A Study of Prefix Hijacking and Interception in the Internet

Hitesh Ballani
Cornell University
Ithaca, NY
hitesh@cs.cornell.edu

Paul Francis
Cornell University
Ithaca, NY
francis@cs.cornell.edu

Xinyang Zhang
Cornell University
Ithaca, NY
jzhang@cs.cornell.edu

ABSTRACT

There have been many incidents of prefix hijacking in the Internet. The hijacking AS can blackhole the hijacked traffic. Alternatively, it can transparently intercept the hijacked traffic by forwarding it onto the owner. This paper presents a study of such prefix hijacking and interception with the following contributions: (1). We present a methodology for prefix interception, (2). We estimate the fraction of traffic to any prefix that can be hijacked and intercepted in the Internet today, (3). The interception methodology is implemented and used to intercept real traffic to our prefix, (4). We conduct a detailed study to detect ongoing prefix interception.

We find that: Our hijacking estimates are in line with the impact of past hijacking incidents and show that ASes higher up in the routing hierarchy can hijack a significant amount of traffic to any prefix, including popular prefixes. A less apparent result is that the same holds for prefix interception too. Further, our implementation shows that intercepting traffic to a prefix in the Internet is almost as simple as hijacking it. Finally, while we fail to detect ongoing prefix interception, the detection exercise highlights some of the challenges posed by the prefix interception problem.

Categories and Subject Descriptors: C.2.2 [Network Protocols]: Routing Protocols.

General Terms: Measurement, Security.

Keywords: Routing, BGP, Hijacking, Interception.

1. INTRODUCTION

In the recent past, there have been many instances of "prefix hijacking" in the Internet wherein an Autonomous System "hijacks" routes simply by advertising the corresponding prefixes. Such incidents are regularly reported on the NANOG mailing list [1]; [2–6] report a few specific ones. This, in turn, has prompted a number of proposals to address the problem [3,4,7–21] – some of these target the specific goal of detecting prefix hijack attempts while others strive to improve the general security of inter-domain routing.

Irrespective of whether it is caused by a misconfiguration or a malicious entity, the AS that hijacks a prefix can *blackhole* all the hijacked traffic and thus, cause a denial-of-service attack against the prefix owner [22]. It can also *redirect* the traffic to an incorrect destination and use this for a phishing attack [22]. Spammers have also been known to use hijacked prefixes [23]. In all these cases, the prefix's traffic does not reach the destination. However, it is also possible for an AS to hijack the traffic to a prefix and then *forward this traffic on to the prefix owner* [22,24]. Hence, instead of blackholing the destination's traffic, this would allow the AS to "intercept" the traffic without disrupting the destination's connectivity to the Internet and thus, become a man-in-the-middle. For instance, this may be used by an AS in the USA to transparently capture, record and subsequently deliver IP traffic between end points in Europe and the Middle East.

While these attacks are a bleedingly obvious consequence of the way inter-domain routing operates, their egregiousness cannot be disputed. This is especially true for interception since the intercepted traffic still reaches the proper destination. Consequently, it is less likely that an unsuspecting victim would notice ongoing interception and unlike the other possibilities, this is one case where a prefix could actually be hijacked for a long period. Indeed, it is possible that interception may be happening undetected, on a regular basis, on the Internet today!

However, despite all the incidents and subsequent work in the research community, an actual quantification of the impact of prefix hijacks on the Internet is sorely missing. Motivated by this, in this paper we present an analysis of the impact of an invalid advertisement on ASes in the Internet with specific emphasis on the possibility and practical feasibility of using routing advertisements for traffic interception. To this effect, this paper studies the following aspects of Internet prefix hijacking and interception (with our contributions italicized):

First, we use common routing policies to *analyze the probability of an AS hijacking the traffic to a prefix from another AS.* Note that while hijacking traffic to a prefix simply involves advertising the prefix into inter-domain routing, prefix interception seems trickier because the invalid advertisement originated by the hijacking AS can impact the valid route that it uses to forward the traffic to the prefix's owner. Consequently, we extend our analysis to *determine scenarios where interception is possible and propose a general methodology for prefix interception.* Our analysis shows that a hijacking AS, with high probability, can statically determine the neighbors to which it can safely advertise an invalid route for a prefix while still being able to forward the hijacked traffic back to the prefix owner.

SIGCOMM'07, August 27–31, 2007, Kyoto, Japan.

Second, we use routing tables collected at the Route-Views repository [25] to *estimate the fraction of other Route-Views ASes whose traffic to any prefix can be hijacked and intercepted by a given Route-Views AS*. As one would expect, our estimates show that tier-1 ASes can, on average, hijack traffic to any prefix from a significant fraction of ASes (52% to 79%). These estimates also apply to hijacking of popular prefixes that carry a lot of traffic. Further, tier-1 ASes can route all the hijacked traffic back to the owner and hence, can also intercept traffic to any prefix from a significant fraction of ASes. However, these fractions drop off for ASes lower down in the routing hierarchy. For instance, tier-3 ASes and beyond can, on average, hijack traffic to any prefix from 13% to 31% of ASes and intercept traffic from 7% to 17% of ASes. We also *verified our estimates against known prefix-hijacking events on the Internet* and found them to be fairly accurate.

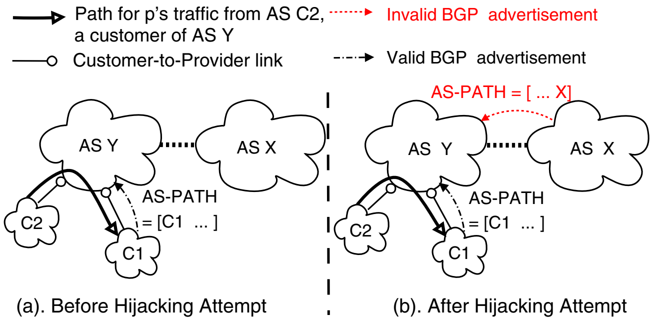
Third, we *implement the aforementioned interception meth--odology and use it to actually intercept traffic to a prefix* belonging to us in five different scenarios. Further, in each scenario, we probe the prefix from >20,000 vantage points to *quantify the fraction of traffic that can be hijacked and the fraction that can be intercepted*. These results, at the very least, provide anecdotal evidence of the claim that a significant amount of traffic to prefixes on the Internet can be intercepted. Moreover, the implementation suggests that intercepting traffic to a prefix in the Internet is almost as simple as hijacking it, requiring changes only in BGP routing policy at the intercepting AS.

Finally, we use a combination of control-plane and data-plane information to *look for actual interception in the Internet*. The study yielded a few unexplained anomalies that could be due to prefix interception. However, our analysis shows that these anomalies can just as well arise from valid routing arrangements. While negative, this result captures some of the challenges in detecting ongoing prefix interception. More generally, the estimates presented in this paper rely on a simplistic model of Internet routing and have several other limitations that we discuss in section 7. However, in spite of these limitations, our quantification and implementation efforts serve to highlight the severity of the problem. In this context, we hope that this paper would bring to the fore the (obvious) possibility of traffic interception in today's inter-domain routing and influence the design of Internet security protocols.

2. METHODOLOGY

ASes in the Internet can use *invalid advertisements* for a *target prefix*, i.e. advertisements with an AS-PATH that does not represent the true AS-PATH to the prefix, to convince other ASs to route traffic for the prefix to itself and hence, hijack the prefix. Among other things, the *hijacking AS* can forward the hijacked traffic to the owner and hence intercept the prefix. Consequently, prefix interception is always preceded by prefix hijacking.

The most obvious form of an invalid advertisement is one where the *hijacking AS*, say X, claims to own the prefix and hence, advertises the prefix with AS-PATH=[X]. We refer to this as an advertisement with an *invalid origin*. However, such an invalid advertisement would lead to a Multiple Origin AS (MOAS) anomaly [26]. The hijacking AS can avoid this by advertising the prefix with AS-PATH=[X, O] where AS O is the owner of the prefix. We refer to this as an advertisement with an *invalid next hop*. Of course, the hijacking AS can advertise the prefix with an even longer AS-PATH but, as we show later in the paper, that would significantly reduce the amount of traffic it can hijack. Hence, we focus on hijacking and interception with routing advertisements that have an invalid origin or an invalid next hop.


Path for p's traffic from AS C2, a customer of AS Y
Invalid BGP advertisement
Customer-to-Provider link
Valid BGP advertisement
AS Y
AS X
AS-PATH
= [C1 ...]
C2
C1
AS-PATH = [... X]
AS Y
AS X
AS-PATH
= [C1 ...]
C2
C1

(a). Before Hijacking Attempt

(b). After Hijacking Attempt

Figure 1: AS Y has an existing customer-route to p and hence, hijacking p's traffic from Y with an invalid provider or peer route is not possible.

Apart from advertising an invalid route for an already rout--able prefix, there are a couple of other approaches that an AS could possibly use for hijacking traffic to a prefix:

(a). An AS could advertise a more specific prefix than the one being advertised by the owner and this would hijack all the traffic to the specific prefix. However, the hijacking AS would not be able route this traffic onto the owner and hence, interception would not be possible.

