Measuring BGP Route Origin Registration and Validation

Daniele Iamartino[1,2], Cristel Pelsser[1] and Randy Bush[1]

[1] Internet Initiative Japan, Japan
[2] Politecnico di Milano, Italy

Abstract. BGP, the de-facto inter-domain routing protocol, was designed without considering security. Recently, network operators have experienced hijacks of their network prefixes, often due to BGP misconfiguration by other operators, sometimes maliciously. In order to address this, prefix origin validation, based on a RPKI infrastructure, was proposed and developed. Today, many organizations are registering their data in the RPKI to protect their prefixes from accidental mis-origination. However, some organizations submit incorrect information to the RPKI repositories or announce prefixes that do not exactly match what they registered. Also, the RPKI repositories of Internet registries are not operationally reliable. The aim of this work is to reveal these problems via measurement. We show how important they are, try to understand the main causes of errors, and explore possible solutions. In this longitudinal study, we see the impact of a policy which discards route announcements with invalid origins would have on the routing table, and to a lesser extent on the traffic at the edge of a large research network.

1 Introduction

Mis-originations, an Autonomous System (AS) announcing an IP prefix to which it has no rights, regularly appear in the Internet. Sometimes they arise from BGP misconfigurations. They may also result from malice. A notorious prefix mis-origination was the "YouTube incident" [9] where Pakistan Telecom advertised one of YouTube's IPv4 prefixes. The original intent was to censor traffic from Pakistan destined to YouTube. However, when PT "'leaked" the prefix to the world, the event had a much larger impact than desired; traffic destined YouTube was blackholed at global scale. A more recent example is the "Indosat event" [17, 19]. In April 2014, Indosat originated 417,038 prefixes normally announced by other ASs. This is believed likely due to a mis-configuration, a maintenance event gone bad [17]. In August 2014, a bitcoin miner [16] was attacked with the goal of diverting the traffic from the miners to relay the result of their computation and divert the monetary benefit of their work. The attack on bitcoin miners was malicious. This last example shows the limitations of route origin validation. Attackers will find another way to perform the attack if route origin validation is widely deployed.

In the current taxonomy, there are three pieces to improving BGP security, the RPKI, RPKI-based origin validation, and in the future path validation. In this paper, we focus on RPKI and RPKI-origin validation.

The RPKI is an X.509 based hierarchy congruent with the Internet IP address allocation administration, the IANA on top, then Regional Internet Registries (RIRs), and ISPs, ... It is the substrate on which origin and path validation are based. It is currently deployed by all five RIRs, AfriNIC, APNIC, ARIN, LACNIC, and RIPE.

RPKI-based origin validation uses RPKI data to allow routers to verify that the AS originating an IP prefix is in fact authorized to do so. This is not crypto checked, as a BGP update message does not carry signatures, so can be violated. But it should prevent the vast majority of accidental 'hijackings' on the Internet today, e.g. the Pakistani accidental announcement of YouTube's address space. RPKI-based origin validation is in shipping code from Cisco and Juniper, and others soon.

A Route Origination Authorization (ROA) is an RPKI object which verifiably asserts that a specified AS is authorized to originate BGP announcements for a given set of prefixes [15]. A ROA is composed of an AS number, a list of IP prefixes, and for each prefix, a maximum length. The maximum length is a macro to authorize the AS to advertise more specific prefixes than the original prefix, up to the length as specified.

It is important to understand the status of deployment of route origin validation. For this purpose, we have been collecting data from the RPKI infrastructure since April 2012. Here we analyse these data to show the scale of deployment of ROA registrations. We find that registration is significantly deployed in Europe and Latin America, but is extremely poorly deployed in north America, Asia/pacific, and Africa. We illustrate some of the events that occurred while publishing entities, the RIRs, learned to operate the RPKI system. There were serious problems regarding reliability of the RIR's RPKI infrastructure. Overall, it varied from bad to acceptable.

