On the use of BGP AS numbers to detect spoofing

Ravi Vaidyanathan, Abhrajit Ghosh and Yuu-Heng Cheng
Telcordia Technologies, Inc.
{vravi,aghost,yhcheng}@research.telcordia.com

Akira Yamada and Yutaka Miyake
KDDI R&D Laboratories, Inc.
{yamada.akira,miyake}@kddilabs.jp

Abstract—Spoofed IP traffic (traffic containing packets with incorrect source IP addresses) is often used by Internet-based attackers for anonymity. This method reduces the risk of traceback and avoids attack detection by traffic-based sensors. An ISP’s Security Operations Center (SOC) needs an efficient spoofed source detection mechanism to protect its customers from network-based attacks. Typically an SOC needs to offer such protection under the following operational constraints: a) Limited traffic monitoring points within the network core rather than at the edge, owing to the performance cost associated with incorporating monitoring b) Limited information on network topology and routing paths c) Very high data rates d) Sampled traffic data and e) Limited storage and processing capabilities for analysis. This paper describes an approach for spoofed source detection intended for an operational ISP network under the above constraints. The approach relies on the creation of concise source BGP AS (Autonomous System) profiles for each available monitoring point in the network. Profiles are constructed by observing recent historical monitoring data; each constructed profile is then used to detect spoofed traffic in real-time. An AS based network profile is advantageous compared to an IP address based profile due to (a) the relative conciseness of the former and (b) the ability to make inferences about network source IP addresses not observed during training or profiling periods. A preliminary evaluation of AS based profiles was performed using real time traffic observed in an enterprise network. The evaluation focus was on profile size and profile convergence time.

Keywords: Spoofing, Distributed Denial of Service (DDoS), Border Gateway Protocol (BGP).

I. INTRODUCTION

Internet attackers often spoof (and thereby mask) the source addresses of machines which are used to carry out network based attacks. Spoofing has been used to obfuscate the sources of network attacks for a while and continues to be a significant issue in the Internet [1]. This strategy is often used for Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks. With a spoofed source address, a Security Operations Center (SOC) may not be able to identify the true sources of attack traffic and may sometimes shift attention to innocent third parties. A skillful attacker can spoof source IP addresses in network traffic originating from most operating systems. Since IP routing is destination-based, spoofed IP packets are delivered to the intended target in the same way as non-spoofed IP packets. Spoofed IP packets are particularly prevalent in DDoS attacks, wherein an attacker can compel multiple intermediate compromised hosts to inundate a target host or network with a cumulatively high-volume IP traffic stream. Detection of such DDoS attacks by network-based sensors is difficult since spoofing ensures that traffic volume from individual hosts appears to be low. In addition to high-volume attacks such as DDoS, relatively stealthy attacks may also employ spoofed IP packets. A notable example was the Slammer worm which used to send out a single source IP spoofed UDP (User Datagram Protocol) packet that compromised the destination node. Thus, Spoofed IP traffic detection is a generic means by which to detect several different types of network attacks without using specialized detectors for each attack.

Approaches to prevent traffic with spoofed source addresses include validation of source addresses before packets travel from an edge network to the Internet (Ingress Filtering) and vice versa (Egress Filtering) as discussed in [2]. Egress filtering rules allow traffic to enter an edge network only if the source IP address does not belong to it. In contrast, Ingress filtering allows traffic to depart the edge network only if the source IP address belongs to it. Egress filtering prevents an edge network from receiving a very specific range of spoofed sources but cannot protect against arbitrary spoofing. Ingress filtering prevents spoofed traffic from entering the public Internet from an edge network and therefore does not directly impact the protection of the users within the latter. As a consequence, there is a general unwillingness on the part of ISPs to implement such filtering techniques since they result in operational overheads with either marginal or indirect benefits. In particular, these techniques require significant large-scale deployment by ISPs in the Internet before benefits can be realized. Accordingly, even though the mechanisms to implement egress/ingress filtering are available on most routers in the Internet, a large number of ISPs currently do not use them. As a consequence, spoofed traffic can be freely originated within a majority of hosts at these ISPs.

