Assessing the security of Internet paths: A case study of Dutch critical infrastructures

Shyam Krishna Khadka
University of Twente

Suzan Bayhan
University of Twente

Ralph Holz
University of Twente and University of Münster

Cristian Hesselman
SIDN Labs and University of Twente

ABSTRACT

Many critical infrastructures (CIs) rely on cloud services (e.g., email) for their daily operations. However, these CIs typically have limited insight into the security status of the paths that their traffic might follow across the Internet to reach their cloud provider's infrastructures. For example, a CI might not know that their traffic passes through Autonomous Systems (ASes) that do not implement Route Origin Validation (ROV). As a result, the CI is vulnerable to prefix hijacks, which can render the cloud operator unavailable to the CI or breach the confidentiality and integrity of the CI's data. To provide such insights, we develop a generic method that finds plausible paths from one AS to another and identifies to what extent the ASes on the path support ROV. We use our method for a case study to find secure paths from four CIs in the Netherlands to Microsoft mail, which many CIs use. We use Border Gateway Protocol (BGP) routing data from four route collectors in the Netherlands in combination with the ROV scores of the ASes. Our analysis shows the existence of multiple fully ROV-protected paths from the four CIs to Microsoft among a larger set of partially ROV-protected paths. Our case study also shows that implementing ROV fully by the immediate upstream providers of CIs would result in an increase in the number of fully ROV-protected paths by 72.5% on average.

CCS CONCEPTS

• **Networks** → **Network measurement**; • **Security and privacy** → **Network security**.

ANRW '24, July 20–26, 2024, Vancouver, CA

ACM ISBN TBA-XXXX-X/
https://doi.org/XXXXXXX.XXXXXXX

KEYWORDS

Internet path finding, Path security

ACM Reference Format:
Shyam Krishna Khadka, Suzan Bayhan, Ralph Holz, and Cristian Hesselman. 2024. Assessing the security of Internet paths: A case study of Dutch critical infrastructures. In *Proceedings of (ANRW '24).* ACM, Vancouver, Canada, 7 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

According to the European Commission, "critical infrastructures (CIs) consist of those physical and information technology facilities, networks, services, and assets which, if disrupted or destroyed, have a serious impact on the health, safety, and security or economic well-being of citizens or the effective functioning of the governments in the Member States" [6]. Examples of CIs are facilities for national transport, distribution and production of electricity, oil, and gas, drinking water supply, and financial services [8]. Like many enterprises in the European Union (EU), CIs rely heavily on email services provided by hypergiants such as Microsoft and Google [3, 33], which is a development that even hit the mainstream news in the Netherlands recently [28]. For example, ING Bank, KPN (a big telecom operator in the Netherlands), and Schiphol Airport (the main international airport of the Netherlands) depend on Microsoft Mail.

As a result, CIs have a strong need for secure paths across the Internet to their cloud-based email service, which often involves multiple Autonomous Systems (ASes) collaboratively forwarding traffic from the CI to the cloud operator and vice versa. We argue that for a path to be secure, it is important that all ASes on that path are secure. However, finding such fully secured paths is a problem for two reasons. First, a source AS (e.g., a CI's AS) does not know all the available paths to a particular destination (e.g., Microsoft mail) because ASes might filter Border Gateway Protocol (BGP) route advertisement messages by forwarding routes to a selection of their BGP peers rather than to all of them. This is known as "selective announcement" and is based on an individual AS' traffic engineering policies [15, 35]. Second, a source AS does not know if paths are fully secure or

not because there is no mechanism to measure the security status of the overall path based on the security of the ASes on the path.

In this paper, we address the problem of finding fully secure paths in terms of their Route Origin Validation (ROV) [4] status. ROV is an example of a routing security metric that has become a more widely deployed solution compared to ASPA, and BGPSec to secure BGP in recent years. The intuition behind ROV is that it validates the signatures of the address space that ASes announce, thus preventing *BGP prefix hijacks*. These are common incidents on the Internet and have been used to attack payment systems [25], steal crypto-currency [26], disrupt traffic [16], and create DDoS attacks [17]. Finding fully ROV-protected paths is important because prior research [11, 20] shows that an AS that does not implement ROV can cause ASes that do implement ROV on a path to be a victim of BGP prefix hijacking.

