Analysis of IP Prefix Hijacking and Traffic Interception

Khin Thida Latt, Yasuhiro Ohara, Satoshi Uda and Yoichi Shinoda

Japan Advanced Insitute of Science and Technology, Ishikawa, 923-1292 Japan

Summary
In the Internet, BGP is de facto inter-domain routing protocol. And it is vulnerable to a number of damaging attacks. Among these attacks, IP prefix hijacking and traffic interception are regarded as the serious threats in the Internet. There have been many incidents of IP prefix hijacking in the Internet. The hijacking AS can blackhole the hijacked traffic by introducing network unreachability problem. Alternatively, it can transparently intercept the hijacked traffic by forwarding it onto the owner. Although there is no reported incident about traffic interception yet, it cannot be said that there was no such attack in the Internet. Because traffic interception does not introduce any network unreachability problem and it is transparent to the victim. Many ideas have been presented to try to detect or prevent prefix hijacking. However, there is no enough analysis towards both areas. This paper makes analysis of IP prefix hijacking and traffic interception for a stepping-stone towards solving these two threats. In this paper, we survey IP prefix hijacking incidents and we present the analysis of IP prefix hijacking and traffic interception.

Key words:
Hijacking, Interception, BGP, Routing

1. Introduction

The goal of our work is to provide the comprehensive analysis to detect IP prefix hijacking and traffic interception in inter-domain routing. The de facto standard inter-domain routing protocol is Border Gateway Protocol (BGP) [2] and the Internet relies on it to exchange network reachability information. BGP route update consists of a particular prefix and associated AS_PATH to get to that prefix.

Due to unintentional router mis-configurations or intentional malicious attacks, IP prefix hijacking happens if an AS makes an advertisement of invalid AS_PATH or a prefix that it does not own. It becomes an attack on the routing infrastructure or the control plane of the Internet.

BGP has no mechanism to authenticate such invalid advertisements since it assumes a significant level of trust among BGP peering ASes. Therefore, such invalid advertisements can quickly spread to the Internet and it leads to some BGP routing tables install invalid routes. Subsequently the victim (i.e., the prefix owner) will experience severe performance degradation or security threat. As an attack against performance, a malicious AS can hijack a prefix and launch denial-of-service attack by black-holing all hijacked traffic [4]. As an attack against security, after hijacking the prefix, malicious AS can also launch Man-in-the-Middle attack by forwarding the hijacked traffic back to the real destination.

There are many proposals to protect or detect the unauthorized invalid advertisements such as IP prefix hijacking. However, there are still open problems. Even the recent good proposals such as [17] and [3] do not give the complete view. [17] provides a comprehensive classification of prefix hijacking scenarios. However the classification and attack model for traffic interception are not included. In [3], it analyzes the possibilities that an AS can conduct hijacking and intercepting the traffic. It mainly focuses on only an attack type referred to as “regular prefix hijacking and interception as invalid origin”. However, for example, the attack type called “invalid transit” is not discussed in that work.

As related with IP prefix hijacking, the research community proposes a number of ideas to address this attack. Some of them targets to detect prefix hijack attempts while others strive to improve the general security of inter-domain routing. Many ideas have been presented to try to detect or prevent prefix hijacking. However, there is no enough analysis towards both areas. To detect the attacks, we need to understand and analyze how the attacker manipulates BGP i.e attacker’ s behaviors and methods. The comprehensive analysis provides the foundation to detect IP prefix hijacking and traffic interception. Moreover, analysis of the attacks shows the hints towards detection and hence it is a stepping-stone towards solving these problems. Motivated by this, in this paper, we present an analysis of IP prefix hijacking and traffic interception.

To make analysis, we surveyed and studied the hijack incidents happened in the past (from 1997 to 2009) and explored the characteristics of each attack. According to the characteristics, we describe the attack models and IP prefix hijacking and Traffic Interception. Along with these models, we classify each attack type. Then we thoroughly analyze and explore the characteristics and nature of each attack type.

In summary, in this paper, we present the analysis of IP prefix hijacking and traffic interception. Our main

Manuscript received July 5, 2010
Manuscript revised July 20, 2010

contributions are 1) survey of IP prefix hijacking incidents 2) identification of possible attack models and 3) their analysis.

2. Related Work

There are many proposals to protect or detect IP prefix hijacking and traffic interception. Those proposals can be classified into four groups.

The first group requires public key infrastructure so that routing updates can be cryptographically verified [37-42]. They include S-BGP [37], soBGP [38], psBGP[39], Securing BGP [40], SPV [41] and Origin Authentication [42].

The second group, [44,45,51] proposed non-cryptographic schemes. However approaches in both first and second are not easily deployable because of requiring changes to routing protocol, router software, router configuration or network operations.

Third group proposals such as [12,34,48-50] focus on passive monitoring to detect anomalies on BGP routes (called "control plane information"). In this group, there are well-known detection systems. IAR [62] used the methods described in PG-BGP [27] to identify advertised routes that are potentially bogus. This method uses route history information to determine prefix ownership, as opposed to using stale registry data. When any invalid origin AS appears, RIPE MyASN project [59] triggered an alarm to the prefix owner for registered valid origin set for a prefix. PHAS [12] also provides notification of origin AS changes via email to the owners of individual prefixes. The prefix owners identify real hijack alerts and filter out normal origin changes. Although anomaly detection approaches can be incrementally deployed, they suffer from false positives or negatives. The reason is that legitimate route changes cannot be distinct from hijacking.

Fourth group [3,6,17,52,53] utilize forwarding plane information together with control plane information. Among them, [6] relies on real-time data i.e., it does not rely on any BGP feeds.

However, above mentioned works focus on how to prevent or detect a certain attack type of IP prefix hijacking. And approaches in all groups cannot identify traffic interception.

This paper targets to capture the whole picture of IP prefix hijacking and traffic interception by providing thorough analysis.