Another approach for detecting and containing spoofed IP traffic is Unicast Reverse Path Forwarding (uRPF [3]). A uRPF enabled edge router drops an incoming IP packet at a given interface if the outbound path back to the packet’s source IP address does not use that interface. Due to the dynamic nature of Internet routing protocols and the fact that a router always chooses the best path to a destination based on these protocols, there can be many cases where uRPF based traffic filtering will drop traffic with valid source IP addresses. Thus, uRPF only works in certain specific situations and is not a complete solution to the problem of detecting spoofed IP traffic.

Another scheme to defend against DDoS attacks based on IP source address filtering near the attack target has been discussed in [4]. According to this scheme, each edge router
keeps a history of all the legitimate IP addresses, which have previously entered the network. When the edge router is overloaded, this history is used to decide whether to admit an incoming IP packet. However, this scheme only provides a limited solution to the problem, because it makes use of a history set of source IP addresses observed independently at each edge router. In particular, this technique does not address false positives that may be generated by a previously unseen source generating traffic to the destination network.

The InFilter scheme discussed in [5] addresses some of the shortcomings of [4]. It presents a predictive filtering approach that makes use of an “InFilter” hypothesis to detect spoofed source IP addresses in traffic near its destination. The approach leverages historical source IP address information across multiple edge routers to infer spoofing activity in observed traffic. This scheme alleviates the problem faced by [4] to an extent, by using source IP address histories across multiple edge routers. If the source IP address on an incoming packet is not in the incoming edge router’s history, the packet is dropped only if the source IP address is in a different edge router’s history. However, this method still suffers from a limitation when a source IP address has not been seen at any of the edge routers in the destination network.

An SOC is a distinct entity that provides security services to the network operators. These services include monitoring the network for traffic anomalies. In many cases, the SOC function is outsourced to a 3rd party and consequently, operates under various constraints. These include:

(a) Limited traffic monitoring at points within the network core rather than at the edge. Router performance, capability and cost considerations may dictate that network traffic monitoring is not implemented at the numerous edge routers of a large ISP, but rather at a limited number of core monitoring points. Further, monitoring is often accomplished by mirroring traffic to monitoring points, making it hard to determine the edge router at which a particular traffic flow was observed.

(b) Limited availability of topology and routing information about the monitored network. Such information may not be readily available from a single source and may also be poorly documented making it hard to infer paths traversed by monitored traffic. This makes it hard to apply edge based spoof detection techniques since there is no information about how a monitoring point relates to an edge.

(c) Very high data rates. It is not unusual to observe several terabytes worth of data at the network monitoring points. Any monitoring solution is required to keep up with these traffic rates.

(d) Sampled data. Most monitoring solutions employ data sampling techniques [6], [7]. As a consequence any constructed profiles of the network monitoring points may be incomplete.

(e) Limited storage and processing capabilities. A SOC has limited computing hardware and storage capabilities relative to the rates at which traffic is generated within the network. This limits the amount of traffic related information that can be stored and requires the use of analysis algorithms that depend on minimal data storage. This also impacts the level of detail at which analysis can be performed and requires the use of coarse grained analysis algorithms.

In this paper, we describe an approach for spoofed source detection system that addresses the issues described above. Our approach can provide value even when network flow information is collected from within the network core rather than at the edge. It stores network profiling information in terms of BGP AS (Autonomous System) numbers rather than network IP addresses. This allows for both concise data representation as well as the ability to draw inferences about IP traffic from previously unobserved sources, thus mitigating a major drawback of [5].