The incentive for operators to register ROAs is high, as it protects their resources. In order for this to be effective other operators need to deploy route origin validation in their ASs. That is, their routers need to check the validity of each route's origin. The drive to do this is multifold. It protects one's customer traffic from following a bogus/malicious route and it protects one's infrastructure from accepting many more routes than usual from a given peer (this can lead to a session reset or the restart of the router). It will also become common good practice, on the same level as prefix filtering, in that the effect of misconfigurations are contained close to the source of the event instead of affecting the entire Internet infrastructure. The second part of our study focuses on the validation of routes based on the registered ROAs. We take the views from public BGP monitors [8], and study the evolution of route origin validity over a 2.5 year time period with the objective to show that mis-origination occurred and could have been detected. In addition, we are interested in mis-matches between information registered in the RPKI and advertised routes. We try to understand these as they may highlight misunderstanding of the technology by network operators or poor tools or controls at the publishers. Does the validity of a route depend on the location where the advertisement is received? We try to answer that question next by looking at the validity status of routes at multiple locations.

Among the invalid prefixes, 81% are covered by a valid prefix or a prefix not registered in the RPKI. A network operator strictly enforcing route-origin validation would not drop many prefixes. 54% of the invalid prefixes result from a mis-match between

the prefix length and the MaxLength in the ROAs. The other major issue results from ISPs not helping their multi-homed customers to register their sub-allocations.

Last, performing route origin validation means BGP routes selected by routers may change and thus can affect traffic forwarding. We try to understand the traffic impact by looking at the statistics of an operational router within an American research network. The router counts traffic forwarded by routes with valid, notfound, and invalid origin. This tells us the amount of traffic that would be dropped by the router should different BGP policies be adopted. It shows that if an operator was to configure its routers to strictly drop routes with invalid origin, the effect on the traffic would be negligible.

The paper is organized as follows. We describe our methodology and data sets in section 2. In section 3 we look first at the extent of RPKI ROAs publication across the different administrative regions. Second, we study the different causes of mismatch between route advertisements and RPKI registrations. Third, we present traffic statistics for each class of routes (valid origin, invalid, and unknown). We present some related work in section 4, and conclude in section 5.

2 Methodology

2.1 Validation Process

As we are analyzing historical data, to determine the validity of a BGP route advertisement at some point in time, the first step is to get all the published ROAs for a given time and build a radix tree. The radix tree will then be used to validate the route entries of subsequent BGP RIB dumps.

Each ROA file is composed of an AS number, multiple IP prefixes, and a maximum length for each prefix. For all X.509 validated ROA files, we extract tuples (ASN, Prefix, MaxLen, Expiration time). We insert these tuples as nodes of a radix tree where the key is the IP Prefix of the tuple. That is, each node of the radix tree is identified by the IP prefix that it is covering. Note that more than one ROA record might exist for a particular prefix. Consequently, each node may contain more than one ROA record.

After building the radix tree, we take the BGP RIB dump following the download of the ROAs from the RPKI infrastructure, and before the next download of ROAs. We validate the content in each RIB dump separately. Each dump gives us a view of the validity at a different point in time. For each announcement found in a RIB dump, we search for the longest prefix match in the radix tree. If no such node is found, we mark the announcement as ”ROA not found.” Then, for each ROA present in the node, we check if the max length of the node covers the announced prefix and if the AS number specified in the ROA record is equal to the origin AS number of the announcement. If these conditions are met, the ROA validates the route announced for the prefix. If no validating ROA is found in the given node, we traverse upward to shorter prefixes until we either find a validating ROA or there is no parent node. If we moved upward in the tree and never found a matching ROA, the route is marked as invalid, else its origin AS is deemed valid.

In a RIB dump, there may be multiple announcements for a single prefix, as a monitor may learn the same prefix from different BGP peers. We validate each announcement separately.

2.2 Datasets

This study relies on a number of datasets: (1) the download of ROAs from the RPKI infrastructure every hour from March 2012 to August 2014, (2) BGP RIB dumps from RouteViews [8] for the same period. RouteViews RIB dumps are available every two hours, and (3) the marked statistics taken from a live router in a research network. We perform most validation on the LINX RIB dumps. To determine the sensitivity of route origin validity at different locations we also consider the ISC, Sao Paulo, Sidney, and WIDE RouteViews monitors.

Regarding the first dataset, as the IANA has not been allowed to provide an RPKI root, we chose trust anchors following the recommendation of the IETF SIDR working group [15], using the rcynic tool [7] to download ROAs from the RIPE, LACNIC, AfriNIC, APNIC and CA0 trust anchors, with two exceptions; for legal reasons, we only have ARIN data starting from August 2014 and we add the CA0 data. ARIN has a policy of providing access to the data only to those who have signed a document. CA0 is the trust anchor for some legacy and experimental address space that ARIN will not register.

