

Economics of Security
Final Assignment block 2 - Group 2
Source Address Validation

University of Twente

Akbar Aryanto (s1770705), Amit Gupta (s1637614), Jonathan Quigley (s1844261),
Manish Kumar (s1858882), Vasileios Merdis (s1789309),


Introduction

Nowadays, IP source address forgery, or spoofing, is a well known aftermath of the Internet's lack of packet-level authenticity. Although, many efforts for filtering and tracing have been taken place during the past years, attackers continue to employ spoofing for anonymity and cheating.

It's because the Internet forwards packets according to the IP destination address, packet forwarding typically takes place without inspection of the source address and malicious attacks have been launched using spoofed source addresses. Spoofed DDoS attacks are just one kind, among others.

In an effort to enhance the Internet with IP source address validation and seeking to minimize Internet's susceptibility to spoofed DDoS attacks, there is an open-source tool "Spoofers" from CAIDA that was developed to assess and report on the deployment of source address validation (SAV) best anti-spoofing practices.

This project includes applied research, software development, new data analytics, systems integration, operations and maintenance, and an interactive analysis and reporting service.



Center for Applied Internet Data Analysis

HOMERESEARCHDATATOOLSINTERACTIVEPUBLICATIONSWORKSHOPSPROJECTSFUNDING

Recent tests

[Spoofers Project Page](#) [Download](#) [FAQ](#) |
| **Data:** [Stats Summary](#) [Recent Tests](#) [Results by AS](#) [Results by Country](#) |

Result filters:
ASNs: Country codes: ☐ Exclude NAT ☐ Only show spoofing [Change filters](#)

Session	Timestamp	Client IP	ASN	Country	NAT	Spoof Private	Spoof Routable	v4 Adjacency Spoofing	Results
71087	2016-09-21 06:29:15	80.100.158.x	3265 (XS4ALL-NL)	nld (Netherlands)	yes	rewritten	rewritten		Full report
		2001.984.:x	3265 (XS4ALL-NL)		no	blocked	blocked	none	
71086	2016-09-21 06:28:34	73.163.170.x	7922 (COMCAST-7922)	usa (United States)	yes	blocked	blocked	none	Full report
71084	2016-09-21 06:12:06	65.205.30.x	701 (UUNET)	usa (United States)	yes	unknown	unknown	none	Full report
71083	2016-09-21 06:04:44	212.88.118.x	20294 (MTN-UGA)	uga (Uganda)	yes	unknown	unknown	none	Full report
71082	2016-09-21 05:57:56	87.192.78.x	25441 (IBIS-AS)	irl (Ireland)	yes	blocked	blocked		Full report
		2001.770.:x	1213 (HEANET)		no	blocked	blocked	none	
71081	2016-09-21 05:57:21	192.0.47.x	16876 (ICANN-DC)	usa (United States)	yes	blocked	received	/8	Full report
71080	2016-09-21 05:57:13	173.239.198.x	20473 (AS-CHOOPA)	sgp (Singapore)	yes	blocked	blocked	none	Full report
71078	2016-09-21 05:49:29	50.140.19.x	7922 (COMCAST-7922)	usa (United States)	yes	rewritten	rewritten	none	Full report
71076	2016-09-21 05:28:24	118.41.227.x	4766 (KIXS-AS-KR)	kor (South Korea)	no	blocked	blocked	/11	Full report
71075	2016-09-21 04:59:17	154.118.18.x	37340 (Spectranet)	nga (Nigeria)	yes	unknown	unknown	none	Full report
71074	2016-09-21 04:57:41	222.103.100.x	4766 (KIXS-AS-KR)	kor (South Korea)	no	blocked	blocked	/11	Full report
71072	2016-09-21 04:43:55	59.25.156.x	4766 (KIXS-AS-KR)	kor (South Korea)	no	blocked	blocked	/11	Full report
71070	2016-09-21 04:40:57	217.165.153.x	5384 (EMIRATES-INTERNET)	are (United Arab Emirates)	yes	rewritten	rewritten	none	Full report
71069	2016-09-21 04:34:13	23.28.214.x	12083 (WOW-INTERNET)	usa (United States)	yes	blocked	blocked	none	Full report

Who can make use of this paper?