3. Analysis of IP Prefix Hijacking

IP prefix hijacking leads to DoS attack against prefix owner. As brand spoofing or phishing, a malicious AS can impersonate the prefix to steal confidential information by redirecting the traffic to a compromised environment [4]. It is mentioned in [5] that spammers often use hijacked IP prefix from which they send spam emails and launch DDoS attacks from the hijacked prefix [6]. [7] said that there are some spammers that hijack the prefixes and use those for malicious purpose and when these address blocks are blacklisted, hijacked prefixes are found to be entirely or partly sold or leased to other companies. Besides malicious attempt, unintentional network misconfigurations can also lead to prefix hijacking [8].

We describe, in Section 3.1, what IP prefix hijacking is, in Section 3.2, IP prefix hijacking incidents, in Section 3.3, attack models, Section 3.4, its classification and in Section 3.5, its analysis.

3.1 What is IP Prefix Hijacking?

IP prefix hijacking is shown in Figure 1. In the Figure, AS 1 is the origin AS and it owns IP prefix *p*. AS 2 and AS 1 have a provider-customer[1] relationship in which AS 2 is provider and AS 1 is the customer. AS 3 is the provider of AS 2 and AS 4. And malicious AS 5 has peer relationship[2] with AS 3. AS 4 has two providers which are AS 3 and AS 5.

In this simple topology, AS 1 sends BGP route update which advertise prefix *p* to its provider AS 2. The resultant AS_PATH is [1]. When AS 2 passes this route to AS 3, it prepends its own AS number in the AS_PATH which results in [2,1] and when AS 3 passes that route to AS 4 and AS 5, it does prepending its own AS numbers accordingly. Now every AS in the topology knows how to get to the prefix *p* which belongs to AS 1. When AS 4 wants to send the traffic to AS 1, it chooses AS 3 of its two providers according to AS_PATH [3,2,1] it has. And through AS 3 and AS 2, the traffic finally reaches to AS 1.

However, malicious AS 5 sends invalid route update to AS 4. The invalid route update says that AS 5 owns the prefix *p* and it adds its AS number into the AS_PATH. Although this route is invalid, AS 4 prefers this route because AS_PATH [5] is shorter than original valid one [3,2,1] and it takes that route. When AS 4 sends traffic to prefix *p* using that invalid route, the traffic goes to AS 5 and it encounters unreachability to AS 1 which we refer as “blackhole”.

[1] A customer pays its provider for connectivity to the rest of the Internet. Therefore, a provider does transit traffic for its customers. However, a customer does not transit traffic between two of its providers.

[2] A pair of peers agree to exchange traffic between their respective customers free of charge. A mutual-transit agreement allows a pair of administrative domains to provide connectivity to the rest of the Internet for each other.

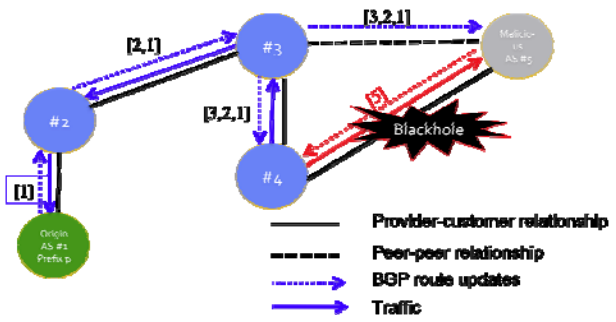

Figure 1: IP Prefix Hijacking

3.2 IP Prefix Hijacking Incidents

We surveyed the real incidents happened from 1997 to 2009 which were reported in NANOG. Table 1 describes these incidents along with the dates, victim ASes and their impacts.

Table 1: Prefix Hijack Incidents from 1997 to 2009 that have been reported to NANOG mailing list

No	Date	Description
1	April 1997	Wow, AS 7007! AS 7007 announces a large number of network prefixes [8].
2	April 1998	AS8584 taking over the internet By a mistake, AS 8584 announced loads of prefixes that others own [11].
3	Dec. 1999	Short Take: AT & T WorldNet suffers outage- leaving 1.8 million customers without Web access for most a day. An Internet Service Provider made a network change that caused the public Internet to have incorrect information on how to reach AT & T WorldNet servers. The impact was nationwide in scope and affected AT & T's Worldnet Service, Business IP Dial Service, and portions of its Virtual Private Network service [55].
4	April 2001	C & W routing instability AS 3561, AS 15412 was involved in 5532 out of 6627 MOAS conflicts during a day [15]. Based on archived data from [1], AS 15412 normally originates only 5 prefixes. However, on April 6th, AS 15412 suddenly originated thousands prefixes due to a configuration error [16].
5	Dec 2004	Christmas Eve Leak 106K+ routes were leaked from AS9121 (TTnet) and globally propagated. It resulted in blackholing tens of thousands of networks and it was serious global vulnerability[21].
6	Dec 2004	Estonian ISP announced a part of Merit address space [22].
7	Sept 2004	12.0.0.0/8 Prefix Anomaly AS26210 (AES Communications Bolivia S.A.) started announcing 12/8 in addition to AS7018 (ATTW AT ¥&T WorldNet Services) [26].
8	Jan 2006	Con-Ed Steals the 'Net' Con Edison (AS27506), probably by a mistake, originated several prefixes that others own. It leaded to outages for Panix(AS 2033) and many networks. Verio (AS2914) adopted and forwarded invalid routes to other ASes since information in internet routing registry is not up-to-date[13,14].
9	Feb. 2006	Sprint and Verio briefly announced that TTNET (AS9121) was the origin AS for 4/8, 8/8, 12/8 [27,54].
10	May 2007	Two weeks shutdown of all banking, government and political sites in Estonia [23-25].
11	Deb 2008	Youtube IP hijacking! Pakistan Telecom (AS17557) announced 208.65.153.0/24 from YouTube (AS36561). PCCW Global (AS3491) propagates nnouncement. Routers around the world receive nnouncement, and YouTube traffic is redirected to Pakistan [20,28,29].
12	March 2008	Kenyan Route Hijack An ISP from USA and Europe, AboveNet (AS 6461) hijacked prefix owned by Africa Online (AS 36915)[30].
13	Sept 2008	Prefix Hijack by ASN 8997 It looks like that OJSC North-West Telecom" in Russia (ASN8997) leaked full table [31].
14	Nov 2008	Potential Prefix Hijack by Brazil AS Companhia de Telecomunicacoes do Brasil Central (AS16735) announced almost the whole Internet to two of its peers CTBC Multimedia (AS 27664) 174213 routes and Nic.br(AS 22548) 111231 routes. IP prefixes Hijacking by AS16735 was not globally propagated and some AS16735's customers (like AS27664 and AS22548) were affected [32].
15	Jan 2009	Massive routes hijack at AS48400, up to 6000 AS affected? AS48400 multi-homed to two different ISPs announced various prefixes it had. This incident seemed to be ordinary route leak [33].