As ROAs can not cover AS-SETs, we excluded from our study the minuscule portion of BGP announcements which have an AS-SET for the origin AS.

When we validate the origins of advertisements in a RIB dump, we take the ROAs gathered during the rcynic run prior but closest in time to the time-stamp of the RIB dump.

3 Results

3.1 RPKI Deployment

First we look at the extent of RPKI registration deployment. Table 1 shows the number of IPv4 host addresses (/32s) covered by ROAs by each RIR publication point. The 3rd column shows the total number of IPv4 addresses delegated by each RIR. We observe that while ARIN has allocated most of the address space, it lags far behind the other Northern RIRs in registrations, giving many North Americans a distorted view of RPKI deployment. The same is true for APNIC. RIPE NCC is currently the leader in terms of both absolute and relative amount of allocated address space covered by ROAs, and LACNIC is quite active.

In figure 1 we can see, for each RIR, the number of ROAs authenticated by rcynic between March 2012 and September 2014. There is a one-month hole between July and August 2013 due to a problem in our data collection. We only started collecting ARIN's data in August 2014, due to ARIN's legal barriers placed on RPKI use. We see LACNIC data being interrupted from the end of December 2012 to mid August 2013; we believe the reason for this is X.509 expiration of their trust anchor. That this went undetected is operationally quite disturbing. Also the APNIC repository had a similar event for seven months between January and August 2013. Between November 2012 and February 2013 we can see the effects of key roll-over on the RIPE data. We started to collect CA0 data on August 2013. We observe regular drops in the number of ROAs for CA0 because this data is hosted on a machine that is regularly disconnected from

Publication point	Number of IPv4 addresses covered by a ROA	Number of IPv4 allocated	Percentage coverage
RIPE NCC	125,133,312	797,906,680	15.68%
ARIN	30,187,520	1,733,372,928	1.74%
LACNIC	19,089,408	189,833,472	10.05%
AfriNIC	2,814,464	119,534,080	2.35%
APNIC	744,960	872,194,816	0.08%
Total	177,969,664	3,712,841,976	4.79%

Table 1. Deployment status of the registration of IPv4 addresses on September 8, 2014 (data from [1]) compared to the allocation of IPs by these RIRs on the same day [2–6].

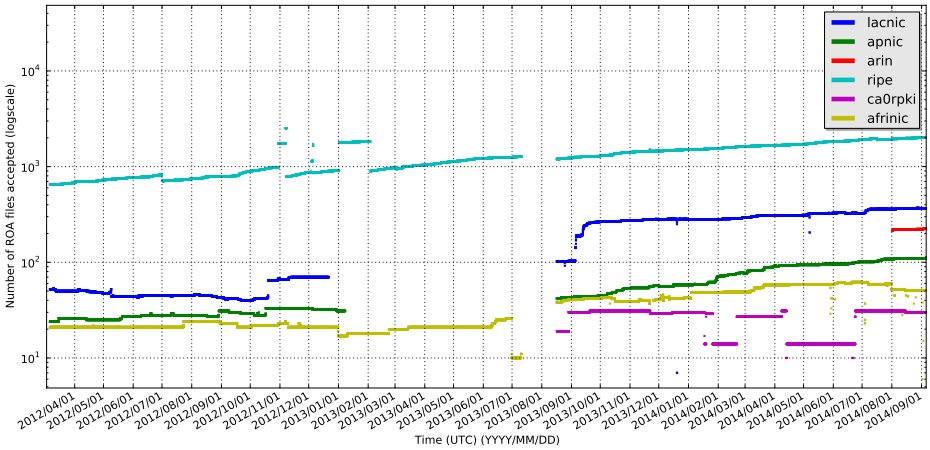

Fig. 1. Accepted (valid) ROA files below the six trust anchors. The discontinuous increases in number of ROAs observed for RIPE NCC occur during key rollovers. LACNIC and APNIC face a loss of valid ROAs for roughly seven months, likely due to an expiration of their X.509 certificate. There is a hole in our data, for all trust anchors between July and August 2013.

the Internet for extended periods of time giving time for objects to expire without being renewed on time.