We answer the following research questions:

- Given a CI (source AS), what is the number of fully and partially ROV-protected paths through which the CI can connect to its cloud provider (destination AS) and what are the path lengths in terms of AS hops?
- What is the effect of a CI's upstream provider implementing ROV fully on the number of fully ROV-protected paths that the CI has at its disposal?

We address these questions by developing a measurement methodology and by applying it in a case study to find ROV-protected paths between four CIs in the Netherlands (e.g., a water supply company and a bank) and Microsoft Mail.

We make the following two contributions:

- We find paths from a source AS to a destination AS by analyzing a month of data from BGP RIBs (Routing Information Bases) using four route collectors in the Netherlands and show the security status of each path by calculating their ROV scores. We calculate the ROV status of each AS on the path using ROVista API [20] to show the security status of the paths. To the best of our knowledge, we are the first to calculate the security status of a path in combination with path-finding.
- For our case study, we show that implementing ROV fully by the upstream provider of two CIs results in an additional 14 and 9 ROV-protected paths which is on average increment of 72.5%.

The remainder of this paper is structured as follows: Section 2 provides background information about BGP and ROV. We discuss related work in Section 3 and introduce our methodology in Section 4. We present our case study in the Netherlands in Section 5, and discuss our findings and limitations in Section 6. We end with conclusions and future work in Section 7.

2 BACKGROUND

In this section, we provide a brief overview of how BGP works, how ROV helps prevent routing attacks, and why having all the ASes implementing ROV on a path is crucial. We use Figure 1 as an example involving two paths that we found using our path-finding method (see Section 4).

2.1 Border Gateway Protocol (BGP)

BGP is the routing protocol that provides information on how to reach a particular destination (prefix) on the Internet. ASes use BGP to exchange routing information with each other. Figure 1 shows an example of a BGP route for prefix 52.96.0.0/12 (Microsoft Mail) , which is *15625 19905 6453 3257 8075* (path 2). AS8075 originates the announcement for the route, which it forwards to its neighbors (AS3257). AS3257 stores it in its routing table and forwards it to the next hop AS (AS6453), and so forth until it reaches the CI's AS (15625). Each AS on the path forwards a route to its neighbors according to its routing policy, which may prefer to only send the advertisement for 52.96.0.0/12 to its selected neighbors. In the opposite direction, ASes use a BGP route to forward their traffic. In our example, the data that AS19905 forwards to AS8075 will go through ASes *6453 3257 8075*.

2.2 Route Origin Validation (ROV)

BGP lacks built-in security. For example, in Figure 1, an attacker (AS1000) falsely claims itself as an owner of prefix 52.96.0.0/12 and announces a more specific prefix 52.101.0.0/16. This type of behavior where an AS illicitly announces an IP prefix owned by another AS is referred to as a *BGP prefix hijack*. To protect themselves against this type of attack, ASes can implement ROV. ROV uses the Resource Public Key Infrastructure (RPKI) [18] to create a cryptographically signed record of an AS Number (ASN) and an IP prefix, known as a *Route Origin Authorization* (ROA) [19]. An AS implements ROV-based filtering if it checks the ROA and drops an illicit IP prefix (RPKI-invalid prefix) originated by an AS.

We illustrate the importance of having all ASes on a path implementing ROV through Figure 1, which shows two possible paths through which AS15625 (CI) can forward its traffic toward AS8075 (Microsoft Mail): path1 *[15625, 19905, 6453, 4755, 8075]* and path2 *[15625, 19905, 6453, 3257, 8075]*. Here, all the ASes except AS4755 (red border) implement ROV filtering and they can filter out the fake routes. When the attacker (AS1000) announces a more specific prefix 52.101.0.0/16, AS4755 stores two routes: 52.96.0.0/12 (from AS8075) and 52.101.0.0/16 (from AS1000), and forwards them to AS6453. AS6453 subsequently discards the route with AS path *[4755 1000]* as AS6453 implements ROV and therefore knows that the path is a fake path. As a result, it stores only the path *[4755 8075]*. Now, when the data traffic with email

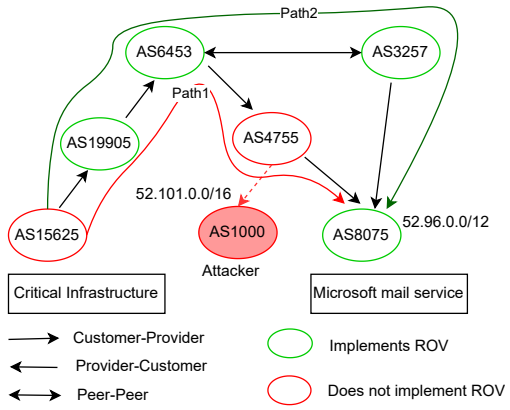


Figure 1: Collateral damage: Although only one AS (AS4755) does not implement ROV, Path1 is prone to prefix hijacking and is unsafe. So, it is crucial that all ASes on a path implement ROV.