3.2 Attack Models of IP Prefix Hijacking

For simplicity, we refer malicious AS or attacker AS as ***X*** and prefix owner AS or victim AS as ***V***.

X can hijack a prefix by manipulating AS_PATH attributes of BGP update message. The AS_PATH attribute is actually the list of AS numbers that a route has traversed in order to reach a destination. The originating AS shall include its own AS number in the AS_PATH attribute of all BGP update messages sent to BGP speakers located in neighboring ASes. Whenever this route update passes through an AS, the AS number is prepended to that update. Generally the last hop of AS_PATH presents the origin AS of network prefix and other hops are the transit ASes through which the traffic reach to origin AS. ***X*** can manipulate origin AS or transit ASes of AS_PATH as follows.

3.2.1 IP Prefix Hijacking as Invalid Origin

Making an invalid route advertisement of an IP prefix that ***V*** owns, ***X*** claims that it is the origin AS of that prefix and sets its AS number in the last hop of AS_PATH as follows.

- Valid AS_PATH =[***V***]
- Invalid AS_PATH =[X]

3.2.2 IP Prefix Hijacking as Invalid Transit

Making an invalid route advertisement of an IP prefix, ***X*** claims that it is one of the transit ASes to get to prefix of ***V*** and sets its AS number in AS_PATH as follows.

- Valid AS_PATH =[... , ... , ... , ***V***]
- Invalid AS_PATH =[... , ... , ***X***, ... , ***V***]

X can hide one or more transit ASes[3] from valid AS_PATH to make AS_PATH shorter because shorter AS_PATH are generally preferred by most ASes.

3.3 Classification of IP Prefix Hijacking

Using one of two ways described in Sections 3.2.1 and 3.2.2, ***X*** can hijack a particular destination prefix, carried in NLRI[4] field, which is as exactly same as already routable one or more or less specific as follows.

- regular prefix hijacking
- sub prefix hijacking
- super prefix hijacking

3.3.1 Regular Prefix Hijacking

To hijack an exactly same prefix that ***V*** owns, ***X*** makes the invalid route advertisement claiming that it is either owner of the prefix (Invalid Origin) or it is one of the transit ASes (Invalid Transit).

3.3.2 Sub Prefix Hijacking

To hijack more specific prefix than the one being advertised by ***V***, ***X*** makes the invalid route advertisement claiming that it is either owner of the prefix (Invalid Origin) or it is one of the transit ASes (Invalid Transit). For example, ***X*** hijacks a /24 subnet; which is a subset of /16 prefix announced by ***V***.

3.3.3 Super Prefix Hijacking

To hijack less specific prefix than the one being advertised by ***V***, ***X*** makes the invalid advertisement claiming that it is either owner of the prefix (Invalid Origin) or it is one of the transit ASes (Invalid Transit). This kind of hijacking is very less attractive because it is possible only when the route to the valid prefix is withdrawn [12].

3.4 Analysis of IP Prefix Hijacking

In this section, we present the analysis of regular and sub prefix hijacking as Invalid Origin and Invalid Transit types and hijacking unused but allocated address space.

3.4.1 Analysis of Regular Prefix Hijacking as Invalid Origin

This type of attack leads to Multiple Origin AS (MOAS) conflict [15] as the same prefix appears to originate from more than one AS i.e., same prefix seems to be owned by multiple ASes. MOAS conflicts can be the result of misconfiguration or hijacking attacks. However, such conflicts also occurs due to valid reasons such as traffic engineering practices at some ISPs, IXP (Internet Exchange Points) addresses, multihoming without BGP or with private AS numbers. Because of these issues, it is difficult to distinguish hijacking route from legitimate ones. If ***V*** uses monitoring services or MOAS-based hijack detection systems, notification email will be sent to ***V*** when suspicious route (possibly legitimate route) in which prefix is same but origin AS is not ***V***, is found. In this way, differentiating hijacking and legitimate routes are done in manual at prefix owner sites.

3.4.2 Analysis of Regular Prefix Hijacking as Invalid Transit

This type of attack does not produce MOAS conflict as ***X*** appears as a transit. [17] argues that this type of attack increases AS_PATH length and this may cause the hijacking route not chosen by some routers. However, X can still hide some hops between itself and ***V*** to make AS_PATH length shorter.

To detect this kind of attack, control plane-based hijack detection systems use passive monitoring mechanisms. In one of such systems [36], besides the prefixes, ***V*** explicitly registers its peers and upstream ASes. It means that AS_PATH in any update should match the registered AS_PATH. For example, as shown in Figure 2, the prefix 150.65.0.0/16 belongs to AS 17932 (JAIST).

---

[3] ***X*** may even hide its AS number in AS_PATH. However ASes adjacent to ***X*** can determine hidden AS number via NEXT_HOP address.

[4] In BGP UPDATE message, the Network Layer Reachability Information (NLRI) field carries the destination IP prefixes. These prefixes are usually announced either by ***V*** itself if it runs BGP and has an AS number; or by its upstream provider AS(es).