3.2 Validity Status of Prefix Announcements Over Time

For this analysis we use a BGP RIB dump taken every 30 days on the LINX monitor of Route-Views. In a RIB dump we usually find several announcements for the same prefix received from different BGP peers. For origin-validation purposes, each announcement is identified by: its time-stamp, the prefix announced, and the origin AS (the right-most AS on the AS_PATH). Note that in the case of a RIB dump file, the time-stamp is always equal to the global time-stamp of the RIB dump. We validate each announcement as described in Section 2.1. In a given RIB dump, we might have several announcements with different origin AS for the same prefix. Consequently, we classify every prefix in one of the following groups:

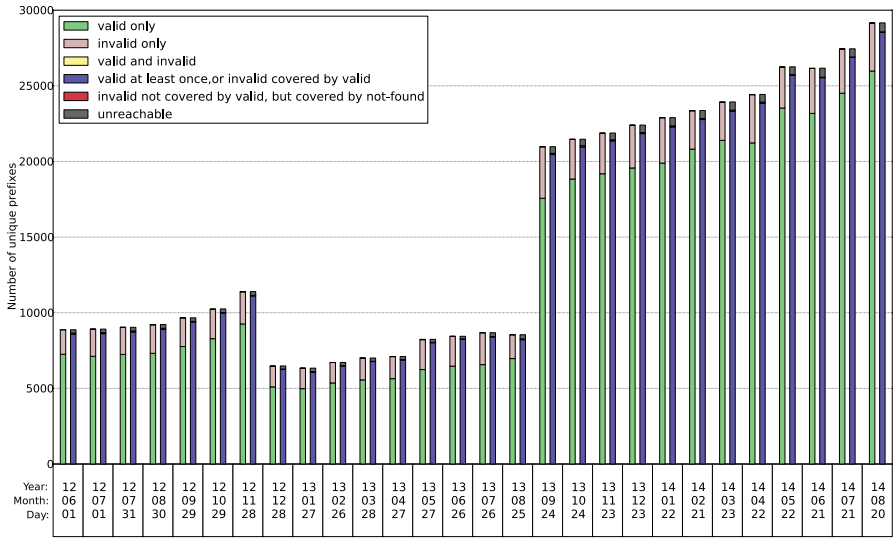

Fig. 2. Validity status of routes seen by route-views LINX monitor between June 2012 and September 2014. The first (green, pink and yellow) bar shows the status of prefixes independently from the existence of covering prefixes. The second bar (blue, red and grey) illustrates the reachability of a prefix considering that an invalid prefix might be covered by another valid or "ROA not found" prefix.

- **Valid only**: All announcements observed for this prefix are valid.
- **Invalid only**: All announcements observed this prefix are invalid.
- **Valid and invalid**: We found both valid and invalid announcements for the prefix. That is, some announcements have a different origin ASs.
- **ROA not found**: There is no ROA covering this prefix.

As seen in Section 3.1, only 4.79% of IP addresses are covered by ROAs. This means that a lot of prefix advertisements will fall in the "ROA not found" category. For readability, we do not show this case in the following figures. When we look at the validity of the advertisements using the above taxonomy (left-side bars of figure 2) we can first see a very significant decrease of prefixes being validated between December 2012 and August 2013. This is due to the problem in the LACNIC repository mentioned in section 3.1. Almost all ROA files of the LACNIC repository disappeared. Thus, all the prefixes which were previously covered by these ROAs are labelled "ROA not found.".

To validate the last RIB dump (August 2014), we added ARIN ROAs. This is not the case for the other months, as we had not captured those data (see Section 3.1). For this reason, some prefixes which were "ROA not found" become covered by an ARIN ROA, leading to a slight increase of the total coverage of prefixes to a final value of 5.41% on August 2014 (see last line, 6th column of table 2).