(b). As AS could advertise a less specific prefix than the one being advertised by the owner. This would hijack traffic to the prefix only when the owner withdraws its advertisements. However, even in that situation, the hijacking AS would not be able to route the hijacked traffic to the owner.

Since the impact of such advertisements can be trivially predicted, we don't study them here. Hence, our estimates for the fraction of traffic that can be hijacked and the fraction that can be intercepted are restricted to hijacking based on advertisement of the same prefix as the one being advertised by the owner.

The discussion in the rest of this section focusses on an AS X trying to hijack (and intercept) the traffic for target prefix p. In the first part of the section we analyze X's ability to hijack p's traffic using an advertisement with an invalid origin (though the arguments can trivially be extended to advertisements with an invalid next hop), while in the second part we study how X ensures that it can forward the hijacked traffic back to p's owner.

2.1 Hijacking Analysis

AS X advertises an invalid route for prefix p with AS-PATH=[X]. We want to evaluate the impact of this advertisement on AS Y that is (n-1) AS hops away from X and thus, receives a route of AS-PATH length n.[1] Specifically, we would like to determine if Y chooses this invalid route over its existing route to p, thus allowing AS X to hijack p's traffic sourced from it. Here, "traffic sourced from AS Y" refers to

[1] Y may be topologically closer to X than (n-1) hops but the shortest path that the invalid advertisement needs to propagate to reach Y comprises of (n-1) ASes.

traffic originating at Y plus "traffic sourced from any of Y's neighbors" that is routed through Y.

Obviously, AS Y's choice depends on both its existing route and the newly-received invalid route to p. We term a route to be a "customer-route" or a "peer-route" or a "provider-route" depending on whether the next-hop AS in the AS-PATH is a customer, a peer or a provider respectively. Since both the existing route and the invalid route could be any of these, there are nine cases to consider. Below we try to answer the aforementioned question for each of these cases, given two assumptions:

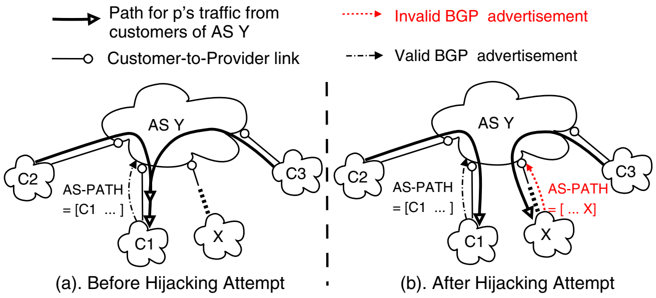
(a). The invalid route advertised by AS X reaches AS Y. ISPs are known to install route filters so as to accept advertisements only for specific prefixes from their neighbors, especially if the neighbor is a stub AS [27]. Thus, route filters employed by any AS along the path from X to Y would falsify this assumption. Further, for the invalid advertisement to actually reach Y, it must be accepted and propagated by all ASes along the path. Thus, an implicit assumption here is that X is able to hijack traffic from all ASes along the path from X to Y (in practice, one could verify this assumption by applying the analysis presented below to each AS along the path).

(b). AS Y's choice also depends on its routing policies. Measurement studies in the past have shown that a large majority of ASes on the Internet tend to assign higher local-preference values to customer-routes than to peer-routes than to provider-routes [28]. Since local-preference values are the first step of the BGP decision process [29], ASes prefer customer routes to peer routes to provider routes. We assume that this holds for Y as this lets us analyze the possibility of Y's traffic being hijacked. Further, a part of the analysis also assumes that AS Y assigns the same local-preference value to all its customers, the same value to its peers and the same value to its providers; however, most of the arguments below apply even if this last assumption does not hold. As detailed in section 3.1, we verified these assumptions for tier-1 ASes.

Cases 1-3. *Existing route is customer-route, invalid route is a customer/peer/provider route.* If the invalid route that AS Y receives is a peer or a provider route, irrespective of the attributes (for example, the AS-PATH length) of this route, Y prefers the existing customer-route (assumption (b)). Thus, Y's traffic is not hijacked. Figure 1 shows this scenario.

On the other hand, if the invalid route is a customer-route, AS Y's policy would give equal preference to both routes and hence, the decision is based on the length of the route [29]. If the AS-PATH length of the existing route is less than n, it is preferred. If the AS-PATH length of the existing route is more than n, the invalid route is preferred. Finally, if Y's existing route is n AS-hops long, it must choose between two routes with the same local preference and the same length. This choice is based on other factors such as the IGP metric of the routes [29]. Consequently, some routers belonging to Y may choose to stick with the existing route while others may choose to use the invalid route. Hence, in this case, some fraction of Y's traffic for p may be hijacked. Figure 2 shows this scenario.

Case 4-6. *Existing route is a peer route, invalid route is a customer/peer/provider route.* If the invalid route that AS Y receives is a provider route, it prefers the existing peer-route. Thus, Y's traffic is not hijacked. As a contrast, if the invalid route is a customer-route, Y prefers it and Y's traffic is hijacked.



Path for p's traffic from customers of AS Y
Invalid BGP advertisement
Customer-to-Provider link
Valid BGP advertisement
AS Y
C2
C3
AS-PATH = [C1 ...]
C1
X
(a). Before Hijacking Attempt
AS Y
C2
C3
AS-PATH = [C1 ...]
AS-PATH = [... X]
C1
X
(b). After Hijacking Attempt

Figure 2: AS Y has an existing customer-route to p and receives an invalid route (advertised by AS X) of equal length through a customer. This causes some fraction of p's traffic to be hijacked.

Invalid route ⇒ Existing route	Length	Customer	Peer	Provider
	<n	✗	✗	✗
Customer	=n	–	✗	✗
	>n	✓	✗	✗
	<n	✓	✗	✗
Peer	=n	✓	–	✗
	>n	✓	✓	✗
	<n	✓	✓	✗
Provider	=n	✓	✓	–
	>n	✓	✓	✓

Table 1: AS Y's traffic to prefix p can (✓), cannot (✗) or can partly (–) be hijacked depending on its existing route and the invalid route.

Finally, if the invalid route is a peer-route, AS Y's policy would give equal preference to both routes and hence, the decision is based on the AS-PATH length of the route [29]. If the length of the existing route is less than n, traffic is not hijacked; if the length is more than n, traffic is hijacked; if the length is n AS hops, some fraction of the traffic may be hijacked.

Case 7-9. *Existing route is a provider route, invalid route is a customer/peer/provider route.* The possibility of hijacking AS Y's traffic in these cases follows from the arguments presented above. Table 1 summarizes the hijacking possibility for all nine cases.

2.2 Interception Analysis

In order to be able to intercept traffic to the prefix p, the hijacking AS needs to forward the hijacked traffic on to p's owner. It can do so by forwarding the hijacked traffic along its existing valid route to p. Figure 3 shows the process by which hijacking AS X hijacks prefix p's traffic from Y (originating at Y's customer $C2$) and then forwards it on to p's owner through its peer W. However, for this to work, X's existing route to p should not be impacted by the invalid route that it advertises. Hence, the hijacking AS X would like to ensure the following *safety*[2] condition:

> *None of the ASes along the route to prefix p used by the hijacking AS should choose the invalid route advertised by it (if they do receive the invalid route) over their existing route to p.*

Note that the obvious way for AS X to satisfy the above

[2] Here, safety refers to the fact that X does not introduce routing instability and is able to route the hijacked traffic to its owner.

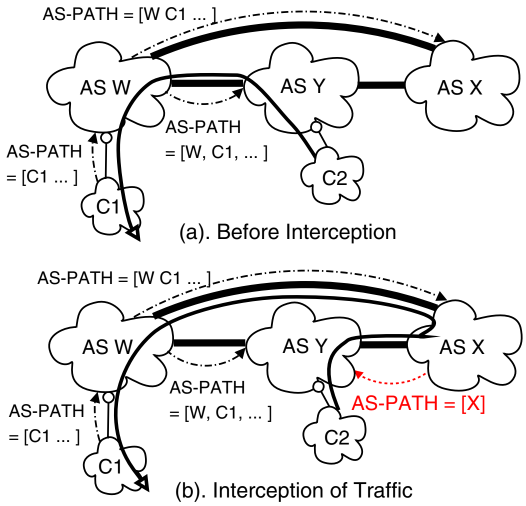


Figure 3: AS X uses an invalid advertisement to hijack traffic from AS Y and then routes the traffic to the owner using its existing route through peer AS W.

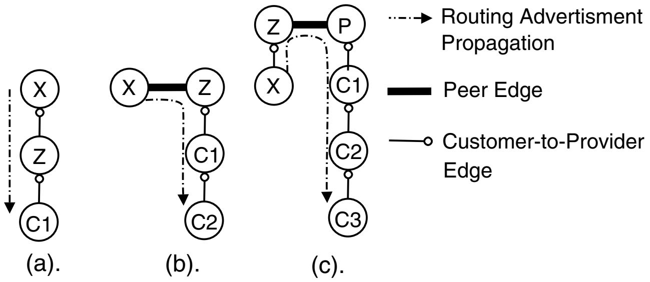


Figure 4: Propagation of the invalid route advertised by AS X to its (a) customer, (b) peer, (c) provider.

condition would be to advertise the invalid route such that the traffic from the ASes along its existing route to p is not hijacked. In theory, the discussion from the previous section applies to the possibility of hijacking from these ASes. However, this observation doesn't have much practical value since X wouldn't know how an invalid route advertised to any of its neighbors would be propagated to these ASes and hence, would not be able to determine if an invalid advertisement can indeed hijack the traffic from a given AS along the path.