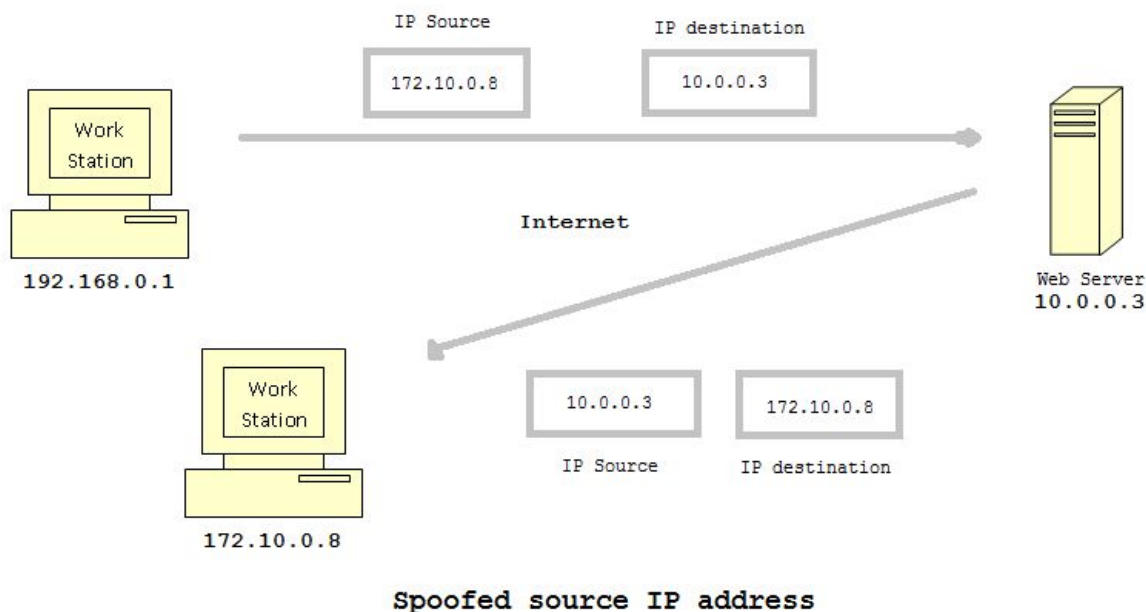
This research will primarily help the Internet Service Providers (ISP) to understand the current situation of the global network systems vulnerable to age old DDoS Attack. Based on the information the ISPs can take corrective measures and investments to immune their servers from these cyber attacks. Thereby, creating a stronger, not just more ethical but also better performing inter-networks.

In particular what we are looking in this Project is to produce useful reports and visualizations of the metrics that can help decision makers to pinpoint the best area to invest.

Problem

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a web site, hijack browsers, or gain access to a network. IP spoofing is one of the most common forms of on-line camouflage.

Because the Internet forwards packets according to the IP destination address, packet forwarding typically takes place without inspection of the source address and malicious attacks have been launched using spoofed source addresses. IP Spoofing designates the alteration of the source address in IP packets, in order to fake the sender's identity.



This kind of attack can be used in the context of Denial of Service (DoS) attacks or Distributed Dos (DDoS) by sending data packets to a machine with the address of the victim. The receiver of the packets will then answer to the victim instead of the original sender. Also sometimes the response can be of a bigger size.

Scientists have been continuously putting their effort to enhance the Internet with OP source address validation techniques over IPV4 and IPV6. There have been many efforts in the research to evaluate mechanisms related to the validation of source IP addresses. One important mechanism is the ingress filtering.

Security Issue Dataset speaks about

The dataset taken into consideration for this research intends to provide a current aggregate view of ingress and egress filtering and IP Spoofing on the Internet.

While the data in this report is the most comprehensive of its type we are aware of, it is still an ongoing, incomplete project. So it's safe to assume all the finding that we share in this report does not represent full picture of respective country, area or entity we are talking about. Instead all the calculations must be taken as a full picture of available data from the test run only.

The data here is representative only of the netblocks, addresses and autonomous systems (ASes) of clients from which CAIDA has received reports. The more client reports they receive the better increase our accuracy of coverage it became.

Background

The Center for Applied Internet Data Analysis (CAIDA), is an organization funded by the U.S. Department of Homeland Security Science and Technology Directorate. Its mission is to conduct research in macroscopic usage and behavior of the Internet. CAIDA's aim is to improve the security and the stability of the global cyber environment, by conducting several projects of data monitoring and connectivity mapping. The results of these projects are then shared with governments and commercial organizations in order to take countermeasures to the vulnerabilities which may have strong impact towards creating a dependable global network.