Date	Total prefixes seen	Valid prefixes	Invalid prefixes	Valid and invalid prefixes	Percentage of RPKI-covered prefixes	Reachable prefixes	Unreachable prefixes	Percentage of invalid covered
2012/06/01	432,516	7,253	1,621	0	2.05%	8,648	226	86.05%
2012/11/28	454,601	9,258	2,123	13	2.50%	11,149	245	88.45%
2012/12/28	458,955	5,097	1,368	16	1.41%	6,276	205	85.01%
2013/09/24	504,733	17,567	3,400	8	4.15%	20,537	438	87.11%
2014/05/22	525,241	23,531	2,693	31	4.99%	25,731	525	80.50%
2014/07/21	534,519	24,511	2,916	18	5.13%	26,904	541	81.44%
2014/08/20	538,926	25,973	3,168	17	5.41%	28,565	593	81.28%

Table 2. A few data points to compare valid and invalid prefixes to the reachability of these prefixes should the LINX monitor drop invalid prefixes. Most invalid prefixes are still reachable because of the existence of a covering prefix that is either marked as "valid" or "ROA not found".

Prefixes tagged both "valid and invalid" are very rare. In some dumps they are not present at all. We observed a peak of 31 on 2014/05/22. We believe that these could be due to either an anycast prefix with ROAs missing for some of the potential origin AS, a misconfiguration (some origins are private AS numbers that in theory should not be leaked to the route-views monitor), or an attack. We saw that, for several of these, the failing AS and the valid AS have very similar AS names, hinting that these are likely not attacks.

Table 2 shows some of the data points of Figure 2. Column 3-5 correspond to the elements of the first bar for some times on the x-axis in the figure. We can further deduce the amount of 'ROA not found' prefixes by looking at column 6. In June 2012, 97.95% of the prefixes were not covered by any ROAs. This decreases to 94.59% in August 2014.

3.3 Taking Coverage into Account

It is often assumed that operators who validate advertisements will drop invalids. In order to better understand the effect of that policy on reachability, we cannot simply look at prefixes separately. We need to consider the coverage of invalids by other prefixes. Let's assume that a BGP border router receives the same routes as our LINX monitor. It drops all "invalid only" prefixes. In addition, in the deployment phase, we expect operators to also accept announcements for prefixes with no ROA. If a prefix is "valid" or "valid and invalid", we consider it as reachable, because it means that at least one valid announcement for that prefix was present. When a prefix is marked "invalid only", there are some cases when it could be reached:

- The invalid prefix is **up-covered by another valid** prefix (Example: announcement of 10.1.2.0/24 is invalid, but 10.1.0.0/16 is also announced and valid, so the monitor can reach 10.1.2.0/24 anyway exploiting the covering valid announcement)
- The invalid prefix is **completely down-covered by other valid** prefixes (Example: announcement of 10.1.0.0/16 is invalid, but 10.1.0.0/17 and 10.1.128.0/17 are also announced and valid)

Monitor name	All prefixes seen	RPKI-covered reachable prefixes seen	RPKI-covered unreachable prefixes seen	Percentage of unreachable	Percentage of RPKI-covered prefixes
ISC	540,197	27,587	591	2.14%	5.21%
LINX	538,926	28,565	593	2.07%	5.41%
Sao Paulo	547,554	28,521	580	2.03%	5.31%
Sydney	538,378	28,741	596	2.07%	5.44%
WIDE	528,883	27,457	588	2.14%	5.30%

Table 3. Reachable and Unreachable prefixes from different route-views monitors on 20 August 2014

– The invalid prefix is **up-covered by a "ROA not found"** prefix (Example: announcement of 10.1.2.0/24 is invalid, but 10.1.0.0/16 is also announced and there is no covering ROA for the latter)

So we can finally say that a given prefix is **reachable** if it is "ROA not found", "valid only", "valid and invalid" or "invalid only" covered as in one of the three cases above. Instead, when a prefix is "invalid only" and there is no coverage by another valid or "ROA not found", we mark it as **unreachable**. The right-side bars of figure 2 show the reachability of prefixes considering coverage. Table 2 list of few of the key values in columns 7-9. We note that around 80% of invalid prefixes are in fact reachable. They are "rescued" by another valid or a "ROA not found" covering prefix.

3.4 The effect of monitors

Up to now we considered the data from the LINX monitor because it has a lot of peering links. This monitor is interesting because it receives a lot of heterogeneous announcements. Here we aim to see if our observations are highly dependent on that monitor. For that purpose, we consider 4 additional route-views collection points: **ISC** (Palo Alto CA, USA), **SAOPAULO** (Sao Paulo, Brazil), **SYDNEY** (Sydney, Australia), **WIDE** (Tokyo, Japan). The main difference between monitors is that they do not receive routes for the same amount of prefixes (see Table 3). However, the percentage of RPKI-covered prefixes seen is very similar. We think that in order to detect specific events, it might be better to combine the data from all monitors, but for the purpose of our measurements it's enough to consider one of the biggest. The percentage of unreachable prefixes due to an invalid origin is almost the same at any of the 5 locations considered.