There are two upstream providers for that prefix and these are AS 2907 (SINET) and AS 2500 (WIDE-BB). So AS_PATHs [2907, 17932] and [2500, 17932] can be defined. Let's say one of these two AS_PATHs should be the tail of any AS_PATH for the traffic destined to prefix 150.65.0.0/16. In a particular route update, says [..., X, 17932], if ***X*** is out of the set of registered AS_PATH {(2907, 17932), (2500, 17932)}, ***V*** is sent an alarm i.e., notification email. If there are a few peers and providers for ***V***, it may be possible to register these ASes as direct next hops that should be appeared in the tail of any AS_PATH, however, it is impossible to express other ASes beyond peers and providers especially if they are Tier-1 ASes which hold several peers. As shown in Figure 2, among the providers of AS 2500, according to [61] there are Tier-1 ASes such as AS 701 (Verizon formerly UUNET) and AS 2914 (NTT). And one of the providers of AS 2907 is AS 3356 (Level-3) which is also Tier-1 AS. Since it is obvious that it is not possible to define all AS_PATHs in full length from every AS in the planet to get to ***V***, ***X*** can blind such detection systems and hijack the traffic by expressing itself from a few hops away from ***V*** instead of expressing as a direct next hop to ***V***. For instance, resulting AS_PATH may look like [X, ... ,3356, 2907, 17932]. Moreover, there are still possible valid reasons such as failure, maintenance or installation of routing entities, disasters, interaction of intra-domain traffic engineering with inter-domain routes, unpredictable sudden traffic shift makes AS_PATH change.

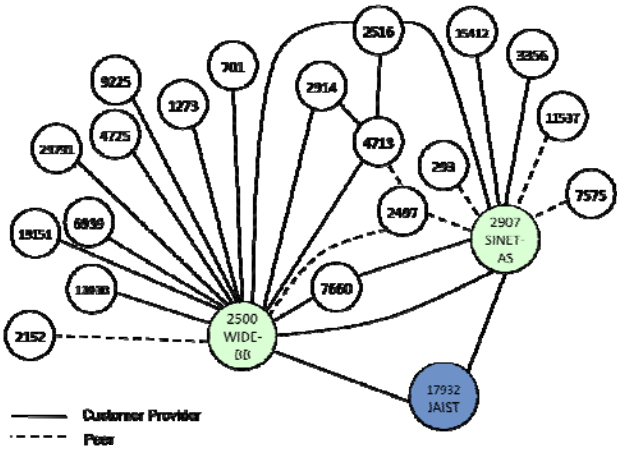

Figure 2: Upstream Providers of AS 17932

Data plane-based hijack detection systems such as [3,6] use active probing mechanisms from several vantage points or from V. In these systems, IP-level traceroute paths are mapped to AS-level paths and then resultant AS_PATHs are analyzed to investigate that the reachability problem is due to hijacking or the conventional disruptive problems such as traffic congestion or link failures.

3.4.3 Analysis of Sub Prefix Hijacking as Invalid Transit

If the destination IP is within the range of sub prefix hijacked by ***X***, the traffic goes to ***X*** since this kind of attack takes advantage of longest prefix matching rule. Besides, most of ASes takes a hijacking route as the best path regardless of AS_PATH length. Generally, although sub prefix hijacking attracts just a portion of traffic that belongs to its super prefix[5], this type of hijacking is not as simple as regular prefix hijacking.

This type of attack can be overlooked by ordinary MOAS-based hijack detection mechanism. [17] said that MOAS conflict would not be occurred unless its super prefixes are examined. In their term, this kind of attack would lead to subMOAS conflict i.e., MOAS involving a subnet of a prefix. MOAS and subMOAS-based hijack detection systems can identify this kind of attack by checking if a particular prefix falls in the range of the ***V***'s regular prefix while Origin AS is different from ***V***.

3.4.4 Analysis of Sub Prefix Hijacking as Invalid Transit

This type of attack would not introduce MOAS and subMOAS conflict not only because of longest prefix matching rule but also expressing ***X*** as a transit rather than an Origin AS. Hence, this type of hijacking is the most difficult one to be detected. Even if Origin AS is the same and the prefix is in the range of registered prefix, such route cannot be said as hijack route because ***V*** can announce more specific prefixes due to load balancing or traffic engineering purposes. Still, although it is not the best practice, hijack detection system can send alarm or report to ***V*** whenever it finds a prefix within a range of registered prefix because it is only ***V*** which can decide that prefix is announced by itself or not.

3.4.5 Analysis of Hijacking unused but allocated address space

It should be noted that not only “currently used prefix” can be hijacked but also “unused but possibly be assigned IP prefix” can be hijacked [5]. For instance, as shown in Table 2, networks of US Department of Defense were hijacked several times during 2008 [20]. As these prefixes are not currently being used although they are owned by Department of Defense, any legitimate traffic cannot be disrupted without any impact on ***V*** 's networks. However the reputation of ***V*** can be affected.

[5] However, if this sub prefix is popular prefix, traffic being hijacked can be a significant portion of the super prefix.

Hijacking unused but allocated address space can be detected using bogon-like filters. Normally bogon prefixes are from private address space and address space that has not been allocated by the Internet Assigned Numbers Authority (IANA) or Regional Internet Registry (RIR). These bogon routes can be filtered by router ACLs or firewalls or BGP blackholing i.e., silently discarding incoming traffic. Since IANA and other registries frequently assign new address space to ISPs, IP addresses that are bogon today may not be bogon tomorrow. [58] also shows that some ASes that filter bogon prefixes continue to filter them for as long as five months after they have been allocated and become legitimate. As announcements of new prefixes assignments are often published on network operators' mailing lists (such as NANOG), when new prefixes are allocated, bogon filters should be updated to allow newly allocated prefixes. If bogon filters are not up-to-date, it would prevent the newly allocated prefixes from being globally visible and bogon filters will introduce false negative effect.