messages from AS15625 is en route to Microsoft Mail's server IP (e.g., 52.101.73.6), AS6453 will likely forward traffic toward AS4755 rather than to AS3257. This is because AS4755 is a customer of AS6453 and AS6453's routing policies will usually prefer sending traffic to customers rather than to peers as carrying a customer's traffic has a monetary benefit for an AS. Since AS4755 does not implement ROV, it cannot distinguish the fake route (to AS1000) from the genuine one (to AS8075) and will likely forward the traffic to the attacker's network (AS1000) because the attacker is announcing a more specific prefix (/16) than the genuine one (/12). AS6453 could however choose the path through AS3257 (Path2) if it knew AS3257 was ROV-protected. This example shows that even if an AS deploys ROV, it can remain vulnerable to BGP hijacks, which is known as collateral damage [11, 20]. The solution is that all ASes on its path implement ROV.

3 RELATED WORK

We report on related work on finding paths and their security status.

Path finding. Most of the studies on path-finding such as [7, 21, 22, 24, 34] focus on the quality of service (QoS) like packet loss, latency, and the shortest path. For example, the methods from Li et al. [21, 22] have some similarities to our path finding method as they also use AS paths of the BGP RIBs data collected by the route collectors. Their goal was to display the best path in terms of QoS parameters, whereas we look to find the security status of the paths. Their approach might result in a large number of unnecessary paths that take longer to process because they also consider multiple origin ASes (MOAs). However, for our case study, we focus on the Microsoft-originated prefix that is used for mail servers and is not a MOA. Similarly, [27] finds AS paths that are the shortest and conform with AS relationships in an AS graph obtained from BGP tables at multiple vantage points. They developed a method to infer AS relationships and find paths in the "wild" without a clear application goal of their path inferring method and without considering any particular ASes as source and destination. This is unlike our study, in which we focus on finding paths and the ROV status of paths from a specific source to a destination AS. Also, our method is based on CAIDA's AS relationship data which is widely used in related research. Tao et al. [34] provide a theoretical basis for stitching paths from multiple AS paths. If there is more than one stitched path, they consider only the shortest one. Unlike them, our method considers all the paths. Cunha et al. [7] propose a system, called Sibyl which infers different levels of Internet paths using active measurement from probes around the globe, but their method is constrained by the number of probes.

Finding the security status of paths. Alizadeh and Oprea analyze the dependency of Dutch CIs on foreign registered ASes at the AS level [1]. They leverage the BGP routes originated by an ASN, ignoring valley-free conditions and not inferring paths from a source to a destination. Another study [14] detects the forged paths in an AS path whenever a new link appears. However, their method does not show the overall path security status from a source to a destination.

Our study thus differs from prior work in that we find the feasible paths based on passive measurement data (BGP data) and use this information to assess the ROV status of the paths.

4 METHODOLOGY

We devise a four-step methodology to identify potential paths from a source AS to a destination AS and assess the ROV of the identified paths: (i) path collecting, (ii) path stitching, (iii) path sanitizing, and (iv) security scoring.

4.1 Path collecting

We choose the public route collectors from the projects RIPE RIS and Route views to collect BGP routes from source ASes to destination ASes. Out of around 70 collectors located throughout the world, we chose the collectors based in the Netherlands: rrc00, rrc03, rrc25, and route-views.amsix. The reason is that when we perform traceroutes to Microsoft Mail using 300 different RIPE Atlas probes that are based in different locations within the Netherlands, we see Microsoft routers located in Amsterdam as the first hop of the Microsoft network (AS8075). As the source and destination are in the same geographic location and the study [31] shows

that route collectors are biased toward the location, it hints that the collectors located in the Netherlands capture most of the BGP data and meet our purpose of path-finding.

For a CI's AS, we look for all its BGP announcements while for Microsoft we look for BGP announcements with the prefix 52.96.0.0/12. In this way, we have two types of paths as seen from the route collectors: from the CI's AS to the route collectors and from Microsoft's AS to the route collectors. For example, Figure 2 is a real example showing the two paths towards the route collector 2: *6453 19905 15625* (Path1, CI originated for any prefix) and *6453 3257 8075* (Path2, Microsoft originated for prefix 52.96.0.0/12).