Instead, we would like to analyze if a hijacking AS can ensure the safety condition based on local information alone. Specifically, AS X would like to determine if advertising an invalid route for p to a neighboring AS, say Z, can impact its existing route for p. X's existing route to p can be a customer, peer or provider route and Z can be X's customer, peer or provider and hence, there are nine cases to consider. Below we try to answer the aforementioned question, given two assumptions:

(a). As with the hijacking analysis, we assume that ASes prefer customer routes to peer routes to provider routes.

(b). We assume that Internet paths follow the "Valley-free" property [30], i.e. after traversing a provider-to-customer edge or a peer edge, the path cannot traverse another customer-to-provider or peer edge. Analogously, once a routing advertisement traverses a provider-to-customer edge or a peer edge, the advertisement cannot traverse another customer-to-provider or peer edge.

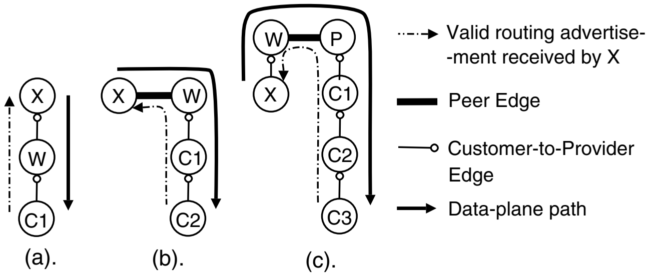

X
W
C1
(a).
X
W
C1
C2
(b).
W
P
X
C1
C2
C3
(c).
Valid routing advertise--ment received by X
Peer Edge
Customer-to-Provider Edge
Data-plane path

Figure 5: AS X's existing route for prefix p is through a (a) customer, (b) peer, (c) provider.

Consequently, when X advertises the invalid route to a customer, the advertisement can only traverse provider-to-customer edges. Hence, the advertisement is restricted to ASes below X in the AS hierarchy and represents a provider route for these ASes. When X advertises the invalid route to a peer, the advertisement traverses one peer edge followed by provider-to-customer edges only. Hence, other than the peer being advertised to, the advertisement is restricted to ASes below X in the AS hierarchy and represents a provider route for these ASes. Figure 4(a,b) illustrate these scenarios.

When X advertises the invalid route to a provider, each control plane path traversed by the advertisement comprises of one or more customer-to-provider edges followed by zero or one peer edges and zero or more provider-to-customer edges. Hence, the advertisement is propagated to all levels of the AS hierarchy. However, it is important to note that while ASes that are above X in the AS hierarchy may receive the invalid advertisement from a customer, peer or provider, ASes at the same level or below X will always receive the advertisement from a provider (i.e. a provider route). Figure 4(c) illustrates this scenario.

Case 1-3. *X's existing route is a customer route, X advertises the invalid route to a customer/peer/provider.* The fact that X's existing path to p is a customer-route implies that the first edge along this path is a provider-to-customer edge. Further, the valley-free property of Internet paths implies that this is a "downhill path" (as defined by [30]) comprising of a sequence of provider-to-customer edges. Thus, all ASes along the path are below X in the AS hierarchy and use a customer route to p. Figure 5(a) illustrates this scenario. As discussed in assumption (b), irrespective of whether X advertises the invalid route to a customer/peer/provider, the invalid route would appear as a provider route to ASes below X and hence, will not be chosen by them over their existing customer route. Thus, X can advertise the invalid route to all its neighbors.

Case 4-6. *X's existing route is a peer route, X advertises the invalid route to a customer/peer/provider.* The valley-free property implies that X's existing path to p comprises of one peer edge followed by a sequence of provider-to-customer edges. Thus, all ASes along the path use a customer route to p. Figure 5(b) illustrates this scenario. Also, as before, even if the invalid route advertised by X propagates to any of the ASes along the path, it will be a provider or a peer route and hence, will not be chosen over the existing customer route. Thus, X can advertise the invalid route to all its neighbors.

Case 7-9. *X's existing route is a provider route, X advertises the invalid route to a customer/peer/provider.* The valley-free property implies that X's existing path to p comprises of one or more customer-to-provider edges followed by

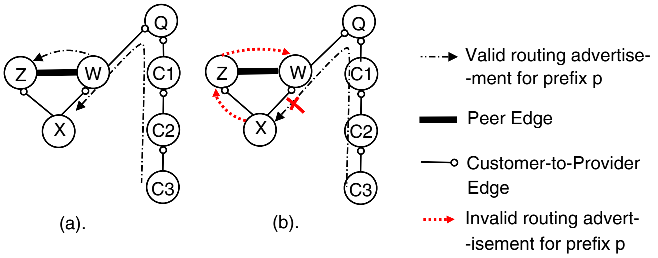


Figure 6: (a) Hijacking AS X has a route for p through provider W. (b) The invalid route advertised by X to another provider Z to intercept p's traffic impacts its existing route for p.

zero or one peer edge followed by zero or more provider-to-customer edges. Hence, ASes along the path may be using a customer or peer or provider route to p. However, any ASes along the path that are at the same level or below X in the AS hierarchy would be using a customer route to p. Figure 5(c) illustrates this scenario.

As discussed in assumption (b), when X advertises the invalid route to a customer or a peer, the advertisement is restricted to ASes at the same level or below X in the AS hierarchy and represents a provider or peer route for them. This implies that the invalid route will not be chosen by these ASes. Hence, X can advertise the invalid route to its customers and peers.

However, when X advertises the invalid route to a provider, the route may be received by ASes above X in the AS hierarchy. For these ASes, both the invalid route and the existing route can be a customer, peer or provider route implying that it is possible they prefer the invalid route. This violates the safety condition and hence, X cannot advertise the invalid route to its providers. Figure 6 shows such a scenario wherein the invalid route advertised by AS X to its provider AS Z impacts its existing route for prefix p.

The analysis presented above implies that an AS trying to intercept traffic for target prefix p can advertise the invalid route to all its neighbors unless its existing route for p is through a provider, in which case the invalid route should not be advertised to other providers of the AS. However, there are a couple of other things to note: First, while our assumptions regarding AS policies and valley-free paths hold for a majority of ASes on the Internet, exceptions certainly do exist. Hence, the aforementioned policy for advertising invalid routes *ensures safety with a high probability*; an AS advertising invalid routes may still cause routing instability and needs to account for it. It can do so by observing if its existing route for p changes as a result of advertising the invalid route. If such a change occurs, the hijacking AS can pin point the anomaly-causing neighbor based on the recently received advertisements for p and hence, stop advertising the invalid route to this neighbor.

Second, even when the hijacking AS's existing route for p is through a provider, advertising the invalid route to another provider may not necessarily impact the AS's route for p. Hence, it is possible to imagine the hijacking AS using an aggressive approach by advertising the invalid route to all neighbors and then stopping the advertisement to specific neighbors if route instability arises.

Based on the description above, the following pseudo-code represents the conceptual process by which hijacking AS X can intercept traffic to target prefix p from its neighbors:

```
If (existing route to p is through a provider)
then
 Advertise to all peers and customers a route
 for prefix p with AS-PATH [X];
else
 Advertise to all neighbors a route for prefix
 p with AS-PATH [X];
endif
If (the invalid advertisement causes the
  existing route for p to change)
then
    Stop the advertisement to the
    anomaly-causing neighbor;
endif
```

3. HIJACKING AND INTERCEPTION ESTIMATES

Given the methodology described in the previous section, we can estimate the fraction of ASes in the Internet whose traffic to a *target prefix* that can be hijacked and intercepted by any given AS.

3.1 Hijacking by tier-1 ASes

Here we focus on hijacking by tier-1 ASes and determine the fraction of other tier-1 ASes whose traffic to a prefix can be hijacked and intercepted by a tier-1 AS in the Internet today. A tier-1 AS is an AS with no providers and a peering with all other tier-1 ASes [31]. Hence, tier-1 ASes are at the top of the routing hierarchy. We used CAIDA's AS ranking tool [31] and commercial reports on AS ranking [32] to come up with a list of 15 highly ranked ASes that are considered as tier-1 ASes in this paper. Note that we treat hijacking by tier-1 ASes as a special case since we can verify the two assumptions made by the analysis presented in section 2.1:

Assumption (a). *An invalid route advertised by the hijacking AS reaches the AS whose traffic ought to be intercepted.* The fact that all tier-1 ASes peer with each other makes this trivially true. Further, it is unlikely that the invalid route advertised by a hijacking tier-1 AS would be filtered out by any of the other tier-1 ASes [27].