Table 2: Hijacking incidents on unused address space of U.S Department of Defense during 2008

Prefix	Month	Origin AS	Country	Duration
11.11.11.0/24	Jan	9304	Hong Kong	1.1 hours
7.7.7.0/24	March	18305	South Korea	16 min
11.1.1.0/24	March	21240	Russia	3.5 weeks
11.0.0.0/24	April	6983	US	16 hours
30.30.30.0/24	April	10834	Argentina	40 mins
11.1.1.0/24	May	9340	Indonesia	2.1 mins
11.11.11.0/24	May	42075	Turkey	6.5 mins

Consequently, in above all types of hijacking except the case of unused prefixes, hijacked traffic leads to be outage without reaching proper destination. Then ASes of a polluted area i.e., ASes which choose a hijacked route as a best path, will experience reachability problem. Hijacking is to be detected after blackholing the traffic and therefore a prefix cannot be hijacked for a long period.

4. Analysis of Traffic Interception

After hijacking a prefix, ***X*** can forward the hijacked traffic to ***V*** [9]. Since the hijacked traffic is forwarded to the real destination, connectivity is not disrupted and interception is transparent to ***V*** and ASes from a polluted area. Hence it becomes more difficult to be detected. This type of attack can lead to a Man-in-the-middle attack. It allows ***X*** to eavesdrop or modify the traffic.

We describe, in Section 4.1, what traffic interception is, in Section 4.2, attack models of traffic interception, in Section 4.3, its classification and in Section 4.4 its analysis.

4.1 What is Traffic Interception?

After hijacking the prefix, malicious AS can also forward the hijacked traffic back to real destination and this type of attack is called Traffic Interception. As the traffic reach to the destination, connectivity is not disrupted and interception is transparent to the victim ASes. This type of attack can lead to a Man-in-the-middle attack which allows a malicious AS to eavesdrop or modify the traffic.

Traffic Interception is shown in Figure 3. The topology and relationship between ASes are the same as Figure 1. However, in this scenario, there is no blackhole. Because when the traffic from AS 4 comes to AS 5, AS 5 forwards the traffic back to AS 1 through valid AS_PATH [3,2,1]. Since there is no outage or unreachability problem, AS 4 does not know its traffic is being intercepted.

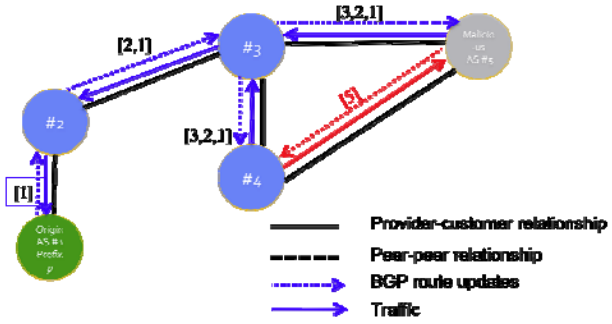

Figure 3: Traffic Interception

4.2 Attack Models of Traffic Interception

To intercept the traffic, at first ***X*** needs to hijack a prefix of ***V*** and then forward the hijacked traffic back to ***V***. To forward the traffic, ***X*** must know valid route to ***V*** and it must somehow maintain that valid route. Whether valid route to destination is maintained by itself or not, attack model of traffic interception can be classified as follows.

4.2.1 Traffic Interception by hiding valid ASes from the AS_PATH

In this type of traffic interception, ***X*** hides valid ASes appears in the route from itself to ***V*** from the AS_PATH it announces to other ASes and maintains valid route to get to ***V*** by itself. To do so, [3] reveals that ***X*** must maintain its safety condition with a high probability. Safety condition means that, not to introduce routing instability, ***X*** should carefully choose ASes to which invalid route advertisements are going to be propagated. Their methodology is based on the business AS relationships and valley free nature of internet routing. If ***X*** 's existing valid route to ***V*** is through its provider, invalid route

advertisements can be sent to its all peers and customers. If ***X*** 's existing valid route to ***V*** is not through its provider, invalid route advertisements can be sent to its all neighbors i.e., providers, peers and customers. Following this methodology to maintain valid route to ***V, X*** would intercept the traffic of other ASes destined to ***V***. However, if ***X*** does not carefully choose which ASes to which invalid route advertisements should be propagated or if such attempt fails, ASes along the valid route to ***V*** may prefer invalid route and subsequently valid route to ***V*** will be lost. In this case, the traffic is blackholed and service is disrupted. Consequently it is likely that this kind of attack may become unsuccessful interception or just prefix hijacking.

4.2.2 Traffic Interception by adding valid ASes into the AS_PATH

In this type of traffic interception, ***X*** adds valid ASes appears in the route from itself to ***V*** into the AS_PATH it announces to other ASes and thus it does not need to maintain valid route to get to ***V*** by itself [57]. In fact, this kind of traffic interception takes advantage the underlying features of BGP known as loop prevention mechanism. If a BGP speaking router sees its own AS in AS_PATH of received route, it rejects that route. By adding valid ASes into the AS_PATH, ASes that appear along the valid route will ignore such route updates. By this way, routing instability can be overcome by ***X***. Therefore this kind of attack is easiest way for ***X*** because it does not have any burden to carefully consider to which ASes it should propagate invalid route, to maintain the route by itself and to prepare router look up for the prefixes it is trying to intercept. Moreover, since it takes advantage of loop preventing mechanism, this kind of attack is the safest way for ***X*** since it does not need to worry about blackholing or outage and as a result, no AS will suffer reachability problem.

4.3 Classification of Traffic Interception

Using one of two ways described in Section 4.2.1 and Section 4.2.2, ***X*** can intercept the prefix of ***V***. Since intercepting the traffic follows prefix hijacking, classification of traffic interception is usually similar with that of IP prefix hijacking described in Section 3.3. Again, as described in Section 3.3.3, super prefix hijacking is possible only when the route to the valid prefix is withdrawn. As the valid route is already withdrawn, ***X*** cannot forward the hijacked traffic back to ***V*** i.e., the interception is not possible. Therefore we will discuss only regular and sub prefix cases for traffic interception.