4.2 Path stitching

We create an undirected graph from the two types of paths which we obtain from path collecting step (see Section 4.1). The ASNs are the nodes in the graph and ASes on the AS path form the edges. For example, for path *6453 3257 8075* (path1 in Figure 2), we form a graph with corresponding ASNs and two edges *(8075, 3257), (3257, 6453)*. Similarly, for *6453 19905 15625* (path2), we create additional nodes in the original graph with corresponding ASNs and two edges *(15625, 19905), (19905, 6453)*.

The common node between the two paths is AS6453. This is a vantage point that dumps routing data to the route collectors and is a stitching point for us to join the two paths. In our example, we join the two paths *(8075, 3257), (3257, 6453)* and *6453 19905 15625* into *[15625 19905 6453 3257 8075]*. We use the "NetworkX" module of Python for forming this graph and the paths [13]. NetworkX uses a modified version of the depth-first search algorithm to find all the paths in the graph without repeating the nodes [30].

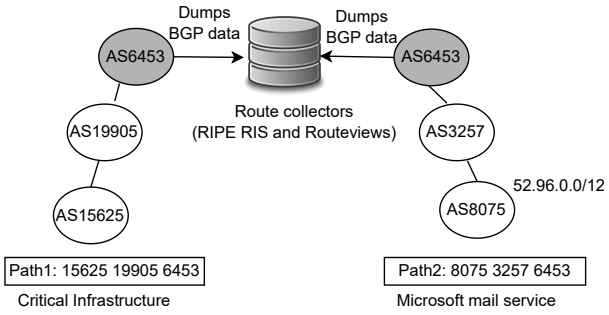


Figure 2: Path collecting and stitching: As AS6453 is a common AS in two paths (path1 and path2), it is a stitching node that stitches two paths two form a new path: *15625 19905 6453 3257 8075*.

4.3 Path sanitizing

For the existence of two-way paths from a source AS to a destination AS, the prefix originating from one of these ASes should be able to reach the other AS. Hence, a stitched AS path may not be a valid path without checking that condition. This condition is described as Gao Rexford's model for route export [10], which defines the following three rules:

(1) Routes learned from customers are exported to any providers or peers.
(2) Routes learned from providers are exported only to customers.
(3) Routes learned from peers are exported only to customers.

For example, a provider AS charges its customer AS for forwarding the customer's BGP routes. So, a provider AS forwards customer routes to all its BGP peers.

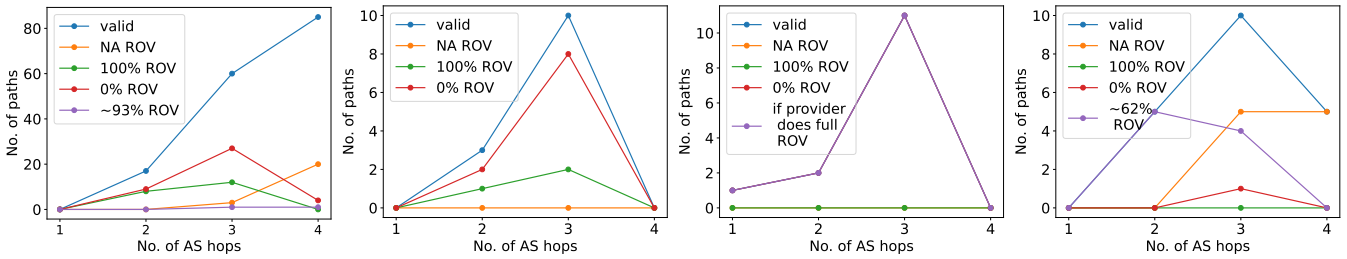
Underpinning the above-mentioned rules is a concept called "valley-free routing", proposed by Gao [9]. This concept states that an AS path cannot traverse a customer-to-provider or peer-to-peer edge after traversing a provider-to-customer or peer-to-peer edge. If all the ASes set their route export policy accordingly, then the AS path in any BGP routing table entry is valley-free. Hence as a first step of path sanitization step, we check the relationship between ASes on the stitched path using CAIDA AS Rank API [2] which considers the following three types of relationships between two ASes: Customer to Provider (C2P), Provider to Customer (P2C), and Peer to Peer (P2P). Then the second step of path sanitization is to check if the following three conditions hold for valley-free routing in the stitched paths:

(1) At most one P2P link exists in the path;
(2) A P2C link must not be followed by a C2P or P2P link;
(3) A P2P link must not be followed by C2P link.