3.5 The causes behind invalids

What are the reasons behind failed route origin validations? For every "invalid only" or "valid and invalid" prefix, we look at the reason why the ROA record(s) present in the longest-prefix matching node of the radix tree does not match the advertisement under validation. We analyze all invalid prefixes, discarding their potential coverage by other prefixes, contrary to Section 3.3. We divide the failed validations into three categories:

– **Invalid maximum prefix length:** For example, the monitor receives an announcement for 10.1.2.0/24 but the ROA record covers only 10.1.0.0/16-16.

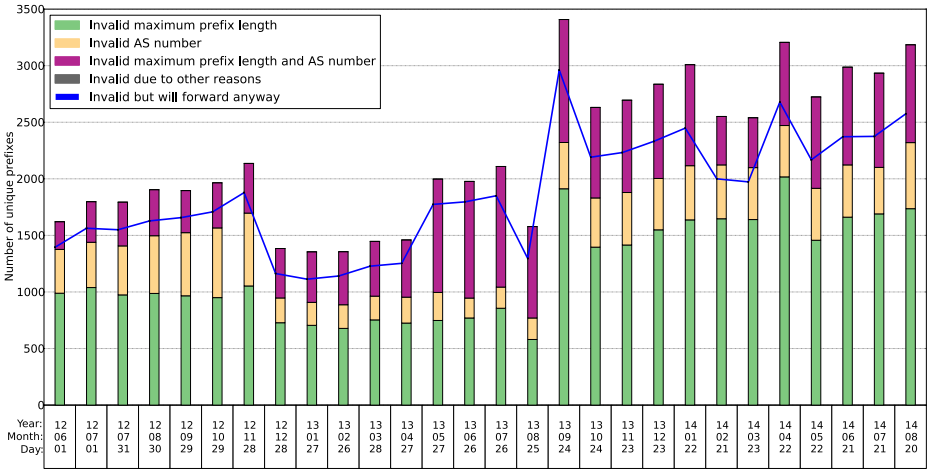

Fig. 3. Breakdown of invalid prefixes, by failing cause, as seen by LINX monitor

Date	Prefixes invalid due to MaxLength	Prefixes invalid due to wrong ASN	Prefixes invalid due to MaxLength and ASN
2012/06/01	989 (61.01%)	387 (23.87%)	245 (15.11%)
2012/11/28	1053 (49.30%)	644 (30.15%)	439 (20.55%)
2014/06/21	1661 (55.61%)	462 (15.47%)	864 (28.93%)
2014/07/21	1690 (57.60%)	411 (14.01%)	833 (28.39%)
2014/08/20	1736 (54.51%)	584 (18.34%)	865 (27.16%)

Table 4. Percentage of invalid prefixes, divided by failing reason: MaxLength/ASN/both. Data from LINX monitor of route-views project.

- **Invalid origin AS number:** The monitor receives an announcement by AS666 for 10.1.2.0/24 but the ROA record authorize 10.1.2.0/24 only from AS42.
- **Both maximum length and AS number:** At least two ROAs are found in the longest-prefix matching node for the prefix, one or more of them failing on AS number, the other(s) failing on MaxLength; or there is a single ROA failing for both reasons. This may cover a lot of different causes and we don't have enough information to classify them.

In figure 3 we can see that mismatched maximum length is the most widespread cause for invalids (see table 4 for some numbers relative to the figure). There are less invalids due to non-matching origin ASs.

We can further subdivide the class of "invalid origin AS number" and "both maximum length and AS number" errors by looking for the valid AS within the AS path. This indicates that the up-stream provider registered the covering prefix but did not do their job and create a ROA for their customer's sub-allocation. For example, the service provider (ISP) registers (prefix 10.0.0.0/16, AS42) and allocates 10.0.1.0/24 to its multi-homed customer AS666. The monitor receives the AS path 100 200 42 666. The

announcement of the customer is invalid because only AS42 is authorized by the ROA. However AS42 is present in the AS path. We took invalid prefixes of the last RIB dump of August 2014, and for each of them we check whether at least one of the announcements of that prefix contains a correct AS in the AS path. Results are that 57.36% of "invalid origin AS number" invalid prefixes and 83.23% of "both maximum length and AS number" invalid prefixes contains the correct AS on the AS path.

