Stealthy IP Prefix Hijacking: Don't Bite Off More Than You Can Chew

Christian McArthur
Department of Computer Science
Texas State University-San Marcos
San Marcos, Texas, U.S.A.
christian@cs.txstate.edu

Mina S. Guirguis
Department of Computer Science
Texas State University-San Marcos
San Marcos, Texas, U.S.A.
msg@txstate.edu

Categories and Subject Descriptors

C.2.2 [**Computer-Communications Networks**]: Network Protocols—*Routing Protocols*

General Terms

Security

Keywords

BGP; Prefix Hijacking; Routing

Introduction and Motivation: The potential of prefix hijacking poses an ongoing threat to any Autonomous System (AS). In prefix hijacking, an AS advertises invalid BGP routes for prefixes that are owned by another AS, so that the traffic intended for the real owner is hijacked and received by the attacker. Regardless of the intent behind the hijack, we will refer to the AS sending out invalid advertisements as the "attacking AS" and the owner as the "victim AS".

One of the latest incidents occurred on February 24, 2008, when Pakistan Telecom advertised a prefix that belonged to YouTube and caused traffic to YouTube to be diverted to Pakistan [5]. While this hijacking was unintentional, it highlights the potential damaging effects should a devious individual(s) desire to intentionally hijack a prefix.

Previous research into prefix hijacking has focused on invalid origin and invalid next hop attacks [1, 3]. Their research confirmed that an attacker could potentially affect a large number of ASes on the Internet. But, what if the attacker's goal is not to maximize the number of affected ASes, but rather impact a smaller number of ASes, so that (1) the attacker can handle the amount of hijacked traffic (for phishing, recording, rerouting) and (2) the victim would not observe a sharp drop-off in its incoming traffic that would raise an alarm? Indeed, such an attack can result in longer periods of hijacking traffic that can be potentially more damaging than hijacking traffic from the majority of ASes for a shorter period of time (until detected and mitigated).

In this work, we explore a new class of prefix hijacking attacks that is stealthy in nature. We aim to answer the following questions:

1. How can an attacker construct a stealthy prefix hijacking that does not affect the majority of the Internet?
2. How much control does an attacker have in tuning the effects of its attack?
3. How much traffic (in bytes) can really be hijacked?
4. How can a skilled attacker avoid detection by current methods other than just looking at the victim's traffic?

SIGCOMM'08, August 17–22, 2008, Seattle, Washington, USA.
ACM 978-1-60558-175-0/08/08.

How to Carry Out a Stealthy Prefix Hijacking? In order to perform a successful stealthy prefix hijacking, the BGP advertisements should have a small impact on the Internet. To do so, the attacker advertises an invalid route for the victim's prefix that has a longer path length than what may be preferred by the majority of ASes. In particular, the exact length should be *long enough so that its effects will not be noticed by the victim's administrators, yet short enough to attract a fraction of the traffic intended for the victim.*

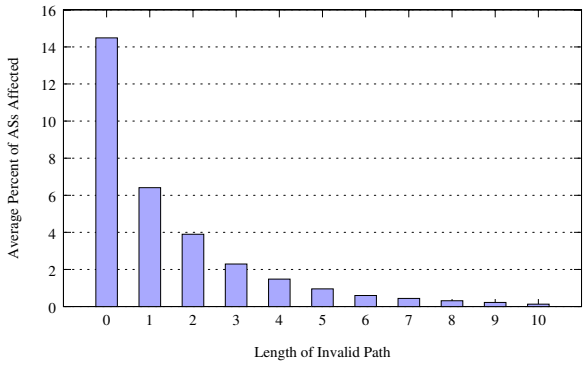

Figure 1: Average effects of a single stealthy attack.

How Many ASes Can Be Affected? To assess the impact of stealthy prefix hijacking attacks, we utilized BGP advertisements provided by Route-Views [6]. These views were combined to create a tree of AS paths for every prefix seen by the observer routers. We analyzed the effects of varying the lengths of the invalid advertisements on the number of ASes that would be tricked into believing those invalid advertisements. Figure 1 shows our results. As an attacker announces longer routes, fewer ASes are effected on average. We are particularly interested in the cases where the length of the invalid path is longer than 2, since they raise less attention. Notice that these results do not translate directly into amounts of hijacked traffic since different ASes have different characteristics in terms of the bytes they produce/carry. Part of this work is to infer those values. Our initial results show a "heavy-tailed" like distribution of bandwidth capacities across ASes. This means that an attacker, in the general case, would have more chances of impacting ASes that carry low volume of traffic than a high volume of traffic and would be able to tune the effects of its attack.

Fakeroute and Defeating Detection Methods: Current detection methods rely on traceroute to detect hijacking attacks [2,4,7]. To defeat those methods, we have created a tool, "fakeroute", that intercepts traceroute requests and falsifies its replies. *Before* the attacker hijacks a prefix, it does a traceroute to the intended victim to learn about the ASes, routers and timing information along the legitimate path. Fakeroute uses this information to respond with the IP addresses (via spoofing the source IPs) and round-trip times (via adding the appropriate delay) of the legitimate routers, after the hijacking occurs. Responses from fakeroute could not be differentiated from legitimate responses.

Illustrative Examples: There have been several proposals on detecting prefix hijacking attacks. For the purpose of this work, we will only focus on the most relevant ones that are likely to catch stealthy attacks. First, we will illustrate how these methods detect prefix hijacking attacks, and then we show how a skilled attacker using fakeroute could defeat them. We will evaluate the effectiveness of those methods using a real AS tree for Texas State (being the victim).