We consider a path to be valid if it meets the above valley-free conditions. In the example of Figure 2, the relationships between the ASes of the newly formed stitched path *[15625 19905 6453 3257 8075]* are [C2P, C2P, P2P, P2C], as determined by CAIDA's AS rank. This path satisfies the valley-free condition and is therefore valid.

4.4 Security scoring

The final step is security scoring. For this purpose, we get the ROV scores of ASes on valid paths from the ROVista API [20]. Our ROV values are based those of 14 March 2024 because ROVista conducts active scans daily, resulting in slight fluctuations in the ROV score over time. The main reason for choosing ROVista is that it determines the score based on the number of RPKI-invalid prefixes reachable by an AS, which is a data plane-based measurement. The ROV score varies from 0% to 100%. A higher ROV score suggests that



(a) AS15625 (ING bank). (b) AS56517 (Vitens). (c) AS40985 (Eneco energy). (d) AS15916 (ABN-Amro Bank).

Figure 3: Number of paths for different numbers of AS hops between the four CIs and Microsoft mail service.

the AS filters more RPKI-invalid prefixes. So, implementing ROV fully by an AS means that AS has ROV score of 100%. While there might be multiple ways of computing the ROV status of a path, we choose the following simplified approach for computing the ROV score of a path in our study:

(1) Determine the ROV scores of each AS on an AS path;
(2) If an AS on the path has an ROV score of zero, the ROV of the whole path is zero;
(3) If an AS on the path has an ROV score of "NA", then the ROV score of the path is "NA".
(4) Otherwise, the ROV score is the lowest ROV scores of the ASes on the path.

5 CASE STUDY IN THE NETHERLANDS

We use our method [1] of path finding and identifying the ROV status of the paths to answer our two research questions.

Critical infrastructures. We selected four CI companies in the Netherlands for our case study: two banks (AS15625 and AS15916), a drinking water supplier (AS56517), and an energy company (AS40985). We choose these companies based on the following two criteria: (i) the company owns an ASN and IP prefixes, and (ii) it uses Microsoft for its mail service.

We determine mail providers of the four companies using the approach developed by Liu et al. [23], in which they map domain names to mail service providers using data from MX records, Banner/EHLO messages, and TLS certificates. We look for the IP addresses shown in those domains' MX records. Next, we find the corresponding matching prefix originated by Microsoft by examining the BGP updates data collected by route collectors of RouteViews and RIPE RIS. We find that the prefix of Microsoft Mail is 52.96.0.0/12 and Microsoft's AS (AS8075) originates it. So, for our case study, a source AS is an AS of one of the four CIs, and the destination AS is AS8075.

Analysis of ROV-protected paths. We find that the total number of paths from the four CIs (AS15625, AS56517, AS40985, and AS15916) to AS8075 is 8192, 202, 236, and 201 at a maximum distance of 4 AS hops away, respectively. AS15625 has the highest number of paths which might be because it is a multi-homed AS with four providers according to the CAIDA AS rank. More providers means more ways that an AS gets BGP routes.

Figure 3 shows the breakdown into the number of valid paths, fully ROV-protected paths (100% ROV), ROV-unprotected paths (0% ROV), and ROV status unknown paths (NA ROV). We find that AS15625 and AS56517 have 12 and 2 fully ROV-protected paths respectively at an AS path length of 3 hops; 8 and 1 paths at an AS path length of 2 hops, but do not have any 100% ROV paths when the AS path is more than 3 hops long. For AS15625, we find two valid paths having an ROV score of 92.85%, one of which is 2 hops away and the other is 3 hops away from the source. Also, there exists a greater number of ROV-unprotected (40) paths compared to fully ROV-protected paths (20) in total for a maximum path length of 3 AS hops. For the case of AS56517, there exist 10 ROV-unprotected paths and 3 ROV-protected paths for a maximum path length of 3 AS hops. This shows that there is quite a significant number of paths that are prone to BGP prefix hijacking, which is a risk for the CI's mail traffic as it might take these paths toward their mail server at Microsoft.