Assumption (b). *Tier-1 ASes prefer customer-routes over peer-routes and give the same preference to routes from different peers.*[3] A lot of tier-1 ASes offer publicly-accessible route-servers and policy guides which let us determine their import policies expressed in the form of local-preference values. We were able to do this for nine of the fifteen tier-1 ASes. While we don't show the actual local-preference values in the interest of brevity, we found that this assumption was satisfied for all the nine ASes.

This validation of the assumptions improves our confidence in the accuracy of the estimates presented here. The actual estimates were guided by two observations. First, the fact that tier-1 ASes don't have any provider routes implies that they can safely advertise the invalid route to all neighbors. Consequently, (almost) all traffic that can be hijacked by a tier-1 AS can also be routed back to its owner.

Second, from the point of view of other tier-1 ASes, the invalid route advertised by hijacking AS X is a peer route one AS-hop long. This, combined with table 1, implies that X can hijack all traffic for prefix p from a peer AS if the

[3] Tier-1 ASes don't have provider routes. Also, we focus on hijacking from other tier-1 ASes that are peers of the hijacking AS and hence, their preference amongst routes from different customers is not relevant.

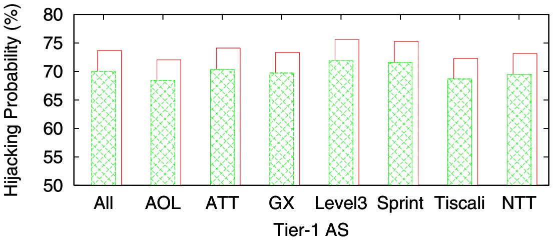


Figure 7: Probability of prefix hijacking on average and for each of the tier-1 ASes that serve as hijacking ASes in our estimation.

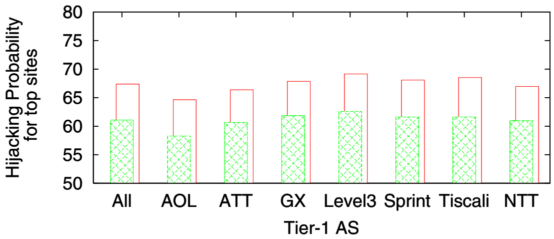


Figure 8: Probability of prefix hijacking for prefixes corresponding to top-100 sites.

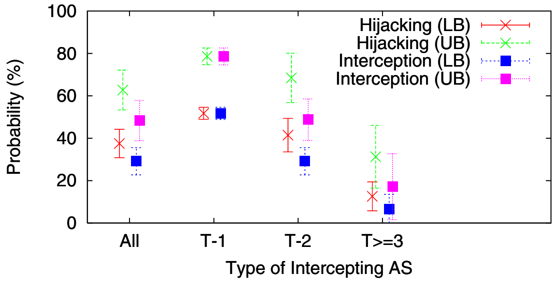


Figure 9: Probability of prefix hijacking and prefix interception for ASes in the RV-set.

peer's existing route for p is a provider route or a peer route of length more than one AS hop. AS X can intercept some fraction of the traffic if the peer's existing route for p is a peer route of length one. However, this fraction depends on both the intra-domain metrics of the peer AS and the locations at which X peers with it. Given that we lack this information, we define the upper and the lower bounds of hijacking; the lower bound assumes that none of p's traffic from such peers is hijacked while the upper bound assumes that all of p's traffic from such peers is hijacked.

Overall, we can determine if X can hijack traffic for prefix p from a peer tier-1 AS based on the peer's existing route for p. Since the Route-Views repository collects routes from 7 of the 15 tier-1 ASes (AOL, ATT, Global Crossing, Level3, Sprint, Tiscali and NTT), we focussed on these seven ASes and for each of them, determined the prefixes in the Internet routing table whose traffic from the other six tier-1 ASes (and their customers) can be hijacked. For ease of exposition, we hereon refer to the fraction of other ASes whose traffic is hijacked by the hijacking AS (averaged across all prefixes) as the *probability of hijacking*. The *probability of interception* is defined analogously. Thus, we were able to determine the probability of hijacking for each of the seven ASes. The fact that the hijacking AS is a tier-1 AS implies that the interception probability is the same.

Figure 7 shows the lower and the upper bound for probability of prefix hijacking on average and for individual ASes. The figure shows that a tier-1 AS can, on average, hijack the traffic for a prefix from another tier-1 AS with ≈70-75% probability. The fact that the ability to hijack a prefix's traffic from a peer depends only on the peer's existing route for the prefix shows up in that the hijacking probability does not vary much across tier-1 ASes. Further, this implies that the estimate also applies to hijacking of tier-1 traffic by multiple colluding tier-1 ASes.

While we have focussed on the probability of prefix hijacking, another important question is the amount of traffic that can be hijacked. Note that the fact that a small number of prefixes carry a majority of the Internet's traffic [33] implies that the probability estimates can be misleading. To address this, we focussed on the top 100 web-sites in terms of the traffic carried according to the Alexa's web-site rankings [34]. We mapped these sites to the corresponding prefixes and determined if a tier-1 AS can hijack traffic for these popular prefixes from its peers. Figure 8 plots the hijacking probability for the popular prefixes. As can be seen, a tier-1 AS can hijack traffic for these prefixes with a probability of ≈60-70%, which is close to the overall estimate.[4] This suggests that our estimates should closely approximate the fraction of traffic that a tier-1 AS can intercept from its peers.

3.2 Hijacking by any AS

We now try to estimate the probability of prefix hijacking and the probability of prefix interception for ASes in general, not just tier-1 ASes. To this effect we focus on all the 34 ASes that contribute to the Route-Views repository – these ASes are hereon referred to as the RV-set. This includes 7 tier-1 ASes, 19 tier-2 ASes and 8 other ASes (tier$\geq$3). For each AS in the RV-set, we determined the prefixes in the Internet routing table whose traffic from the other ASes in the set can be hijacked and routed back to the prefix owner. Specifically, the estimation procedure required us to answer the following questions: Can an AS in the RV-set, say X, hijack traffic for target prefix p from another AS, say Y, in the RV-set? If yes, can it route this hijacked traffic on to p's owner?

As described in section 2.1, AS X's ability to hijack p's traffic from AS Y depends on both Y's existing route for p and the invalid route received by Y. The Route-Views data provides Y's existing route for each prefix p. As far as the propagation of the invalid route advertised by X is concerned, we determined a prefix owned by X (i.e. the origin AS in the AS-PATH for the prefix is X) and used Y's route to this prefix as an approximation of the invalid route that Y would receive. Lets assume that the AS next to the origin AS in the AS-PATH for this route is Z. Hence, AS X advertises the invalid route to its neighbor Z and this propagates onto AS Y. Section 2.2 detailed that the safety of X advertising the invalid route to its neighbor Z depends on both X's existing route for p and X's relation with Z. As before, the Route-Views data provides X's existing route for each prefix p. Finally, we used CAIDA's AS relationship data [35] to determine X's relation with Z.

Using this basic methodology, we estimated the upper (UB) and lower bound (LB) for the probability of hijacking and the probability of interception for the ASes in the RV-set. These

[4] In practice, their popularity suggests that these prefixes are well engineered and monitored and hence, we believe that it is unlikely that an AS will attempt to hijack or intercept their traffic.

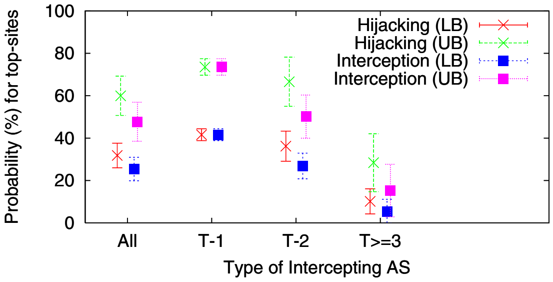


Figure 10: Probability of prefix hijacking and prefix interception for popular prefixes.

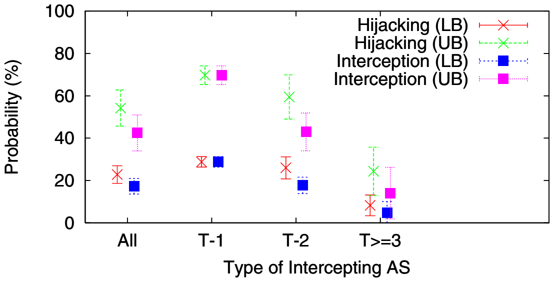


Figure 11: Probability of prefix hijacking and prefix interception with routes that have an invalid next-hop.

are plotted in figure 9 – the error bars in the figure represent the 95% confidence interval for the corresponding bound. The graph shows that the overall probability of hijacking a prefix varies between 38% and 63% while the probability of intercepting a prefix varies between 29% and 48%. Also plotted are the probabilities for ASes of different kinds. As mentioned earlier, for tier-1 ASes, the hijacking and interception probabilities are the same and these vary between 52% and 79%. Note that this encompasses the range in the previous section. However, as one would expect, both the hijacking and the interception probabilities drop off for tier-2 ASes and onwards. Also, such ASes have a higher variance and hence, a larger confidence interval for the various bounds.