II. SPOOFED SOURCE DDOS ATTACK DETECTION

Our solution makes the following hypothesis: packets from the same origin AS traverse the same set of monitoring points when traversing a destination network. This is an extension of the hypothesis used in [5] which says that the same ‘last hop’ AS is used by packets from the same source AS prior to entering the destination AS. This is a reasonable extension based on the fact that traffic routes within an AS change infrequently. Thus based on this extended hypothesis we expect that IP prefixes from the same origin AS will be observed at the same network interface or network interconnection point within the destination AS (or set of interfaces, in the case of redundant or load balancing network configurations).

This property is used to construct the Expected AS (EAS) set, a set of AS numbers that is deemed as valid for a particular network interface at a monitoring point. The EAS set is constructed by examining historical traffic traces associated with a particular network interface. Source IP addresses in IP packets are correlated with origin AS information by leveraging BGP routing information or routing registries as described below. If a packet with origin AS $A_S$ is observed at an interface $IF_j$, $A_S$ is added to the EAS set for that interface. This method is most effective when it can be implemented at interfaces in AS border routers. However, in commercial networks this may not always be feasible since (1) historical traffic traces at border routers may not be available and (2) implementing computationally intensive AS translation and matching mechanisms at border routers may not be practical. Based on our hypothesis, we expect that the EAS based spoofing detection mechanisms can also be implemented by observing historical traffic traces at core routers, or dedicated traffic collection points in the network.

A notional network where EAS based spoofing detection may be applied is shown in Figure 1. Here, a Target network is shown to contain several edge routers that receive traffic from multiple external networks (ISP_X, ISP_Y etc.). Internal to the Target network are several core routers that route traffic within this network. There are also several flow exporters (i.e. traffic monitors) that collect information about traffic traversing the network. Typically such monitors export collected information using NetFlow [6] or sFlow [7]. Such information typically includes source and destination IP addresses, source and destination ports, packet sizes, time at which packet was observed and so on.
described in more detail below: a RouteViews server contain conflicting AS information about them. For some IP prefixes, the data sources may be BGP data from the sources discussed above, our method however, there may be several issues with this information. There is no guarantee that the training traffic flows with network interfaces at dedicated traffic collection points in the same IP Prefix, the operator may choose to assign a higher preference to information from the IRR database, indicating a relatively higher trust level. It may also be possible to assign relative preferences to individual IRR databases or RouteViews servers for more fine-grained control of AS information. Our solution also allows the operator to combine data from various databases, effectively resulting in a more conservative superset (or union) across the various IP prefix – AS information sources.

Figure 1. EAS deployment environment.

Our solution involves the following steps: (1) Acquisition of IP Prefix to Origin AS mappings (2) Profiling network interfaces using training traffic (3) Detection of anomalous source AS numbers in operational traffic. These steps are described in more detail below:

1. Acquisition of IP Prefix to Origin AS mapping: The creation of the EAS set includes generating a map from IP prefixes to their corresponding AS numbers as depicted in the upper half of Figure 2. BGP route information pertaining to specific source prefixes can be collected locally from the network operator’s routers, from RouteViews servers (www.routeviews.org), or from Internet Routing Registry (IRR) databases (www.rr.int).

IRR databases can contain authoritative information mapping registered IP prefixes to their corresponding ASes. However, there may be several issues with this information. First, the mapping of an IP prefix to an AS may not be one to one. For example, one IP prefix can be registered with several AS numbers belonging to a single corporate entity. Secondly, a registered IP prefix does not necessarily indicate that the specific prefix is used in the registered network. Finally, every IP prefix is not necessarily registered with a given set of IRR databases and it may not be possible to infer the corresponding originating AS based on these databases.