Increasing the number of ROV-protected paths. We find two CIs (AS40985 and AS15916) that do not have any paths with 100% ROV. This is because AS40985 has only one upstream provider through which it connects to the Internet and that provider does not implement ROV. However, all other ASes that are on the valid paths from AS40985 have a 100% ROV score. So, if AS40985's provider would implement ROV, then AS40985 would have all of its 14 valid paths ROV-protected instead of 0, as shown in Figure 3c. It means the ROV-percentage of the ROV-protected path will increase by 100%.

Similarly, AS15916 has two upstream providers: one with the ROV score "NA" (upstream 1) and the other has an ROV score of around 62% (upstream 2). As we take the lowest ROV scores of ASes on a path, we see 5 paths with ROV score

[1] https://github.com/shyamkkhadka/anrw_path_security_insights.

61.54% that are 2 hops away (through upstream 2) and 4 other paths with ROV score 61.54% that are 3 hops away from the source (through upstream 2). As all the other ASes on those paths have a 100% ROV score, having a 100% ROV score for upstream 2 will result in 9 fully ROV-protected paths out of 20 valid paths. So, the percentage of fully ROV-protected paths will increase by 45%.

The above results of those two CIs (AS40985 and AS15916) show that implementing ROV by their upstream providers increases the number of additional ROV-protected paths: 14 and 9 respectively, which is an increment by 72.5% on average for both the CIs.

6 DISCUSSION AND LIMITATIONS

Our path-finding method and analysis show that some CIs have fully ROV-protected paths to their email provider (Microsoft), but that the number of such paths depends on the CI as well as the AS path length. In addition, the number of fully ROV-protected paths will also likely change over time as a result of route changes. Such a longitudinal analysis is part of our future work.

With CIs having more insight into the ROV security of their network paths, the next question is how a CI can have more fully ROV-protected paths. One possibility is that CIs convince their immediate upstream ASes to implement ROV fully that would result in a significant increase in the number of fully ROV-protected paths. We provided a first indication in Figure 3c, which shows that if the upstream provider of the CI (AS40985) implements ROV, all 14 valid paths that the CI has at its disposal will be fully ROV-protected. Similarly, AS15916 will have 9 fully ROV-protected paths if its upstream provider implements ROV fully as shown in Figure 3d. We will be studying this topic further, for instance, to develop a measurement-based metric that indicates which ASes would have to implement ROV to be most effective.

Table 1: CIs and the unique ASes that are on their valid paths to Microsoft mail having 100% ROV scores

CI ASN	No. of unique ASes	No. of valid paths
15625	15	85
56517	10	13
40985	12	14
15916	13	15

Another approach of having more fully ROV-protected paths for CIs might be that ASes that support ROV form a group and agree to prefer forwarding traffic amongst each other, which is similar to a Trust Zone [5]. We look for unique ASes that are on valid paths and have 100% ROV scores for 4 CIs. As an example of AS15625, Table 1 shows that there exist 15 unique ASes having 100% ROV scores on 85 different valid paths. If these 15 ASes form a Trust zone to forward CIs traffic, the number of ROV-protected paths will increase. However, the number of such paths depends on their agreement of forwarding traffic among them.

In the future, ASes could also offer such concepts as a value-added service to their customers along with visualizations to provide easy insight into paths.

Two limitations of our study are as follows.

(i) For path construction: our method is based on the BGP data from route collectors, which cannot capture all BGP routes due to their non-uniform deployment [32]. Another limitation in path construction is using the AS_PATH attribute of BGP announcements as seen by the route collectors, which could be manipulated. Moreover, our reliance on the valley-free condition for inferring paths aligns with a widely accepted norm on the Internet. However, there are still cases where AS relationships are not valley-free [12]. Finally, some relationships are not captured by the CAIDA AS relationship dataset [29], which means that we cannot infer for all paths whether they are valid or not.

(ii) For ROV calculation: we rely on the ROV score from [20], which currently covers only around 30k ASes. Therefore, there are many ASes whose scores are "NA".

7 CONCLUSIONS AND FUTURE WORK

We have presented a method to find possible paths from an AS to its destination and used it to compute the ROV security status of the overall path based on the ROV status of individual ASes. Although we use our method to find paths from CIs to Microsoft Mail in the Netherlands, it can be used to assess the ROV security of paths from any source AS to any destination AS with or without a particular destination IP prefix. Our case study based on CIs in the Netherlands shows that there are multiple paths that are 100% ROV-protected and multiple others without ROV protection, which might introduce security risks for CI operators. However, our analysis also reveals that implementing ROV fully by upstream providers of CIs will increase the number of fully ROV-protected paths toward the Microsoft mail service by 72.5% on average.