As before, we also determined these probabilities for popular prefixes corresponding to the top-100 sites. These are plotted in figure 10. The figure shows that both the hijacking and interception probabilities for the popular prefixes are only slightly lower (≈5-10%) than for all prefixes. Overall, our results show that ASes higher up in the AS hierarchy (tier-1 and some tier-2 ASes) can both hijack and intercept any prefix with a high probability (>50%). However, invalid routes advertised by ASes lower down in the hierarchy wouldn't have as significant an impact.

Note that the estimates in this and the previous section have assumed that the hijacking AS advertises routes with an invalid origin. As mentioned earlier, this can lead to a MOAS anomaly and the hijacking AS can avoid this by advertising routes with an invalid next hop. This would increase the length of the invalid route and hence, reduce the amount of traffic that can be hijacked (and intercepted) but would make detection harder. We measured the hijacking and interception probabilities for ASes in the RV-set with such advertisements. These are plotted in figure 11. The figure shows that using advertisements with an invalid next-hop reduces the hijacking and interception probabilities by ≈10-20% with the probabilities for tier-1 ASes ranging between 30% to 70%.

Prefix	Owner (AS name)	Hijac- -ker	Estimated Hijacking LB-UB %	Actual Hijack- -ing (%)
64.233.161.0/24	Google	Cogent	35.5-64.5	45.2
12.173.227.0/24	MarthaStewart Living	ConEd.	36.4-84.9	42.4
63.165.71.0/24	Folksamerica	”	39.4-72.7	39.4
64.132.55.0/24	OverseasMedia	”	18.2-51.5	18.2
65.115.240.0/24	ViewTrade	”	27.2-54.5	21.2
65.209.93.0/24	LavaTrading	”	39.4-72.7	45.5
66.77.142.0/24	Folksamerica	”	90.9-90.9	90.9
66.194.137.0/24	MacKayShields	”	18.2-57.5	27.3
66.207.32.0/20	ADI	”	45.5-66.7	63.6
69.64.209.0/24	TheStreet.Com	”	72.7-81.8	84.8
160.79.45.0/24	RhodesASN	”	27.3-75.8	51.5
160.79.67.0/24	TheStreet.Com	”	60.6-75.8	69.7
192.251.16.0/24	T&TForex	”	27.3-57.6	27.3
198.15.10.0/24	TigerFund	”	0-1	60.6
204.13.72.0/24	FTENNY	”	93.9-93.9	75.8
216.223.46.0/24	SDSNY	”	51.5-78.8	18.2

Table 2: Comparing our estimates for known prefix hijacking events with the actual hijack probability.

3.3 Verifying against known events

We now verify our estimates against known prefix hijack events. For instance, Cogent (AS 174) hijacked a prefix (64.233.161.0/24) belonging to Google (AS 15169) on May 07, 2005 through an advertisement with an invalid origin [5]. According to BGP updates collected at the Route-Views repository, Cogent started advertising the prefix on May 07, 2005 14:37:56 and this caused 14 of the 31 (45.2%) distinct ASes part of the RV-set at that time to choose the invalid route. It is not known if the hijacked traffic was blackholed or actually routed back to Google. We ran our analysis on a routing table collected earlier that day (before the hijack) and estimated that the probability that an invalid route for the prefix advertised by Cogent would hijack traffic from ASes in the RV-set ranges between 35.5% and 64.5%. Further, the fact that Cogent is a tier-1 AS implies that the same applies to the probability of interception. As can be seen, our estimate encompasses the fraction of ASes from which traffic was actually hijacked. Further, amongst the 11 ASes whose traffic our analysis predicted would be surely be hijacked (i.e. they were included in the lower bound), only one was not hijacked in reality.

We performed the same exercise for other known hijack events. Since we did not have BGP routing tables from the hijacking AS in these cases, we were only able to predict the probability of hijacking. Table 2 shows the results. As can be seen, our estimate encompasses the actual hijacking probability for 11 of the 16 prefixes analyzed, in 3 cases we over-estimate, in 1 case we under-estimate while in 1 case our estimate provides no information. Note that the assumption that the invalid route actually reaches the ASes in the RV-set cannot be verified and this is a frequent cause for over-estimation. More importantly, the outliers show that Internet routing is certainly more complex than the simplified model used for our analysis. However, the proportion of cases where our estimates were accurate and the exercise in the next section fortify our confidence in the results presented.

4. INTERNET TRAFFIC INTERCEPTION

There have been instances of prefix hijacking in the Internet. However, we are not aware of incidents where the hijacked traffic was still being routed to the owner. While

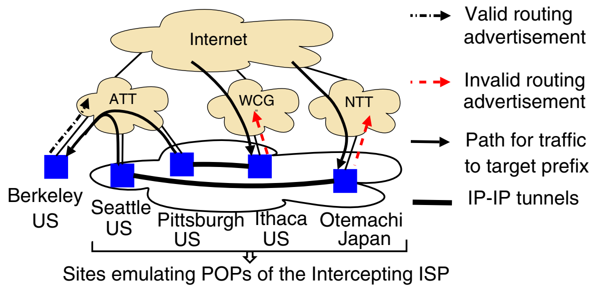

Valid routing advertisement
Invalid routing advertisement
Path for traffic to target prefix
IP-IP tunnels
Internet
ATT
WCG
NTT
Berkeley US
Seattle US
Pittsburgh US
Ithaca US
Otemachi Japan
Sites emulating POPs of the Intercepting ISP

Figure 12: Intercepting traffic from the prefix owner at the Berkeley site. The four other sites emulate an ISP, use invalid routes to hijack traffic and route it back to the owner.

the fact that ISPs can use invalid routing advertisements to intercept traffic is pretty obvious, we still wanted to attempt interception in practice. Apart from serving as a proof of concept, our hope was to derive insights from this exercise into the practicality of intercepting traffic within the existing routing framework. In this section, we detail our deployment and implementation efforts for intercepting traffic in the Internet. We used this to actually intercept a prefix's traffic (of course, the prefix belonged to us).

For these experiments, we deployed hosts at five different sites and used the Quagga software router [36] on these hosts to establish EBGP peerings with different ISPs. Effectively, this allowed us to advertise our prefix (204.9.168.0/22) into the Internet through the peerings. These sites and the upstream ISP at each site are shown in figure 12. The idea behind the experiments was to use our prefix as the *target prefix* with one of the sites serving as the owner of the prefix and the four other sites serving as the geographically distributed POPs of an ISP trying to intercept the prefix. We used IP-IP tunnels between these sites for any intra-domain communication between the POPs of our emulated ISP. Figure 12 shows one such set-up with the site in Berkeley acting as the prefix owner. Invalid routes for the prefix are advertised through the sites at Ithaca and Otemachi. These invalid advertisements hijack traffic for the target prefix which is tunneled to the other two sites and is then routed to its owner.

For hijacking the target prefix's traffic from a given site, we simply advertised the prefix through all the four other sites. However, for interception, the traffic ought to be routed back to the owner. This is tricky since all our sites are effectively stub sites peering with providers and hence, all outgoing edges for the ISP emulated by our sites are customer-to-provider edges. Consequently, the existing route used by the ISP for the target prefix is bound to be a provider route. Also, the invalid route can only be advertised through a provider. As we detailed in section 2.2, this can lead to a routing instability impacting the ISP's existing route for the target prefix. Hence, we manually determined the optimal way of advertising the invalid route so that the ISP is still able to route the hijacked traffic to the designated owner.

We used recursive DNS nameservers across the Internet to generate actual traffic destined to the prefix. To this effect, we collected a list 23,858 of recursive nameservers belonging to 7,566 of the 18,391 routable ASes on the Internet (based on a BGP routing table obtained from the Route-Views repository). We also pointed the NS record for a domain name under our control (`prefix.anycast.guha.cc`) to point to an address in the prefix. Thus, a query for a name such as `query.prefix.anycast.guha.cc` to a nameserver in the aforementioned list causes it to send a DNS packet to our prefix and thus, allows us to probe our prefix from the nameserver. We loosely term the fraction of probes received at a given site as the "fraction of traffic" received at the site.

Ber	Pit	Sea	Ith	Ote	% of traffic Hijacked	% of traffic Intercepted
O	✗	✗	✓	✓	91.7	78.8
✗	O	✗	✓	✓	68.8	67.5
✗	✗	O	✓	✓	97.4	66.2
✗	✗	✗	O	✓	66.0	47.3
✓	✓	✓	✗	O	76.1	23.4

Table 3: Percentage of Traffic Hijacked and Intercepted. Each row corresponds to a scenario with one site acting as the prefix owner (O) and the four other sites emulating the Intercepting ISP – some of these sites advertise the invalid route (✓) while others don't (✗).

The probing methodology described above was used to measure the fraction of traffic that can be hijacked and intercepted from individual sites in our deployment. Table 3 shows these results. For our deployment, the fraction of traffic hijacked varies between 66% and 97.4% while the fraction of traffic intercepted varies between 23.4% and 78.8%. This, at the very least, provides anecdotal evidence that a significant fraction of traffic to prefixes on the Internet can be intercepted.