Summing the percentages, when we see an announcement coming from the wrong origin AS, in %72 of the cases we can find the correct AS in one of the AS paths of that prefix. As the customer (AS666 in the example) is multi-homed, there are likely one or more other AS Paths also starting from AS666 but not having the allocating up-stream in the path. However, the 54.51% percentage of MaxLength problems alone is still the overwhelming invalid cause, and could be easily fixed by submission of correct ROA records by organizations.

This study highlights the need for operators to monitor the status of their prefixes with regard to what is registered in the RPKI. In addition, customers should make sure that their provider registers the prefixes they have been allocated or should perform the registration themselves. Most invalids today are probably a result from operators learning a new technology and have not yet developed good procedures. By monitoring the validity of their prefixes they should be able to learn from their mistakes and fix them. RIRs and researchers could also publish these problems and notify those who should fix them,

3.6 Effect on Traffic in a Real Network

BGP announcement data can give us an idea about the deployment of origin-validation on the global Internet. However, most of the common traffic on the Internet is usually directed to just few destinations. For this reason, we gathered data about how many "RPKI-protected" packets/bytes are passing across a real router within a large research network. We say that a packet/byte is 'RPKI-protected', if the packet/byte was received from an IP address part of an RPKI-covered prefix or sent to such an IP destination. We observe in figure 4 that very little traffic is RPKI-covered, likely because this is an American research network whose prefixes ARIN will not certify. The embedded figure shows the percentages of bytes/packets with invalid source or destination that cross the router. Traffic from/to invalid origins is negligible in this case. This finding is consistent with [13] and [10].

4 Related Work

The closest works to ours are [13] and [10]. They provide snapshots of route validation in specific deployments. Here we go further as we study route validation over an extended period of time. In addition, we provide statistics regarding the RPKI infrastructure, and the registration of resources and events caused by the operation of the infrastructure.

In [18], Wählisch et al. aim to distinguish misconfiguration from intentional hijacks. For this purpose they rely on route origin validation. On the other hand, PHAS [14]

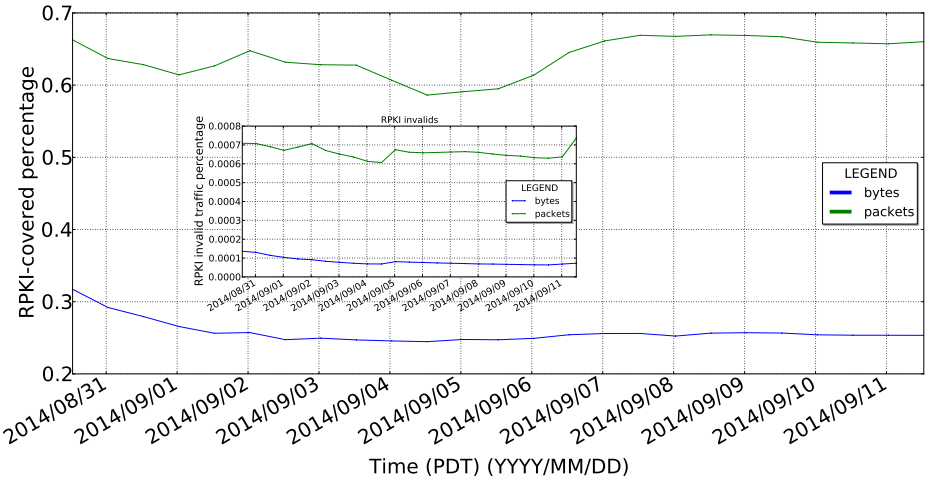

Fig. 4. Percentage of bytes or packets coming or going to an IP address of an RPKI-covered prefix

offers a real-time hijacking detection service. PHAS monitors the set of origin ASs observed in public data. It notifies operators that register to the system of changes in observed origin ASs. In the RPKI, publication points can remove resources from the distributed database with the adverse effect that advertisements from some prefixes may not be validated anymore. The work of Heilam *et al.* [12] aims to prevent publication points from removing resources from the system without the consent of the owner(s) of the resources. The objective of [11] is to measure the effect of attacks on the traffic. The authors observe that even with secure routing mechanisms, it is possible to attract a large amount of traffic by advertising routes along valid paths but infringing the BGP policies for targeted prefixes.