RouteViews servers contain live BGP routing data that represents the actual information used by routers in the Internet to forward traffic. This data can also be used to infer a corresponding AS number for a given IP prefix. However, as was the case with IRR above, RouteViews data from a given set of servers may not contain information about a given IP prefix since said prefix may not be visible at these servers. Further, due to misconfiguration or malicious advertisements, it is possible that some of the IP Prefix to AS number mappings may be incorrect. A network operator’s local BGP routers are subject to similar constraints. Given the deficiencies in the BGP data from the sources discussed above, our method combines BGP routing information across the various sources (RouteViews, IRR & local BGP servers) and attempts to merge them. For some IP prefixes, the data sources may be complementary while in case of others, they may be conflicting. Conflicts are resolved by assigning higher trust levels to some subset of sources. Thus, if an IRR database and a RouteViews server contain conflicting AS information about

Figure 2. EAS profile creation.

2. Profiling network interfaces using training traffic: Once the IP prefix to AS number mappings are determined, our method uses training traffic flows to associate AS numbers with network interfaces at dedicated traffic collection points in the network. As shown in Figure 2, the source IP address is extracted from each training flow as observed at the network interface. This source IP address is translated into a corresponding AS number using the IP Prefix to AS number mapping created in step (1) above. The information about the AS number and the network interface at which it was observed is retained in the EAS set (described at the beginning of this section). An EAS set maps each network interface at each traffic collection point, to a set of AS numbers observed at that network interface.

It is not possible to guarantee that the training traffic flows do not contain any IP packets with spoofed source addresses. However, we can mitigate this concern by filtering out flows that are destined for attack victims. This could be done, for example, by eliminating all traffic to a destination that sees an abnormally high load (assuming that most attacks which use traffic spoofing are volume based). The EAS sets for a given network interface may be updated based on changes in IP prefix to AS number mappings. It is also possible that a new set of training traffic flows could result in changes to the EAS sets. This could happen due to a change in the routing topology either within the Target network or in some portions of the Internet connected to it.

3. Detection of anomalous source AS numbers in operational traffic: Once EAS sets have been constructed; we are ready to detect anomalies in operational traffic within the Target Network. As was the case with training traffic flows, source IP addresses on operational traffic flows are mapped to their corresponding AS numbers using the IP Prefix to AS number map created in step (1). These AS numbers are compared against the EAS set for the network interface, and
appropriate alerts are generated if the AS number is missing from the EAS set for the given network interface or the AS number is not present in the EAS set for any monitoring point network interface. The specific processing steps used to detect anomalous AS numbers at a network interface are shown in Figure 3. Here SrcAS refers to the AS number corresponding to a Source IP (SrcIP) address in an observed traffic flow. SrcIntf refers to the network interface at which the flow was observed. Finally, ASClass contains the decision of the detection process.

![Figure 3. EAS profile creation.](image)

Our approach offers several advantages when compared to previous work, in particular:

1. In relation with approaches such as uRPF that rely on symmetric routing, our approach leverages AS-level routing information, but has no reliance on symmetric routing.

2. An approach such as Ingress Filtering must be applied by the source network, since it filters traffic originating from source IP addresses not assigned to that network. In contrast, our methodology can be applied at the destination networks by leveraging origin AS information in conjunction with historical traffic traces. It provides immediate benefits to the network deploying the approach thus giving greater incentives than the deployment of Ingress Filtering.

3. Egress filtering provides a destination AS protection against incoming spoofed traffic using source addresses that belong to the destination AS. This protects against traffic that uses a relatively limited set of spoofed sources while our approach can, in general, protect against traffic using arbitrary spoofed sources.

4. Detection and Filtering approaches have centered on the use of IP addresses (e.g. [4][5]) for creating network profiles. In our approach, we use the origin AS of the IP packet for spoofed packet detection. The number of active IP prefixes in the Internet routing tables is roughly 330K, while the number of active AS numbers is roughly 32K. Thus our solution can result in much more scalable detection mechanisms. In addition, filters that leverage AS numbers rather than IP addresses would be an order of magnitude smaller in size, further contributing to the ability to deploy our solution.