More importantly, our proof-of-concept implementation, as described below, represents one approach that ISPs might use to intercept traffic to a prefix with existing routers and routing framework. Given a target prefix, the hijacking AS can determine the next hop AS for its existing valid route to the target prefix - let this be the *preferred AS*. The routers of the hijacking AS that peer directly with the preferred AS and thus, receive valid BGP advertisements for the target prefix are left with unmodified configurations. All other routers are configured with static routes to send traffic destined to the target prefix to one of the unmodified routers. Also, these routers are configured to advertise this internal static route through BGP to the external routers they peer with (while satisfying the advertisement constraints discussed in section 2.2). This ensures that all neighbors of the hijacking AS receive a one AS-hop route to the target prefix while the hijacking AS can forward the hijacked traffic to the destination. All this can be achieved with standard management interfaces and tools used by ISPs today. Thus, intercepting traffic to a prefix in the Internet is almost as simple as hijacking it.

5. INTERCEPTION DETECTION

We wanted to determine if traffic to *any* prefix is being intercepted in the Internet today. Note that there has been work towards detecting prefix hijacks [3,15,18–21] and since the interception of a prefix necessarily involves hijacking it, these would seem to apply. However, they either look for anomalies in routing advertisements [15,18] and hop count changes [21] which are not effective for detecting ongoing interception or use fingerprinting to detect blackholing/redirec--tion of the hijacked traffic [20] and hence, would not work for prefix interception. Alternatively, MyASN [19] uses BGP updates collected at route-repositories and information provided by a prefix owner about the origin AS of the prefix to alert the owner of any attempts to hijack their prefix through

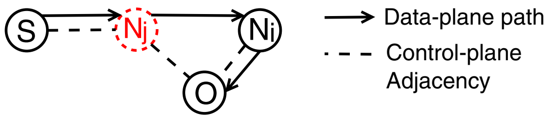


Figure 13: Next-hop Anomaly: a signature for Internet interception. Here, AS N_j uses fake advertisements to claim to be a next-hop for origin AS O and routes intercepted traffic for prefix p through AS N_i.

advertisements with an invalid origin. PHAS [3] is a similar service. These services are guided by the observation that it is the prefix owner that can authoritatively distinguish valid prefix advertisements from invalid ones [37] and hence, require proactive participation of prefix owners. Here we explore the possibility of detecting ongoing prefix interception in the Internet without pro-active participation by prefix owners.

Note that detecting interception (and hijacking) based solely on control plane information is not possible. For instance, a change in the origin AS for a prefix is a frequent occurrence in the Internet [3] and hence, a MOAS conflict cannot be used as an indicator of hijacking based on routes with an invalid origin. Guided by this observation, we attempted to use a combination of control-plane and data-plane information from a number of vantage points to detect interception scenarios in the Internet.

5.1 A Signature for Internet Interception

The key insight guiding our approach for interception detection is that the intercepting ISP relies on its existing route for the target prefix to send the prefix's traffic to its owner. Consider a prefix p with origin AS O and with next-hop ASes $N_1, \ldots, N_n$. Here, *next-hop AS* refers to an AS that appears next to O in the control-plane AS-level paths to p. Given this, in all likelihood, a packet destined to p that reaches AS N_j should be routed directly to the origin AS O. Thus, a data-plane trace wherein packets to p traverse AS N_i after traversing AS N_j (j≠i) would suggest that AS N_j is not a next-hop AS for prefix p and is advertising a route with an invalid next-hop to intercept the prefix's traffic. Figure 13 illustrates this scenario – we refer to such an occurrence as a *next-hop anomaly* and use it as a signature for interception on the Internet. The following sections detail our study of such anomalies in the Internet.

5.2 Data Sources

For control-plane information, we used the BGP routing tables collected at the Route-Views repository. This provides us with a view of the Internet's routing state from a total of 43 vantage points belonging to 34 distinct ASes. For the analysis on any given day, we used a routing table collected on that day to determine the set of next-hop ASes for each routable prefix.

For data-plane information, we use the traceroutes collected as part of the IPlane project [38]. This includes daily traceroutes to ≈100,000 routable prefixes from ≈200 PlanetLab nodes [39].[5] Thus, our data-set for each day of analysis comprised of ≈20 million IP-level traceroutes. We processed these traces to map the IP-level traceroutes to the corresponding AS-level traceroutes by mapping IP addresses to their origin ASes based on BGP routing tables.

	Oct 31	Nov 25	Dec 2	Dec 4
Anomalous Prefixes	5977	6125	4760	4904
Anomalous Clusters	834	749	545	619
After accounting for IP-to-AS mapping errors	440	392	306	348
After validation based on data-plane information	32	26	27	28
After validation based on *whois* information	11	11	10	12
After e-mail survey	9	11	10	11

Table 4: Number of next-hop anomalies at various stages of our analysis.

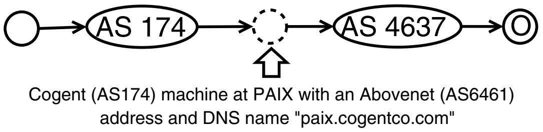

AS 174
AS 4637
O
Cogent (AS174) machine at PAIX with an Abovenet (AS6461)
address and DNS name "paix.cogentco.com"

Figure 14: Erroneous AS-level paths due to presence of IXP machines. Here, Next-Hop ASes for O = {6461, 4637}, Original AS-level Path = { .., 174, 6461, 4637, O} and Rectified AS-level Path = { .., 174, 4637, O}

.

5.3 Detecting Next-hop Anomalies

We used the AS-level traceroutes and the next-hop information extracted from the routing tables to determine instances of next-hop anomalies on four days in Oct-Dec, 2006. The number of prefixes for which we detected next-hop anomalies on each of these days are shown in the first row of table 4. To make the analysis of these anomalies more manageable, we clustered them using triples of the form $\{N_j, N_i, O\}$. Thus, anomalies involving the same next-hop ASes (N_j and N_i) and the same origin AS (0) were clustered as one. It is reasonable to assume that anomalies that are clustered together occur due to the same root-cause. The second row of table 4 displays the number of anomalous clusters on each day.

However, a majority of these anomalies are due to errors in IP-to-AS mappings based on BGP routing tables. These are similar to the errors that Mao et. al. [41] had to account for as part of their AS-level traceroute tool. A brief explanation of these error possibilities and how we accounted for them is given below:
(a). *Internet Exchange Points (IXPs)* refer to locations that host a number of ISPs who can, in turn, peer with each other on top of the IXP infrastructure. Since IXP-hosted machines are typically assigned addresses from address space of the IXP or one of the participating ISPs, this can lead to an additional AS along the data-plane AS-level path. If this additional AS happens to be a next-hop of the prefix being traced, the trace would be falsely flagged as being anomalous. Figure 14 illustrates a scenario at Palo Alto Internet Exchange (PAIX) using AS 6461's (Abovenet) address space that causes Abovenet to be erroneously flagged as an Intercepting ISP.

We detect such errors based on the DNS names of the IXP machines. In figure 14, the DNS name for the IXP machine suggests that it belongs to a participant ISP, AS 174 (Cogent). Consequently, the rectified data-plane AS-level path does not include AS 6461 and hence, is not anomalous.
(b). *Sibling ASes*: ASes from sibling organizations may share their address space and may also have cooperative routing arrangements. Thus, next-hop anomalies wherein the two

[5] Instead of traceroutes to all routable prefixes, the data set contains traceroutes only to one prefix in each BGP atom [40]. However, this suffices for the detection exercise.

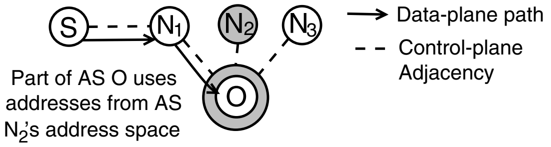


Figure 15: AS O uses part of its provider N_2's address space and this leads to erroneous AS-level paths. Here, Original AS-level Path = {S, N_1, N_2, O} and Rectified AS-level Path = {S, N_1, O}

next-hop ASes are sibling ASes should not be flagged as such. We achieve this by utilizing the similarity in the DNS names for IP hops in the two ASes, though in some cases we had to directly feed the sibling relationships to the analysis.
(c). *Using Provider Address space*: In many scenarios, an ISP will provide its customer with a small part of its address space that the customer ends up using for its peerings with others ISPs too. For instance, in figure 15, AS N_2 assigns its customer O with a part of the address space announced by it and is used by O for its peerings with N_1 and N_3 too. In this scenario, the AS-level path of packets routed to O from N_1 will include N_2 and will be erroneously flagged as a next-hop anomaly.

As before, we detect such errors based on the DNS names of the IP hops involved - the IP hops attributed to N_2 would have the same DNS name suffix as the IP hops belonging to O. In cases where the reverse name lookup for the IP hops in O failed, we looked for similarity between the DNS names of the IP hops attributed to N_2 and the AS name for O.