As hijacking should be placed in first to carry out interception, except forwarding the traffic back to destination, intercepting as Invalid Origin is the same as hijacking as Invalid Origin described in Section 3.2.1. Therefore, not to be redundant information, we will focus only on Invalid Transit type in both models:

- Regular Prefix Interception as Invalid Transit
- Sub Prefix Interception as Invalid Transit

However detection towards Invalid Origin type will be discussed in Discussion Section.

4.4 Analysis of Traffic Interception

4.4.1 Regular Prefix Interception as Invalid Transit

Using the attack model of Traffic Interception by hiding valid ASes from the AS_PATH mentioned in Section 4.2.1, ***X*** can hide[6] one or more ASes between itself and ***V*** to construct invalid path attractive to other ASes. It is very likely that ASes around ***X*** will pick invalid route advertised by ***X*** as best path because invalid AS_PATH is shorter than the valid AS_PATH[7]. Thus generally, this kind of attack will have impact on ASes near ***X***. How big such impact depends ***X*** 's ranking degree and depth of ***X*** 's customer cone, number of peer ASes ***X*** has and the ranking degrees of those peers [3]. However, this impact cannot be global because since the prefix is regular, there are ASes which still prefer valid route while other prefer invalid route.

Attack model of traffic interception by adding ASes into the AS_PATH mentioned in Section 4.2.2, cannot be applied in regular prefix case. If ***X*** intercepts traffic destined to ***V*** 's prefix, being lengthy in resulting AS_PATH, even ASes around ***X*** will not choose the path advertised by ***X***. One can argue that customer ASes of ***X*** will choose the route. It is true but it is not hijacked route but just a legitimate route as long as prefix is regular[8]. Therefore attack model of traffic interception by adding ASes into the AS_PATH can only be applied in sub prefix case.

4.4.2 Sub Prefix Interception as Invalid Transit

Using the attack model of Traffic Interception by hiding valid ASes from the AS_PATH mentioned in

[6] ***X*** can even add one or more ASes to make its invalid AS_PATH less suspicious.

[7] There may be a few ASes around ***X*** which will stick to valid AS_PATH because of policy.

[8] Of course traffic can be intercepted using ordinary legitimate route. This kind of intercepting does not need to manipulate any BGP update message. Since we focus on hijacking and intercepting due to manipulated BGP update messages and routing anomaly, intercepting the data using ordinary legitimate route is beyond our scope because it is related with data security.

Section 4.2.1 ***X*** can hide one or more ASes between itself and ***V*** to make invalid path attractive to other ASes. If ***X*** intercepts the sub prefix of ***V*** and ***X*** can successfully forward the traffic back to ***V*** by strictly following respective attack model, the impact will be considerably higher than that of regular prefix described above. Because, regardless of the length of AS_PATH, most ASes will prefer invalid route advertised by ***X*** as the prefix is more specific.

Using the attack model of traffic interception by adding ASes into the AS_PATH mentioned in Section 4.2.2 makes the resulting AS_PATH becomes longer. Because of being sub prefix, although most of the ASes will prefer invalid route advertised by ***X***, if ***X*** is several hops away from ***V***, resulting AS_PATH will look suspiciously long[9]. Not to make very lengthy AS_PATH, ***X*** can choose ***V*** among nearer ASes from itself. If ***X*** intercepts the sub prefix of ***V***, the impact will be global. Because, most of ASes except ASes along the valid route will prefer the invalid route.

It is obvious that detecting interception is much more difficult than hijacking since it does not introduce any connectivity problem to ***V*** and we will discuss the detection towards interception in Discussion Section.

Discussion

Intercepting the prefix (regular or sub) as Invalid Origin would lead to MOAS or subMOAS conflict, if ***V*** exercises hijack detection systems. Ironically, smart ***X*** would not intercept the traffic destined to ***V*** as Invalid Origin type. However, it does not mean that it is totally impossible for ***X*** to intercept the traffic to prefixes of ***V*** as Invalid Origin. When ***X*** cannot easily know if ***V*** is using hijack detection systems and ***X*** also considers its safety, ***X*** will not use interception as Invalid Origin type. Even if ***X*** intercepts prefixes of ***V*** as Invalid Origin, although it is not the best way, hijack detection system can send an alarm to ***V*** whenever it finds a prefix which is within a range of registered prefix. Reported AS_PATH can be a hijack route or legitimate route announced by ***V*** due to load balancing or traffic engineering purposes. As detection system cannot surely identify the hijack route among legitimate routes, there is only ***V*** which can decide which route is valid. Needless to say, if ***V*** does not use any monitoring system or hijack detection system, prefixes of ***V*** are free to be intercepted as Invalid Origin as long as ***X*** can forward the traffic back to ***V***.

In the case of regular prefix interception as Invalid Transit, to detect the attack type of Traffic Interception by hiding valid ASes from the AS_PATH mentioned in Section 4.2.1 cannot totally rely on MOAS and subMOAS-based hijack detection systems. However hiding one or more ASes between itself and ***V*** the relationship between them in invalid AS_PATH can expose some hints in both control plane and data plane information. In the case of control plane, for instance, invalid AS_PATH advertised by ***X*** may violate the valley free nature of internet routing. Moreover, the difference in ranks of ***X*** and following AS may look suspicious. For instance, Tier-1 AS appears as peer or customer of small AS.

In the case of data plane, hop counts and delay can be much different from those of control plane. Using probing tools such as traceroute, the resultant AS_PATH mapped from IP-level path can then be compared against control-plane AS_PATH. However since there are errors in IP-to-AS mappings due to IXPs, traffic engineering, sibling ASes and other legitimate anomalies [60], whenever two AS_PATHs are not identical one cannot say it is an interception. And as the traffic through congested AS or congested inter-AS link will encounter delay, whenever there is a leap in delays of two ASes, one cannot say it is an interception. Moreover, it should be noted that ***X*** can also handle even such data plane measurements in order to keep the data plane information reasonable and align with control plane information by manipulating probe packets and TTL value.

