2013-07-25

Initial longitudinal analysis of IP source spoofing capability on the Internet

Beverly, Robert

Initial Longitudinal Analysis of IP Source Spoofing Capability on the Internet

Date: 25 Jul 2013
Document Type: Briefing Papers
Tags: Cybersecurity , Routing Security, Security

Robert Beverly, Ryan Koga, kc claffy
The Spoofer project originated in 2005 as the result of discussions over the general ability to successfully send spoofed-source IP packets across the Internet. At the time, a common misconception was that “most networks perform source address filtering, and, even if they don’t, botnets remove any of the anonymity advantage afforded by spoofing.” Such beliefs of course proved incorrect in light of a rash of spoofing-based denial-of-service attacks — attacks that still occur to this day. Despite IP source spoofing being a known vulnerability for at least25 years, and despite many efforts to shed light on the problem, spoofing remains a viable attack vector for redirection, amplification, and anonymity as evidenced most recently and publicly in May 2013 during a 300+ Gb/s DDoS attack against Spamhaus.

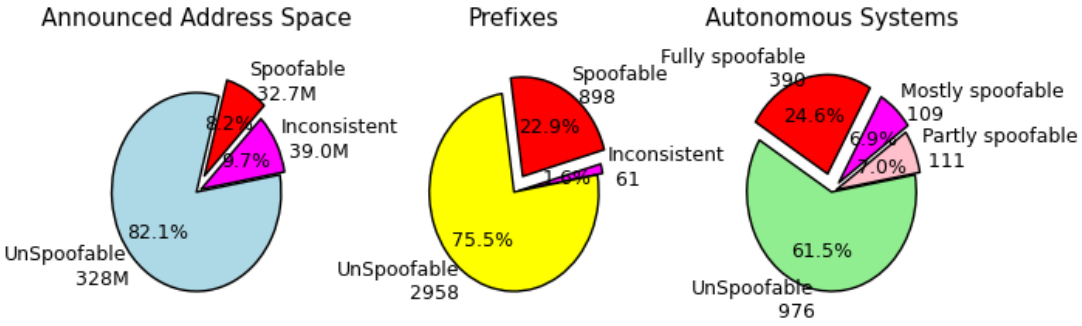
Ascertaining spoofing capability with perfect precision would require instrumenting every independent network on the Internet — an unlikely proposition, at least for an academic research project. Our approach was to develop a measurement software client that volunteers across the Internet could download and run from their networks, testing their own ability to send various types of spoofed packets from their network to our server, which collects and aggregates test results. We have maintained and operated this Spoofer measurement infrastructure for about eight years, using the resulting data to inform the continuing debate on how many networks on the Internet permit spoofed source address packets to exit their networks. We publish aggregated data analysis and summary statistics via our State of IP Spoofing summary page, with several more detailed academic publications. *Based on our collected data, we estimate that today approximately 25% of all autonomous systems (ASes) permit spoofing.* The nature of this vulnerability means that a malicious actor does not need most, or even many, networks to be vulnerable in order to use those networks to do damage. Because existing source address validation filters must be placed near the edge of the network to be effective, a single unfiltered ingress point typically provides a means to circumvent global spoofing protection mechanisms. Thus, even a single network that supports spoofing is an attack surface; thousands of them is a much larger surface. In fact, malicious code can test for spoofing capability, in a similar fashion to our work, to ascertain which hosts, in e.g. a botnet, can be utilized to spoof.

We generally hear two polar reactions to our data, analysis, and inferences: those who think we are drastically underestimating the ability to spoof, and those who think we are overestimating spoofing capabilities. While we trust our own analysis, we emphasize that several factors, inherent to many other Internet measurement efforts as well, can contribute to sample and result bias. Without a doubt, obtaining more robust statistics and higher confidence in results will require additional strategically gathered data points. The first critical issue is the sparsity of our collected data, which we have thus far gathered from only approximately 8,000 BGP-announced IP network prefixes and 2,500 ASes. While significant, this coverage is small relative to the size of the Internet, which limits the robustness of any extrapolation. Another issue is that our measurement client must run with administrative privilege to send raw packets (or Ethernet frames to avoid operating system restrictions), which requires relatively technically savvy volunteers willing to run (untrusted) code. While we have been successful in obtaining a dataset that is diverse and well-stratified in many dimensions: geography, across TLD DNS domains, access media, relative to other sample populations, etc (see section 4.2 of our IMC 2009 paper), even more diverse and thus broadly representative data will strengthen our inferences. We have efforts underway to obtain more data, and hope to report on results of those efforts in the future.