Thus, by utilizing ownership information encoded in DNS names and AS names we were able to account for almost all the IP-to-AS mapping errors in an automated fashion. The number of anomalous clusters after this step of the analysis are shown in the third row of table 4.

5.4 Anomalies due to Traffic Engineering

Apart from active interception by an ISP, a next-hop anom--aly may also result due to traffic engineering by the ASes involved. For instance, the data-path shown in figure 13 may arise if O is a stub-AS multihomed to two providers and is using one as its primary provider (AS N_i) while the other as a backup (AS N_j). As described below, such a primary-backup arrangement can be achieved using a number a techniques and some of these can result in next-hop anomalies.

First, the origin AS O may advertise the prefix p to provider N_i while advertising a less specific prefix that covers p to provider N_j. The more specific advertisement to N_i ensures its primary status. However, when determining the next-hop ASes for the destination being traced, we use only the routing table entries for the longest prefix that matches the destination address. Thus, with such specific advertisements, our analysis would consider only AS N_i as AS O's next-hop for prefix p and so the data-path shown in figure 13 would not be flagged as a next-hop anomaly.

Second, the origin AS O may use *AS-Path prepending* to advertise a longer path for prefix p to N_j than to N_i. This can lead to scenarios where a part of N_j chooses to route packets destined to p directly to O (and hence, it emanates a routing advertisement claiming to be a next-hop for O) while the rest of N_j routes the packets through N_i. Finally, a number of ISPs offer customers *community-attribute based control* over how their prefix advertisements are propagated by the ISP [42]. For instance, AS O may advertise prefix p to AS N_j and direct N_j to propagate this advertisement only to specific peers. As before, such inbound traffic control can result in different parts of N_j using different routes to p.

To account for traffic-engineering induced anomalies and any remaining mapping errors, we use the following tests to verify if AS N_j has direct data-path connectivity to origin AS O:
(a). We utilize the fact that our data-plane information for a given prefix includes probes from a large number of vantage points. If the trace from any of our vantage points indicates that AS N_j can indeed route packets for p directly to AS O, we have conclusive evidence that N_j is a next-hop AS for O and we assume that N_j cannot be an intercepting ISP for p. The fourth row of table 4 shows the number of anomalous clusters after validation of the anomalies based on data-plane information.
(b). Some ASes publish information about their peers and their route import/export policies as part of the *whois* registries. As before, a *whois* entry for AS O indicating that it peers with N_j would imply that N_j cannot be an intercepting ISP for p. The fifth row of table 4 shows the number of anomalous clusters after accounting for such *whois* information.

Thus, we were able to attribute a majority of the observed anomalies to traffic engineering by the origin. More importantly, the fact that the interception signature used here can also result from valid scenarios in the Internet implies that we have to rely on the prefix owners for conclusive evidence of interception. Consequently, for the remaining anomalies, we conducted an e-mail survey asking the prefix owner if they had a peering relation with the next-hop AS suspected of interception. We received only three responses; in all three cases the prefix owner was indeed peering with the next-hop AS in question.

5.5 Unexplained Anomalies

The analysis above yielded a total of thirteen distinct next-hop anomalies that were not explained by any of the heuristics described above. Interestingly, the *whois* entries for the origin ASes in five of the anomalies included information about the ASes they peer with and this did not include the next-hop AS suspected of interception. However, this could just be a result of the *whois* information being outdated.

Further, we manually inspected these anomalous traces and while they look like interception scenarios, we can just as well imagine them resulting from traffic engineering arrangements. These could also result from routing events that impact the link connecting the suspected next-hop AS and the origin AS. Since our control-plane information consists of a routing table snapshot on the same day as the trace, such a routing event is not captured in our next-hop calculations.

Overall, we are unable to conclusively classify any of the unexplained anomalies as actual prefix interception. Fundamentally, this is because other than observing the links traversed by the probes from our vantage points, there is no way for us to verify the data-plane adjacency of two ASes as claimed by the corresponding control-plane advertisements. However, this surely does not rule out ongoing prefix interception. For instance, our study focussed only on interception through advertisement of a route with an invalid next-hop. It is also possible for the intercepting ISP to pose as the origin AS or as an AS that is two or more hops away from the origin. Further, our study also makes a number of rather simplistic assumptions about the behavior of the intercepting ISP and hence, could have missed interception scenarios. For instance, we assume that the intercepting ISP does not manipulate the responses to traceroute-based probes to evade detection – something as a simple as the intercepting ISP configuring its routers to stop generating ICMP responses would defeat our detection. In spite of these limitations, we think that this simple attempt at detection highlights some of the challenges posed by the interception detection problem.

6. RELATED WORK

A lot of recent work has focussed on BGP security with particular emphasis on preventing the hijacking of prefixes. Some of these efforts use cryptography to secure BGP [7–13], while others propose new protocols [14], non-cryptographic additions to BGP [17] or rely on route characteristics [4,16] such as the stability of routes [4]. Wendlandt et. al. [43] argued that securing data delivery is more important than securing routing for secure communication. Our interception estimates show that communication confidentiality can be breached even when data delivery is secured. As discussed in section 5, there have also been efforts towards detecting prefix hijacks in the Internet [3,15,18–21].

The possibility of traffic interception by using invalid advertisements has been discussed by [22,24]. In recent work, Lad et. al. [44] estimate the impact of prefix hijacks through simulations across the Internet's AS-level topology. Such an approach allows them to evaluate the impact of hijacks by a much larger set of ASes than considered in this paper. On the other hand, by restricting ourselves to the ASes that contribute to the Route-Views repository, we observe each AS's actual route for any given prefix and don't need to simulate route propagation. As a matter of fact, the authors of [45] argue that it is difficult to accurately predict Internet routes through simulation over topologies where ASes are represented as nodes.

Apart from specification of attacks on BGP [46], past research has also shown the possibility of invalid advertisements resulting from misconfigurations [26,47]. Feamster et. al. [48] studied the presence of advertisements for unallocated prefixes in Internet routing. Ramachandran et. al. [23] analyzed the use of short-lived invalid routing advertisements by spammers.

7. DISCUSSION

The estimates in section 3 are based on ASes contributing to Route-Views. Further, the analysis itself relies on a rather simplistic model of Internet routing. For instance, the assumptions regarding routing preferences and the valley-free nature of routes don't always hold. The analysis does not account for special arrangements between ASes such as sibling ASes, mutual transit, etc. Also, ASes apply ingress-filters to restrict the prefixes that their neighbors can advertise to them. However, such filtering of advertisements varies greatly with the AS's size [49], relationship with the neighbor [27] and even the AS's location (for example, ASes in Europe are known to use filters aggressively [47]). Overall, a majority of the ASes struggle to maintain up-to-date filters or any filters at all [27,47,49]. More generally, the fact that these assumptions hold in the common case indicates that our estimates should closely reflect the actual amount of hijacking possible and this claim is fortified by our verification efforts.

It seems unlikely that an AS would intentionally hijack a prefix and then blackhole or redirect the hijacked traffic since this would impact the destination's connectivity and hence, would be immediately noticed. Misconfigurations or router compromises are more likely to lead to such an occurrence; to the best of our knowledge, this was the case for all prefix hijacking incidents reported in the past. In this context, it is important to note that our hijacking estimates implicitly assume that the hijacking AS advertises an invalid route to all its neighbors. However, by the very nature of BGP, both misconfigurations at and compromises of only a few (or even a single) well-placed routers can cause the ISP to advertise an invalid route to all of its neighbors and thus, our hijacking estimates capture an extreme yet realistic scenario.

The more interesting scenario is that of prefix interception since the hijacked traffic still reaches the destination. Consequently, it is less likely that an unsuspecting prefix owner would notice the interception which may have been going on for a long period. On the other hand, the presence of easily accessible route-repositories and router-servers implies that an informed prefix-owner can detect most interception attempts. Still, it wouldn't be a stretch to imagine ASes intentionally intercepting the traffic to a not-well-monitored prefix. For instance, this would (for good or for bad) ease lawful interception [50] since law enforcement agencies wouldn't necessarily need to go to different ISPs on a case-by-case basis.

In the past, ARP poisoning, DNS spoofing and other attack vectors have been proposed for man-in-the-middle (mitm) attacks in the Internet [51–53]. The increasing use of encryption for Internet communication would seem to alleviate the privacy concerns arising from such attacks. However, the use of a number of security protocols in the Internet leaves a lot to be desired and hence, the fact that traffic can be intercepted in the Internet does magnify the scope of the problem. For instance, launching a mitm attack on SSL through self-signed certificates leads to an "invalid certificate" warning on most browsers but these are often disregarded not just by common users [52] but by well-informed technical users too [53]. This and other social issues are compounded by technical problems such as frequent warnings resulting from multiple trusted authorities and even flaws in browsers that allow certificates to be forged and hence, allow for attacks where the user is not even warned [52]. All this suggests that even small ISPs that can intercept a small fraction of traffic from other ASes can cause a lot of damage.