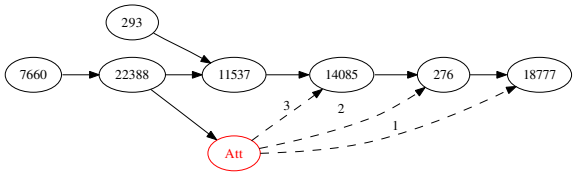

Figure 2: AS Tree with Attack Scenarios.

Figure 2 shows a partial representation of an AS tree for Texas State (AS 18777). It also shows three possible hijacking scenarios. The attacker establishes a peering relationship with AS 22388 and announces a path to Texas State's prefix through AS 14085 (scenario 3), AS 276 (scenario 2), or AS 18777 (scenario 1). In scenarios 1 and 2, traffic from AS 22388 and AS 7660 destined to Texas State will be routed to the attacker. In scenario 3, since both the legitimate path and the attacker's path have the same length, the effects are determined based upon local policies at AS 22388.

Table 1: Traceroute & BGP Paths

Figure 2 Scenario 2	
BGP Paths to the Victim	
Before Attack	7660 - 22388 - 11537 - 14085 - 276 - 18777
After Attack	7660 - 22388 - Att - 276 - 18777
TraceRoute Paths to the Victim	
Before Attack	7660 - 22388 - 11537 - 14085 - 276 - 18777
After Attack	7660 - 22388 - ATT - 276 - 18777
Falsifying Hop Count	7660 - 22388 - ATT - ATT - ATT - 276 - 18777
Falsifying Entire Path	7660 - 22388 - 11537 - 14085 - 276 - 18777
TraceRoute Paths to the Reference Point	
Before Attack	7660 - 22388 - 11537 - 14085 - 276 - 18777
After Attack	7660 - 22388 - 11537 - 14085 - 276 - 18777

Changes in Hop Count: The detection method proposed in [7] periodically performs traceroute requests to prefixes and compares the number of hops with previous results. Whenever there is a significant change in the number of hops, an alarm is raised. Scenarios 1 and 2 in Figure 2 will raise alarms. However, with the use of fakeroute by the attacker, the number of hops will not differ during an attack as indicated by "Falsifying Hop Count" in Table 1.

Traceroute Path Disagreement: The authors of [7] also provide a detection method that relies on comparing a possible route to the victim with another route to a reference point. The reference point is chosen to be as close as possible to the victim, yet outside the victim's prefix. For example, in Figure 2, if a monitor was located in AS 7660, a traceroute to Texas State, AS 18777, would go through the attacker's AS. However, a traceroute to an IP in AS 276 would take a very different path. This can be seen in Table 1. Thus, all scenarios in Figure 2 will raise an alarm. Once again, through the use of fakeroute, the entire path can be falsified as indicated by "Falsifying Entire Path" in Table 1.

AS Traceroute: AS Traceroute [4] takes traditional traceroute listings of routers and maps the routers' IP addresses into the corresponding AS numbers. To detect prefix hijacking, the AS traceroute path is compared to the BGP routing data for any discrepancies [2]. In our scenarios, the announced BGP route will match the AS traceroute response, so no alarm will be raised.

Detecting Stealthy Prefix Hijacking Attacks: We believe that combining the traceroute path disagreement method with the AS Traceroute tool would effectively detect stealthy prefix hijacking. In order to avoid having discrepancies between the hijacked path and the BGP route, the attacker must provide a traceroute path in which the IPs of the routers translate into AS numbers that match the BGP route. The path "Falsifying Hop Count" shown in Table 1 illustrates an AS traceroute version matching the BGP announcement. However, if this route is compared to the route to the reference point there will be discrepancies suggesting a possible hijacking. If the attacker uses fakeroute to respond with a path that would match the route to the reference point, the AS traceroute path would then disagree with the BGP announcement. Therefore, by combining these two methods, path disagreement with a reference point and mapping the IP traceroute to the BGP route, stealthy prefix hijacking attacks are detected.

Ongoing Work: We are currently investigating different classes of attacks that tend to give more control in tuning the effects of attacks (multi-homed attackers, attackers that hijack traffic from a *particular* AS that is destined to the victim, *etc*). We are also interested in inferring the amounts of traffic that can be possibly hijacked.

REFERENCES

[1] H. Ballani, P. Francis, and X. Zhang. A Study of Prefix Hijacking and Interception in the Internet. In *Proceedings of SIGCOMM*, Kyoto, Japan, Aug 2007.

[2] X. Hu and Z. M. Mao. Accurate Real-time Identification of IP Prefix Hijacking. In *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May 2007.

[3] M. Lad, R. Oliveira, B. Zhang, and L. Zhang. Understanding Resiliency of Internet Topology against Prefix Hijack Attacks. In *Proceedings of DSN*, Edinburgh, UK, Jun 2007.

[4] Z. Mao, J. Rexford, J. Wang, and R. Katz. Towards an Accurate AS-level Traceroute Tool. In *Proceedings ACM SIGCOMM*, karlsruhe, Germany, Aug 2003.

[5] RIPE. YouTube Hijacking: A RIPE NCC RIS case study. web: http://www.ripe.net/news/study-youtube-hijacking.html.

[6] RouteViews. University of Oregon Route Views Page. web: http://www.routeviews.org.

[7] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis. A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Realtime. In *Proceedings of SIGCOMM*, Kyoto, Japan, Aug 2007.