2] A. Siddiqui, *Public dns in taiwan the latest victim to bgp hijack*, 2019. [Online]. Available: https://www.manrs.org/2019/05/public-dns-in-taiwan-the-latest-victim-to-bgp-hijack/.

[3] G. Huston. "A survey on secure inter-domain routing." (2021).

[4] D. E. E. 3rd and C. W. Kaufman, *Domain Name System Security Extensions*, RFC 2065, Jan. 1997. DOI: 10.17487/RFC2065. [Online]. Available: https://www.rfc-editor.org/info/rfc2065.

[5] T. Chung, E. Aben, T. Bruijnzeels, *et al.*, "Rpki is coming of age: A longitudinal study of rpki deployment and invalid route origins," in *Proceedings of the Internet Measurement Conference*, ser. IMC '19, Amsterdam, Netherlands: Association for Computing Machinery, 2019, 406–419, ISBN: 9781450369480. DOI: 10.1145/3355369.3355596. [Online]. Available: https://doi.org/10.1145/3355369.3355596.

[6] M. Brouwer and E. Dekker, "The current state of dns resolvers and rpki protection," 2020.

[7] *Domain names: Concepts and facilities*, RFC 882, Nov. 1983. DOI: 10.17487/RFC0882. [Online]. Available: https://www.rfc-editor.org/info/rfc882.

[8] P. Mockapetris, "DOMAIN NAMES - CONCEPTS AND FACILITIES," RFC Editor, RFC 1034, 1987, pp. 1–55. DOI: 10.17487/RFC1034. [Online]. Available: https://www.rfc-editor.org/rfc/rfc1034.txt.

[9] ——, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION," RFC Editor, RFC 1035, 1987, pp. 1–55. DOI: 10.17487/RFC1035. [Online]. Available: https://www.rfc-editor.org/rfc/rfc1035.txt.

[10] I. A. N. Authority. "Trust anchors and keys." (2010), [Online]. Available: https://www.iana.org/dnssec/files.

[11] *Border Gateway Protocol (BGP)*, RFC 1105, Jun. 1989. DOI: 10.17487/RFC1105. [Online]. Available: https://www.rfc-editor.org/info/rfc1105.

[12] J. Yu, J. C. Honig, M. Mathis, D. Katz, and Y. Rekhter, *Application of the Border Gateway Protocol in the Internet*, RFC 1164, Jun. 1990. DOI: 10.17487/RFC1164. [Online]. Available: https://www.rfc-editor.org/info/rfc1164.

[13] T. van Rossum, "A meta-analysis of BGP threats and security to provide a new direction for practical BGP security," M.S. thesis, Delft University of Technology, the Netherlands, 2020.

[14] *Secure inter-domain routing charter-ietf-sidr-04*. [Online]. Available: https://datatracker.ietf.org/doc/charter-ietf-sidr/.

[15] B. R. Smith and J. Garcia-Luna-Aceves, "Efficient security mechanisms for the border gateway routing protocol," 1997.

[16] T. Li, R. Bush, Y. Rekhter, and T. J. Bates, "DNS-based NLRI origin AS verification in BGP," Internet Engineering Task Force, Internet-Draft draft-bates-bgp4-nlri-orig-verif-00, Feb. 1998, Work in Progress, 10 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-bates-bgp4-nlri-orig-verif-00.

[17] A. Reuter, R. Bush, I. Cunha, E. Katz-Bassett, T. C. Schmidt, and M. Wählisch, "Towards a rigorous methodology for measuring adoption of rpki route validation and filtering," *SIGCOMM Comput. Commun. Rev.*, vol. 48, no. 1, 19–27, 2018, ISSN: 0146-4833. DOI: 10.1145/3211852.3211856. [Online]. Available: https://doi.org/10.1145/3211852.3211856.

[18] M. Lepinski and K. Sriram, *BGPsec Protocol Specification*, RFC 8205, Sep. 2017. DOI: 10.17487/RFC8205. [Online]. Available: https://www.rfc-editor.org/info/rfc8205.

[19] H. Birge-Lee, Y. Sun, A. Edmundson, J. Rexford, and P. Mittal, "Bamboozling Certificate Authorities with BGP," 2018.

[20] M. Lepinski and S. Kent, *An Infrastructure to Support Secure Internet Routing*, RFC 6480, Feb. 2012. DOI: 10.17487/RFC6480. [Online]. Available: https://www.rfc-editor.org/info/rfc6480.

[21] *Rpki documentation*. [Online]. Available: https://rpki.readthedocs.io/en/latest/rpki/introduction.html.

[22] T. Bruijnzeels, O. Muravskiy, B. Weber, and R. Austein, *The RPKI Repository Delta Protocol (RRDP)*, RFC 8182, Jul. 2017. DOI: 10.17487/RFC8182. [Online]. Available: https://www.rfc-editor.org/info/rfc8182.

[23] *About peering: Peering - the bgp testbed*. [Online]. Available: https://peering.ee.columbia.edu/about/.

[24] RIPE. "About ripe atlas." (), [Online]. Available: https://atlas.ripe.net/landing/about/.

[25] R. Linssen, "Vulnerability of dns name servers against bgp hijacking," Feb. 2020.

[26] *Latest news*. [Online]. Available: https://openintel.nl/.

[27] Cloudflare. "What is anycast? | how does anycast work?" (), [Online]. Available: https://www.cloudflare.com/learning/cdn/glossary/anycast-network/.

[28] Ítalo Cunha, R. Teixeira, D. Veitch, and C. Diot, "Predicting and Tracking Internet Path Changes," 2011.