5. Techniques such as [4] and [5] rely on historical observations of IP addresses to identify spoofed traffic. Since our technique maps the IP addresses to AS numbers, we are able to classify as legitimate or spoofed, traffic with IP addresses that have never been observed before, as long as some traffic from the same origin AS has been observed. This can result in dramatic decreases in the amount of time required for training the detection algorithm, as well as a decrease in the number of sources classified as “unknown” by the detection algorithm.

III. PERFORMANCE RESULTS

In this section, we provide a preliminary assessment of the benefits that may be achieved by constructing AS based filters. Essentially, these results show that AS based filters can be smaller and therefore more efficient than IP based filters.

Another factor in determining the usefulness of a detection algorithm is the amount of data required for training. We show that the training of AS based filters requires smaller amounts of training data than IP based filters making them relatively attractive for deployment.

The experiments described in this section involved the gathering and analysis of flow data in an enterprise network. Flow data was obtained from two monitoring points situated in the enterprise network.

![Figure 4. Data Set.](image)

A. Data Set

Figure 4 depicts the rate at which flows were observed at two monitoring points within the enterprise network over a period of approximately 9 days. We focus on the data from Flow Exporter 1 with an average flows/minute of ~9000. Overall about 122M flows were observed over a 9 day period.

B. Profiling Size

We next examine the size of profiles constructed using the flow information collected from each monitoring point. We examined 3 types of profiles (a) IP address based profiles (shown as EIA/32) which consisted of unique 32-bit source IP addresses observed at Flow Exporter 1 during the observation period (b) IP subnet address based profiles (shown as EIA/24) which consisted of unique /24 prefixes of observed source IP addresses and (c) AS based profiles (shown as EAS) which consisted of unique AS numbers corresponding to observed source IP addresses.
Figure 5 shows the sizes of the 3 types of profiles for Flow Exporter 1. The EIA/32 profile size increases monotonically through the duration of the profiling period, with a profile size of about 1.6M entries. Using the EIA/24 profile results in the decrease of the profile size by approximately a factor of 2 to about 864K entries. The EAS profile is much smaller than either of the other profiles and is barely visible in this figure, stabilizing at about 16K entries. In summary, using EAS based profiling for this data set results in a decrease of the profile size by a factor of 102.

Figure 6 depicts the time taken for the various profiles to converge. We define the convergence metric as the time taken for the profile to achieve 90% coverage of the data set. The EAS based profile achieves this coverage in approximately 5 days, whereas the EIA/24 and EIA/32 profiles need roughly 7 and 7.5 days to achieve this level of coverage. Thus, EAS based profiling is between 29-34% faster to converge than the other techniques.

The data presented in this section shows that profiles converge much faster for AS number based profiles than IP address based profiles. In addition, the profile sizes for AS number based profiles are much smaller than IP address based profiles constructed using the same training data set.

IV. CONCLUSIONS AND FUTURE WORK

We presented a technique for profiling network monitoring points using AS numbers. This technique provides a way to create efficient filters for potentially detecting traffic that uses spoofed source IP addresses. Further, we found that AS number based profiles can be created using smaller amounts of training data than IP address based profiles.

The results presented in this paper are preliminary. For one, the training data was not verified to be free of attack traffic. The presence of attack traffic that used spoofed source addresses would affect the quality of the created profiles. An approach for detecting the presence of attack traffic in the training data would be to check for volume anomalies. Flows that contribute to such anomalies would be expunged from the training data set. As part of our ongoing work, we are examining this and other approaches for ‘scrubbing’ our training data sets with the aim of creating higher quality AS number profiles.

While EAS based detection has the advantages pointed out in this paper, i.e. smaller profile sizes and faster profiling times, it introduces the possibility of false negatives (i.e. spoofed traffic that is classified as legal) since the granularity of the EAS profiles are coarser. The tradeoff is the higher coverage accorded by EAS profiles when compared to EIA profiles; since EAS profiles cover all prefixes corresponding to an AS. We are undertaking anomaly detection experiments to further evaluate these tradeoffs and quantify the benefits of EAS-based approaches.

REFERENCES