In the case of traffic interception by adding valid ASes into the AS_PATH mentioned in Section 4.2.2, conducting data-plane measurements cannot work for this type. Since this type of interception takes advantage of look prevention mechanism of underlying BGP, invalid route advertisement will be received by at least one AS along the valid route. Still there can be some cases this invalid advertisement will be reached to ***V***. If ASes along valid route check the prefix before discarding the route when it sees its own AS number in newly received route, it can notice that the prefix is different from that of current best path. However, AS which notices such kind of suspicious route can simply neglect it since such route does not affect its own traffic. MOAS and subMOAS-based hijack detection system can also be used although it is not a best solution but still it gives a way to let ***V*** know when it finds a more specific prefix.

IP hijacking can be prevented to some extent by means of filters and hijack detection systems. Announcements by customer ASes and peer ASes in which prefixes are out of the allocated range can be filtered. If route filters at the links between providers and their customers are properly configured in order to prevent customer ASes from advertising the routes for the prefixes which do not belong to them. However, according to following reasons, this is insufficient and difficult:

[9] To make AS_PATH shorter, if ***X*** hides one or more hops, it leads to the attack model of Traffic Interception by hiding valid ASes from the AS_PATH mentioned in Section 4.2.1.

- To install ingress filters, it is not always possible for providers to know which prefixes are assigned to which customers. If customers have multiple providers, they may have different address prefixes from different providers.

- And enforcing ingress filters in peering edges is also difficult as it is not knowable that peer ASes allocate which addresses to their customers.

- Even if route filters are installed in ingress points, when there is one provider that does not practice route filtering, IP hijacking becomes possible.

And similar to ingress filters, bogon filters can be exercised too. Using MOAS or subMOAS based hijack detection systems prevent the prefixes from being hijacked.

Conclusion and Future Work

This paper presents the analysis of IP prefix hijacking and traffic interception. We surveyed the reported incidents happened between 1997 and 2009 from NANOG. Based on these incidents, we systematically describe the attack models of IP prefix hijacking and traffic interception. Then we classify each attack type along with the constructed attack model. Finally, we thoroughly analyze and explore the characteristics and nature of each attack type. In the analysis of traffic interception, we also point out that there is no decent solution yet. This work provides the analysis which previously lacked. Proposed models give useful information to future detection systems. Our future work is how to detect or prevent each type of traffic interception.

References

[1] RIPE, RIS Raw Data. http://www.ripe.net/projects/ris/rawdata.html.
[2] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, Jan. 2006.
[3] H. Ballani, P. Francis, and X. Zhang, "A Study of Prefix Hijacking and Interception in the Internet", In Proc. of ACM SIGCOMM, Aug. 2007.
[4] O. Nordstrom and C. Dovrolis, "Beware of BGP attacks", SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, 2004.
[5] A. Ramachandran and N. Feamster, "Understanding the Network-Level Behavior of Spammers", In Proc. ACM SIGCOMM, Sept. 2006.
[6] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis, "A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Real-Time", In Proc. ACM SIGCOMM, 2007.
[7] Carl Hutzler and Ron da Silva, "The Relationship Between Network Security and Spam", NANOG 29 Meeting. Oct. 2003.
[8] V. J. Bono, "7007 Explanation and Apology", http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html. April. 1997.
[9] Jintae Kim, S.Y. Ko, D.M. Nicol, X.A. Dimitropoulos, G.F. Riley, "A BGP Attack Against Traffic Engineering", In Proc. Winter Simulation Conference, 2004.
[10] J. Markoff, "Internet Traffic Begins to Bypass the U.S.", http://www.nytimes.com/2008/08/30/business/30pipes.html, Aug. 2004.
[11] Nanog Mailing List, "AS8584 taking over the internet", http://www.merit.edu/mail.archives/nanog/1998-04/msg00047.html April. 1998.
[12] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, "PHAS: A Prefix Hijack Alert System", In Proc. USENIX Security Symposium, Aug. 2006.
[13] Nanog Mailing List, "Con Ed 'stealing' Panix routes", http://www.merit.edu/mail.archives/nanog/2006-01/msg00483.html Jan, 2006.
[14] Renesys blog, "Con Ed Steals the 'Net' Panix", http://www.renesys.com/blog/2006/01/coned-steals-the-net.shtml
[15] 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. Internet Measurement Workshop, Nov. 2001.
[16] Nanog Mailing List, "C & W Routing Instability", http://www.merit.edu/mail.archives/nanog/2001-04/msg00198.html, April 2006.
[17] X. Hu and Z. M. Mao., "Accurate Real-time Identification of IP Prefix Hijacking", In Proc. IEEE Security and Privacy, May 2007.
[18] M. Lad, R. Oliveira, B. Zhang, and L. Zhang., "Understanding Resiliency of Internet Topology Against Prefix Hijack Attacks", In Proc. IEEE/IFIP DSN, June 2007.
[19] R. Mahajan, D. Wetherall, and T. Anderson., "Understanding BGP Misconfiguration", In Proc. of ACM SIGCOMM, Aug. 2002.
[20] Martin A. Brown., Todd Underwood, Earl Zmijewski, "The day the youtube died", http://www.nanog.org/meetings/nanog43 Jun. 2008.
[21] Alin C. Popescu, Brian J. Premore, Todd Underwood, "natomy of a leak AS 9121", http://www.nanog.org/meetings/nanog34 May. 2008.
[22] S. Murphy, "Progress Toward Security the Routing Infrastructure", http://www.cyber.st.dhs.gov/public/CATCH/Murphy.pdf March. 2009.
[23] M. Kaeo, "Cyber Attacks on Estonia Short Synopsis", http://doubleshotsecurity.com/pdf/NANOG-eesti.pdf March. 2009.
[24] I. Thomson, "Estonia Under Cyber Attack", http://www.itnews.com.au/News/52345,estonia-under-cyber attack.aspx March. 2007.
[25] Nanog Mailing List, "An account of the Estonian Internet War", http://mailman.nanog.org/pipermail/nanog/2008-May/000676.html May. 2008.