Our future work includes calculating a path's security status based on security metrics other than ROV (e.g., DDoS protection) , which AS operators could take into account during decisions in inter-domain routing, and investigating the effects on path-finding using additional geographically diverse route collectors.

ACKNOWLEDGMENTS

This work was conducted as part of the projects CATRIN (www.catrin.nl) and UPIN (www.upin-project.nl), which received funding from the Dutch Research Council (NWO).

REFERENCES

[1] Fahimeh Alizadeh and Razvan C. Oprea. 2013. Discovery and Mapping of the Dutch National Critical IP Infrastructure. Retrieved March 27, 2024 from https://www.nlnetlabs.nl/downloads/publications/RP2_report_Mapping_the_Dutch_Critical_Infrastructure.pdf

[2] asrank 2024. AS Rank. https://doi.org/10.21986/CAIDA.DATA.AS-RANK

[3] Clingendael Policy Brief. 2024. Too late to act? Europe's quest for cloud sovereignty. https://doi.org/10.21986/CAIDA.DATA.AS-RANK

[4] Randy Bush. 2014. *Origin validation operation based on the Resource Public Key Infrastructure (RPKI).* Technical Report.

[5] David Clark and KC Claffy. 2021. Trust zones: A path to a more secure internet infrastructure. *Journal of Information Policy* 11 (2021), 26–62.

[6] European Commission. 2004. Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism. *Com* (2004), 702.

[7] Ítalo Cunha, Pietro Marchetta, Matt Calder, Yi-Ching Chiu, Bruno VA Machado, Antonio Pescapè, Vasileios Giotsas, Harsha V Madhyastha, and Ethan Katz-Bassett. 2016. Sibyl: a practical Internet route oracle. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. 325–344.

[8] National Coordinator for Security, Counterterrorism. Ministry of Security, and Justice. 2024. Critical Infrastructure (protection) | National Coordinator for Security and Counterterrorism. Retrieved March 28, 2024 from https://english.nctv.nl/topics/critical-infrastructure-protection

[9] Lixin Gao. 2001. On inferring autonomous system relationships in the Internet. *IEEE/ACM Transactions on networking* 9, 6 (2001), 733–745.

[10] Lixin Gao and Jennifer Rexford. 2001. Stable Internet routing without global coordination. *IEEE/ACM Transactions on networking* 9, 6 (2001), 681–692.

[11] Yossi Gilad, Avichai Cohen, Amir Herzberg, Michael Schapira, and Haya Shulman. 2016. Are we there yet? On RPKI's deployment and security. *Cryptology ePrint Archive* (2016).

[12] Vasileios Giotsas and Shi Zhou. 2012. Valley-free violation in Internet routing — Analysis based on BGP Community data. In *2012 IEEE International Conference on Communications (ICC)*. 1193–1197. https://doi.org/10.1109/ICC.2012.6363987

[13] Aric A. Hagberg, Daniel A. Schult, and Pieter J. Swart. 2008. Exploring Network Structure, Dynamics, and Function using NetworkX. In *Proceedings of the 7th Python in Science Conference*, Gaël Varoquaux, Travis Vaught, and Jarrod Millman (Eds.). Pasadena, CA USA, 11 – 15.

[14] Thomas Holterbach, Thomas Alfroy, Amreesh D. Phokeer, Alberto Dainotti, and Cristel Pelsser. 2024. A System to Detect Forged-Origin Hijacks. In *21th USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*. USENIX Association.

[15] Savvas Kastanakis, Vasileios Giotsas, Ioana Livadariu, and Neeraj Suri. 2023. Replication: 20 Years of Inferring Interdomain Routing Policies. In *Proceedings of the 2023 ACM on Internet Measurement Conference*. 16–29.

[16] Brian Krebs. 2020. Not just another BGP Hijack. Retrieved March 29, 2024 from https://manrs.org/2020/04/not-just-another-bgp-hijack/

[17] Brian Krebs. 2022. DDoS Mitigation Firm Has History of Hijacks. Retrieved March 29, 2024 from https://krebsonsecurity.com/2016/09/ddos-mitigation-firm-has-history-of-hijacks/

[18] Matt Lepinski and Stephen Kent. 2012. *An infrastructure to support secure internet routing.* Technical Report.