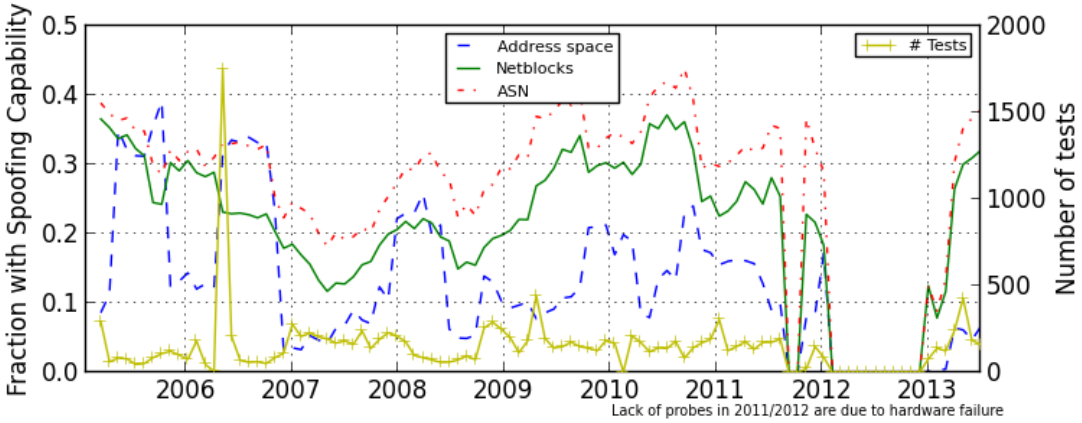
In the meantime, we have improved our published spoofing data analysis in order to provide more detailed results with increased analysis transparency. For instance, a subtlety not immediately apparent in aggregated results we have made available to the community thus far is the prevalence in our data of *inconsistent tests* from the same provider, network, or AS. Consider two samples gathered from different clients within the same AS, one of which indicates the ability to spoof, while the other shows an inability. Do we use the most recent result to label the AS, assuming that the AS has implemented source address validation filtering of some type? Or, do the two clients in fact come from different customers of the same AS (which aggregate into a single announcement from that AS into the globally visible BGP table), but with different filtering policies? In contrast, a single client that submits two results, the first showing spoofing capability and the second showing blocking, is more likely to indicate an instance of a network administrator using our test as a tool to diagnose her network and implement new policy.

To better understand such inconsistencies in our data, we divide our analysis of spoofing capability into those samples that map unambiguously (either can spoof or cannot spoof) versus those that are inconsistent relative to other samples within the same prefix or AS. To filter out policy changes, we use only the most recent valid test result from a given client IP, and only the most recent 12 months of client data for each prefix. To infer the spoofing status of the network prefix to which the client's IP address belongs, we map clients to their prefix as visible in the Route Views global BGP table. To infer the status of ASes, we count the status of each network prefix a given AS announces into the BGP table, and compute the fraction of prefixes that permit spoofing versus total tested prefixes from the AS in question.
Using this methodology, we infer 390 of 1586 (24.6%) of ASes observed within the last 12 months as "fully spoofable" and 976 (61.5%) as "unspoofable." The remaining 220 (13.9%) of ASes are inconsistent. We divide these inconsistent ASes into those with

fewer than half of their prefixes being spoofable versus those with at least half of their prefixes spoofable, labeled “partly spoofable” and “mostly spoofable” respectively. The following revised pie charts, now available in our summary spoofing report, include both consistent and inconsistent results:



Next we perform and publish a basic temporal (time-series) analysis of our data, to explore how spoofing abilities have changed over time. Previously, we have hesitated to publish such temporal analysis because the rate at which clients download the spoofer client and run tests is bursty, with bursts typically immediately following some appearance of the project URL in the press or blogosphere. Instead, to make more robust comparisons, for our IMC 2009 paper, we analyzed two discrete 3-month windows of time corresponding to flash crowds in our data in 2005 and 2009. Comparing these two sample sets, we found that the fraction of sessions that were able to spoof increased from 2005 to 2009 from 19% to 30%.
However, due to popular request, our latest analysis explores the evolution of spoofing, as observed in our data, across the entire duration of the project. The following figure plots an updated temporal analysis, computing the “spoofing capability” metric as we described earlier, and using a 6-month sliding window that proceeds in one-month steps over the duration of our collected data. (The lack of data in 2012 was due to a hardware failure.)



This plot reveals several interesting features of the data. First, while our results are noisy, they are relatively stable over time (using a 6-month sliding window). Second, there is no dominant trend, either up or down, in the fraction of ASes, prefixes, or overall

address space that can transmit spoofed traffic. This lack of progress suggested by this data is consistent with our 2005 analysis, where we explained the misalignment of incentives to prevent spoofing: an IP network infrastructure provider deploying filtering mechanisms to prevent spoofing (e.g.,BCP38) does not add any protection to their own network but increases their own operational costs.

As a courtesy to network operators, we also now provide the ability to generate a customized report of the state of IP spoofing for a given netblock or AS. To prevent misuse, we only send reports to a WHOIS registry point of contact email address the requested netblock or AS.

We are excited to continue to run the spoofer project. We hope to promote network hygiene and continue to usefully inform not only technical anti-source spoofing efforts, but also debate and policy surrounding IP spoofing. In the near term, we hope to collaborate with RIPE to obtain additional measurement sources in Europe. In the longer term, we have several students working on ways to improve the sample representativeness issue, including ways to incent measurements from parts of the topology underrepresented in our data. Feedback from the community is always more than welcome.