8. CONCLUSION

This paper presents a study of Internet prefix hijacking and interception. We estimate that ASes higher up in the routing hierarchy can both hijack and intercept traffic to any prefix from a significant fraction (>50%) of ASes in the Internet. More surprising and perhaps more egregious is that even small ASes can hijack and intercept traffic from a non-negligible fraction of ASes. Further, we implemented the proposed interception methodology and used it for actually intercepting traffic to our prefix. Our experience suggests that it is indeed very simple for ASes to intercept traffic for prefixes within the existing routing set-up. Finally, we conducted a simple study to detect ongoing prefix interception. The study neither detected interception nor did it determine that there is no interception in the Internet; however, it did shed light on some of the issues involved in detecting prefix interception.

On a broader note, while our hijacking and interception estimates are (mostly) along expected lines, the notion of being able to intercept traffic in the Internet has far reaching implications for all aspects of Internet security, both at a technical level and a social level, and we hope that this paper will force a rethink on some of these issues.

Acknowledgements

We would like to thank the anonymous reviewers for their useful feedback. This work was partially supported by AFOSR under Award No. F49620-02-1-0233 and PA8750-05-C-0268 and by a grant from Intel.

9. REFERENCES

[1] "Nanog Mailing List," http://www.nanog.org/mailinglist.html.

[2] "7007 Explanation and Apology," Apr 1997, http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html.

[3] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, "PHAS: A prefix hijack alert system," in *Proc. of USENIX Security symposium*, 2006.

[4] J. Karlin, S. Forrest, and J. Rexford, "Pretty Good BGP: Improving BGP by Cautiously Adopting Routes," in *Proc. of ICNP*, 2006.

[5] T. Wan and P. C. van Oorschot, "Analysis of BGP Prefix Origins During Google's May 2005 Outage," in *Proc. of Security in Systems and Networks*, 2006.

[6] P. Boothe, J. Hiebert, and R. Bush, "Short-Lived Prefix Hijacking on the Internet," NANOG 36 meeting, 2006, http://www.nanog.org/mtg-0602/pdf/boothe.pdf.

[7] Y.-C. Hu, A. Perrig, and M. Sirbu, "SPV: secure path vector routing for securing BGP," in *Proc. of ACM SIGCOMM*, 2004.

[8] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (S-BGP)," *IEEE Journal on Selected Areas in Communication*, vol. 18, no. 4, 2000.

[9] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. Katz, "Listen and whisper: Security mechanisms for BGP," in *Proc. of USENIX/ACM NSDI*, 2004.

[10] T. Wan, E. Kranakis, and P. van Oorschot, "Pretty Secure BGP, psBGP," in *Proc. of NDSS*, 2005.

[11] R. White, "Architecture and Deployment Considerations for Secure Origin BGP (soBGP)," draft-white-sobgp-architecture-01, Nov 2005.

[12] W. Aiello, J. Ioannidis, and P. McDaniel, "Origin authentication in interdomain routing," in *Proc. of conference on Computer and communications security (CCS)*, 2003.

[13] B. Smith and J. Garcia-Luna-Aceves, "Securing the Border Gateway Routing Protocol," in *Proc. of Global Internet*, 1996.

[14] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel, and A. Rubin, "Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing," in *Proc. of NDSS*, 2003.

[15] C. Kruegel, D.Mutz, W. Robertson, and F. Valeur, "Topology-based Detection of Anomalous BGP Messages," *LNCS*, 2003.

[16] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "Protecting BGP Routes to Top Level DNS Servers," in *Proc. of ICDCS*, 2003.

[17] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "Detection of Invalid Routing Announcement in the Internet," in *Proc. of DSN*, 2002.

[18] S. T. Teoh, K. Zhang, S.-M. Tseng, K.-L. Ma, and S. F. Wu, "Combining visual and automated data mining for near-real-time anomaly detection and analysis in BGP," in *Proc. of ACM workshop on Visualization and data mining for computer security*, 2004.

[19] "RIPE MyASN service," http://www.ris.ripe.net/myasn.html.

[20] X. Hu and Z. M. Mao, "Accurate Real-time Identification of IP Prefix Hijacking," in *Proc. of IEEE Security and Privacy (Oakland)*, 2007.

[21] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis, "A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Realtime," in *Proc. of ACM SIGCOMM*, August 2007.

[22] O. Nordstrom and C. Dovrolis, "Beware of BGP attacks," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, 2004.

[23] A. Ramachandran and N. Feamster, "Understanding the Network-Level Behavior of Spammers ," in *Proc. of ACM SIGCOMM*, 2006.

[24] J. Kim, S. Y. Ko, D. M. Nicol, X. A. Dimitropoulos, and G. F. Riley, "A BGP Attack Against Traffic Engineering," in *Proc. of WSC*, 2004.

[25] "Route Views Project Page," May 2006, www.route-views.org.

[26] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "An analysis of BGP multiple origin AS (MOAS) conflicts," in *Proc. of ACM SIGCOMM IMW*, 2001.

[27] C. Labovitz, A. Ahuja, R. Wattenhofer, and V. Srinivasan, "The Impact of Internet Policy and Topology on Delayed Routing Convergence," in *Proc. of IEEE INFOCOM*, 2001.

[28] F. Wang and L. Gao, "On Inferring and Characterizing Internet Routing Policies," in *Proc. of ACM SIGCOMM conference on Internet measurement*, 2003.

[29] "BGP Best Path Selection Algorithm," July 2006, http://www.cisco.com/warp/public/459/25.shtml.

[30] L. Gao, "On Inferring Autonomous System relationships in the Internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, 2001.

[31] B. Huffaker, "CAIDA AS Ranking Project," July 2006, http://www.caida.org/analysis/topology/rank_as/.

[32] "Tier 1 network - Wikipedia entry," July 2006, http://en.wikipedia.org/wiki/Tier_1_network.

[33] J. Rexford, J. Wang, Z. Xiao, and Y. Zhang, "BGP routing stability of popular destinations," in *Proc. of Internet Measurment Workshop*, 2002.

[34] "Alexa Top Sites," http://www.alexa.com/site/ds/top_sites?ts_mode=global.

[35] A. Ma, "CAIDA AS Relationships," July 2006, http://www.caida.org/data/active/as-relationships/.

[36] "Quagga Routing Suite," Apr 2006, http://www.quagga.net/.

[37] G. Huston, "Auto-Detecting Hijacked Prefixes?" RIPE 50 meeting, 2005, http://www.ripe.net/ripe/meetings/ripe-50/presentations/index.html.

[38] H. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani., "iPlane: An Information Plane for Distributed Services," in *Proc. of OSDI*, 2006.

[39] B. Chun, D. Culler, T. Roscoe, A. Bavier, L. Peterson, M. Wawrzoniak, and M. Bowman, "PlanetLab: An Overlay Testbed for Broad-Coverage Services," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 3, July 2003.

[40] A. Broido and kc claffy, "Analysis of RouteViews BGP data: policy atoms," in *Proc. of network-related data management (NRDM) workshop*, 2001.

[41] Z. M. Mao, J. Rexford, J. Wang, and R. H. Katz, "Towards an accurate AS-level traceroute tool," in *Proc. of ACM SIGCOMM*, 2003.

[42] "SprintLink's BGP Policy," May 2006, http://www.sprintlink.net/policy/bgp.html.

[43] D. Wendlandt, I. Avramopoulos, D. G. Andersen, and J. Rexford, "Don't Secure Routing Protocols, Secure Data Delivery," in *Proc. of workshop on Hot Topics in Networks*, 2006.

[44] M. Lad, R. Oliveira, B. Zhang, and L. Zhang, "Understanding Resiliency of Internet Topology Against Prefix Hijack Attacks," in *Proc. of IEEE/IFIP DSN*, 2007.

[45] W. Mühlbauer, A. Feldmann, O. Maennel, M. Roughan, and S. Uhlig, "Building an AS-topology model that captures route diversity," in *Proc. of ACM Sigcomm*, 2006.

[46] S. Convery, D. Cook, and M. Franz, "An Attack Tree for the Border Gateway Protocol," draft-convery-bgpattack-01, July 2001.

[47] R. Mahajan, D. Wetherall, and T. Anderson, "Understanding BGP misconfiguration," in *Proc. of ACM SIGCOMM*, 2002, pp. 3–16.

[48] N. Feamster, J. Jung, and H. Balakrishnan, "An empirical study of "bogon" route advertisements," *SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 1, 2005.

[49] N. Feamster and H. Balakrishnan, "Detecting BGP Configuration Faults with Static Analysis," in *Proc. of Symp. on Networked Systems Design and Implementation (NSDI)*, 2005.

[50] F. Baker, B. Foster, and C. Sharp, "RFC 3924 - Cisco Architecture for Lawful Intercept in IP Networks," Oct 2004.

[51] "Content Verification - Man in the Middle Attack," Jan 2007, http://www.contentverification.com/man-in-the-middle/index.html.

[52] "Mattias Eriksson, An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions," Jan 2007, http://www.cs.umu.se/education/examina/Rapporter/MattiasEriksson.pdf.

[53] K. Fujiwara, "DNS Process-in-the-middle Attack," ICANN Presentation, 2005, http://www.icann.org/presentations/dns-attack-MdP-05apr05.pdf.