[19] Matt Lepinski, Stephen Kent, and Derrick Kong. 2012. *A profile for route origin authorizations (ROAs).* Technical Report.

[20] Weitong Li, Zhexiao Lin, Md Ishtiaq Ashiq, Emile Aben, Romain Fontugne, Amreesh Phokeer, and Taejoong Chung. 2023. RoVista: Measuring and analyzing the route origin validation (ROV) in RPKI. In *Proceedings of the 2023 ACM on Internet Measurement Conference*. 73–88.

[21] Xionglve Li, Zhiping Cai, Bingnan Hou, Ning Liu, Fang Liu, and Jieren Cheng. 2020. ProbInfer: Probability-based AS path inference from multigraph perspective. *Computer Networks* 180 (2020), 107377. https://doi.org/10.1016/j.comnet.2020.107377

[22] Xionglve Li, Tongqing Zhou, Zhiping Cai, and Jinshu Su. 2023. Realizing Fine-Grained Inference of AS Path With a Generative Measurable Process. *IEEE/ACM Transactions on Networking* 31, 6 (2023), 3112–3127. https://doi.org/10.1109/TNET.2023.3270565

[23] Enze Liu, Gautam Akiwate, Mattijs Jonker, Ariana Mirian, Stefan Savage, and Geoffrey M. Voelker. 2021. Who's Got Your Mail? Characterizing Mail Service Provider Usage. In *ACM Internet Measurement Conference (IMC'21)*. ACM, Virtual Event.

[24] Harsha V Madhyastha, Tomas Isdal, Michael Piatek, Colin Dixon, Thomas Anderson, Arvind Krishnamurthy, and Arun Venkataramani. 2006. iPlane: An information plane for distributed services. In *Proceedings of the 7th symposium on Operating systems design and implementation*. 367–380.

[25] Doug Madory. 2018. Recent Routing Incidents: Using BGP to Hijack DNS and more. Retrieved March 29, 2024 from https://www.lacnic.net/innovaportal/file/3207/1/dougmadory_lacnic_30_rosario.pdf

[26] Doug Madory. 2022. What can be learned from recent BGP hijacks targeting cryptocurrency services? Retrieved March 29, 2024 from https://www.kentik.com/blog/bgp-hijacks-targeting-cryptocurrency-services/

[27] Z Morley Mao, Lili Qiu, Jia Wang, and Yin Zhang. 2005. On AS-level path inference. In *Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*. 339–349.

[28] NOS. 2024. The US government can access emails from Dutch governments and critical companies. Retrieved March 28, 2024 from https://nos.nl/artikel/2510923-amerikaanse-overheid-kan-bij-e-mail-van-nederlandse-overheden-en-kritieke-bedrijven

[29] Lars Prehn and Anja Feldmann. 2021. How biased is our validation (data) for as relationships?. In *Proceedings of the 21st ACM Internet Measurement Conference*. 612–620.

[30] Robert Sedgewick. 2001. *Algorithms in c, part 5: graph algorithms, third edition* (third ed.). Addison-Wesley Professional.

[31] Pavlos Sermpezis, Lars Prehn, Sofia Kostoglou, Marcel Flores, Athena Vakali, and Emile Aben. 2023. Bias in Internet Measurement Platforms. In *2023 7th Network Traffic Measurement and Analysis Conference (TMA)*. 1–10. https://doi.org/10.23919/TMA58422.2023.10198985

[32] Pavlos Sermpezis, Lars Prehn, Sofia Kostoglou, Marcel Flores, Athena Vakali, and Emile Aben. 2023. Bias in Internet Measurement Platforms. In *2023 7th Network Traffic Measurement and Analysis Conference (TMA)*. IEEE, 1–10.

[33] Raffaele Sommese, Mattijs Jonker, Jeroen van der Ham, and Giovane C. M. Moura. 2022. Assessing e-Government DNS Resilience. In *2022 18th International Conference on Network and Service Management (CNSM)*. 118–126. https://doi.org/10.23919/CNSM55787.2022.9965155

[34] Narisu Tao, Xu Chen, and Xiaoming Fu. 2015. As path inference: From complex network perspective. In *2015 IFIP Networking Conference (IFIP Networking)*. IEEE, 1–9.

[35] Feng Wang and Lixin Gao. 2003. On inferring and characterizing Internet routing policies. In *Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement*. 15–26.