[26] Merit R & D, "12.0.0.0/8 Prefix Anomaly", http://bgpinspect.merit.edu/reports.php
[27] J. Karlin, S. Forrest, J. Rexford, "Pretty Good BGP and the Internet Alert Registry", www.nanog.org/meetings/nanog37 Jun. 2006.
[28] RIPE NCC News, "YouTube Hijacking: A RIPE NCC RIS case study", http://www.ripe.net/news/study-youtube-hijacking.html
[29] Nanog Mailing List, "YouTube IP Hijacking", http://www.merit.edu/mail.archives/nanog/2008-02/msg00453.html Feb. 2008
[30] Nanog Mailing List, "Kenyan Route Hijack", http://www.merit.edu/mail.archives/nanog/2008-03/msg00237.html Mar. 2008
[31] Nanog Mailing List, "prefix hijack by ASN 8997", http://www.merit.edu/mail.archives/nanog/2008-09/msg00704.html Sept. 2008
[32] Nanog Mailing List, "Potential Prefix Hijack", http://www.mail-archive.com/nanog@nanog.org/msg06515.html Nov. 2008
[33] Nanog Mailing List, "massive routes hijack at AS48400, up to 6000 AS affected? ", http://www.mail-archive.com/nanog@nanog.org/msg08267.html Jan. 2009.
[34] MyASN., http://www.ris.ripe.net/myasn.html
[35] DNSMON., http://dnsmon.ripe.net/
[36] BGPMON., http://bgpmon.net/
[37] Kent, S., C. Lynn, and K. Seo., "Secure Border Gateway Protocol (Secure-BGP)", IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, April, 2000
[38] R. White., "Securing BGP Through Secure Origin BGP", Internet Protocol Journal, vol. 6, 2003.
[39] T. Wan, E. Kranakis, and P. v. Oorschot., "Pretty Secure BGP (psBGP)", In ISOC. San Diego, CA, USA, 2005.
[40] B. Smith and J. Garcia-Luna-Aceves., "Securing the border gateway routing protocol", In Proc. Global Internet, November 1996.
[41] Y.-C. Hu, A. Perrig, and M. Sirbu., "SPV: secure path vector routing for securing BGP", In Proc. of ACM SIGCOMM, 2004.
[42] W. Aiello, J. Ioannidis, and P. McDaniel, "Origin authentication in interdomain routing", In Proc. of conference on Computer and communications security (CCS), 2003.
[43] X. Liu, P. Zhu, Y. Peng, N. Hu., "A cooperative Method for Prefix Hijack Detection in the Internet", Globecom Workshops, 2007 IEEE.
[44] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. Felix Wu,L. Zhang., "Detection of Invalid Routing Announcement in the Internet", In IEEE DSN, 2002.
[45] J. Karlin, J. Karlin, S. Forrest, and J. Rexford., "Pretty Good BGP: Improving BGP by Cautiously Adopting Routes", In Proc. ICNP, 2006.
[46] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, and L. Zhang., "Protecting BGP routes to top level DNS servers", IEEE Transactions on Parallel and Distributed Systems, vol. 14, no. 9, pp. 851–860, 2003.
[47] X. Zhao, M. Lad, D. Pei, L. Wang, D. Massey, S. Wu, and L. Zhang., "Understanding BGP behavior through a study of DoD prefixes.", In Proc. of DISCEX III, April 2003.
[48] G. Siganos and M. Faloutsos., "Neighborhood Watch for Internet Routing: Can We Improve the Robustness of Internet Routing Today?", In Proc. IEEE INFOCOM, May 2007.
[49] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur., "Topology-based Detection of Anomalous BGP Messages.", In Proc. RAID, Sept. 2003.
[50] 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. Dependable Systems and Networks, 2002.
[51] 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. Network and Distributed Systems Security, February 2003.
[52] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. H. Katz., "Listen and Whisper: Security Mechanisms for BGP", In Proc. USENIX NSDI, Mar. 2004.
[53] Z. Zhang, Y. Zhang, Y. Charlie Hu, Z. Morley Mao, R. Bush., "iSPY: Detecting IP Prefix Hijacking on My Own", In Proc. Sigcomm, Aug. 2008.
[54] J. Karlin, S. Forrest, J. Rexford, "NANOG-NOTES Pretty Good BGP Josh Karlin", http://www.merit.edu/mail.archives/nanog/2006-06/msg00035.html Jun. 2006.
[55] J. Borland, CNET News, "Short Take: AT & T WorldNet suffers outage", http://news.cnet.com/Short-Take-ATT-WorldNet-suffers-outage/2110-1033_3-233799.html Dec. 1999.
[56] L. Gao, J. Rexford, "Stable Internet Routing Without Global Coordination", In Proc. SIGMETRICS, 2000.
[57] A. Pilosov and A.T Kapela, "Revealed: The Internet's Biggest Security Hole", http://www.wired.com/threatlevel/2008/08/revealed-the-in/ Aug. 2008
[58] N. Feamster, J. Jung and H. Balakrishnan "An empirical study of "bogon" route advertisements", In Proc. ACM Computer Communications Review, Nov. 2004
[59] N. Feamster, J. Jung and H. Balakrishnan "MyASN", https://ripe.net/projects/ris/docs/myasnhelp.html
[60] Z. M. Mao, J. Rexford, J. Wang, and R. H. Katz "Towards an accurate AS-level traceroute tool", in Proc. of ACM SIGCOMM, 2003.
[61] "Tier 1 network", http://en.wikipedia.org/wiki/Tier_1_network
[62] IAR., "Internet Alert Registry", http://iar.cs.unm.edu/