5 Conclusion

In this paper, we studied the extend of RPKI deployment. We observed that Europe and Latin America are leading today, with many ROAs registered. Regarding the RIRs RPKI infrastructure, there were serious problems. The entire dataset became unavailable for extended periods of time for a couple of RIRs. We then quantified the state of origin-validation deployment. It is about 5%, and increasing. Among the invalid BGP announcements, the number of invalid prefixes due to the MaxLength error alone are the majority, and they could be easily fixed by just correct ROA submissions. We also discovered that many invalid prefixes are due to coverage by a ROA of a service provider. This shows that organizations that are still not planning to deploy RPKI should care about what their service provider is doing.

While we found several invalid BGP announcements of prefixes, most of them are "rescued" by another valid or "ROA not found" covering prefix. This means that, today, filtering invalid prefixes could leave few unreachable prefixes, but not as many as one would think. When looking at the actual effect on the traffic crossing a router, we find

that dropping invalids leads to negligible amount of traffic being dropped, and hence is safe to do.

Acknowledgments

We thank the operator of the large American research network for setting up the collection of the traffic statistics. Rob Austein was a great help toward understanding the mechanics of the RPKI infrastructure and the different events we observed.

References

1. IPv4 Address Space in ROAs (/24s), http://certification-stats.ripe.net/?type=roa-v4
2. IPv4 Prefixes Delegated by AfriNIC, ftp://ftp.afrinic.net/stats/afrinic/delegated-afrinic-extended-latest
3. IPv4 Prefixes Delegated by APNIC, ftp://ftp.apnic.net/pub/apnic/stats/apnic/delegated-apnic-extended-latest
4. IPv4 Prefixes Delegated by ARIN, ftp://ftp.arin.net/pub/stats/arin/delegated-arin-extended-latest
5. IPv4 Prefixes Delegated by LACNIC, ftp://ftp.lacnic.net/pub/stats/lacnic/delegated-lacnic-extended-latest
6. IPv4 Prefixes Delegated by RIPE NCC, ftp://ftp.ripe.net/ripe/stats/delegated-ripencc-extended-latest
7. rcynic RPKI validator, http://rpki.net/wiki/doc/RPKI/RP/rcynic
8. University of oregon route views project, http://www.routeviews.org
9. YouTube Hijacking: A RIPE NCC RIS case study (March 2008), http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study
10. Fincham, M.: RPKI, NZNOG 2014 (February 2014), http://hotplate.co.nz/archive/nznog/2014/rpki/
11. Goldberg, S., Shapira, M., Hummon, P., Rexford, J.: How secure are secure interdomain routing protocols? Computer Networks 70, 260–287 (2014)
12. Heilman, E., Cooper, D., Reyzin, L., Goldberg, S.: From the Consent of the Routed: Improving the Transparency of the RPKI. In: Sigcomm 2014 (2014)
13. Kloots, J.: RPKI Routing Policy Decision-Making, A SURFNET Perspective (February 2014), https://blog.surfnet.nl/?p=3159
14. Lad, M., Massey, D., Pei, D., Wu, Y., Zhang, B., Zhang, L.: PHAS: a prefix hijack alert system. In: Proc. USENIX Security Symposium (2006)
15. Lepinski, M., Kent, S.: An Infrastructure to Support Secure Internet Routing (February 2012), RFC 6480
16. Litke, P., Stewart, J.: BGP Hijacking for Cryptocurrency Profit (August 2014), http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/
17. Toonk, A.: Hijack Event Today by Indosat (april 2014), http://www.bgpmon.net/hijack-event-today-by-indosat/
18. Wählisch, M., Maennel, O., Schmidt, T.C.: Towards Detecting BGP Route Hijacking using the RPKI. In: Sigcomm 2012 (Poster) (2012)
19. Zmijewski, E.: Indonesia Hijacks the World (april 2014), http://www.renesys.com/2014/04/indonesia-hijacks-world/