One of these projects, called Spoofer, focuses on IP Spoofing vulnerabilities. Seeking to minimize Internet's susceptibility to spoofed DDoS attacks, the organization is developing and supporting open-source software tools to assess and report on the deployment of source address validation (SAV) best anti-spoofing practices. As a collaborative project, the tester client is available to any end user, to maximise the coverage of the results.

Methodology

We are using the data provided by *Spoofer*.

Spoofer produces its results by using a client, available for any end user. When running it, your machine sends UDP packets to CAIDA servers to test your network in different ways:

- the ability to spoof with a private class address (RFC 1918), with a routable address, in IPv4 and IPv6;
- the range of neighboring addresses you are able to spoof (IPv4 only);
- the AS path taken by the packets, and whether the filtering is observed on this path (IPv4 only);
- the presence of a NAT device on your network. In this case, the spoofed address may be rewritten, or the device just lets the packet pass.

The results of these tests are then uploaded to the project website, where the records of all users can be found. The data is available for approximately the last 6 months, but it still represents a large amount of records. Thus, we decided to focus on a few countries, which we believe, represent the global context.

After downloading the records of these countries, we decided on which parameter we were going to base our metrics. The available parameters are :

1. Presence of NAT: as the presence of a NAT device does not assure you that spoofing is not possible, we can not use it as an indicator. Plus, NAT does not allow to test fully your network, as it sometimes rewrites the source address. In consequence, the records are not exploitable when a NAT is detected, and that is why we chose to exclude them from our analysis.
2. Private spoofing ability: using a private address is a subpart of the main issue, as less than 40 records out of 20000 show the case where you can spoof using a private address but not a routable one. Otherwise, if you are able to spoof using a private address, it applies to routable addresses as well.
3. Routable spoofing ability: most representative parameter of the problem. The test is positive if packets sent with a routable spoofed address are received by CAIDA's Ark servers.
4. Range of adjacency spoofable addresses: also a valuable parameter. Sometimes the packets are blocked and are not received by the CAIDA servers, but you are still able to spoof within a range of neighboring addresses. This means that the threat of DDoS attacks is still present for a part of the network you are connected to. Therefore, our analysis should provide some measurements about the range of potential attacks based on spoofing.

Ideal Metrics

For decision makers of a company, ideal metrics should provide them sufficient information to invest in some solution or not, to mitigate the effect of a security issue. In our case, the issue is the ability to spoof IP addresses within the company's network. The consequence of this problem is that it allows to perform anonymous DDoS attacks, by hiding the real source address of the attacker.

First, the decision makers could think that DDoS attacks are someone else's problem, as they are not the target. But still, it affects their network by consuming bandwidth which is not available for their

customers. This cost, in terms of performance, represents a metric which could be used in order to promote the establishment of a solution against IP spoofing. However, it is very hard to measure it, because of its stochastic nature.

In addition, allowing spoofed traffic on your network can get your reputation down, especially if you are part of a minority in your geographical area. This is applicable to your customers, who will maybe prefer one of your concurrents over you if they are impacted by spoofing. Plus, in the case of agreements with other AS, we can infer that companies would more likely make peering or transit contracts with you if your network is not spoofable. Consequently, this potential loss of business is another metric for a company which allows spoofing on its network. It is yet difficult to quantify it, as the decisions of the customers and other ISP are subjective, and depend on their own economical situation.

For national policy makers, one of their objectives is to improve the quality of their national cyberspace. Thus, spoofing is one of the issues they are fighting against. As said previously, ISP are the only actors able to mitigate this problem, so national agencies can only urge them to do so. This can be made by legislating, for instance imposing a fine for ISP which allow spoofed traffic on their network. In order to measure the improvement occurred by the policy, an ideal metric would be the evolution of the issue over the years. For example, the percentage of ISP using filtering since the fine has been established. The Spoofer project could be a source of this data, but the records depends on the number of users who run it, so it would need people to run it multiple times for every ISP of the country to have a reliable metric.

Metrics in practice

Source Address Validation (SAV) is often referred as an example of the “Tragedy of the commons”¹. Indeed, the small gain of an ISP made by not spending on a SAV solution is a loss for the whole cyber community, by spreading spoofed traffic.

There is a prevalent false idea for ISP about the cost of implementing an anti-spoofing solution, because of the supplementary equipment needed. This could have been true a few years ago, but solutions like BCP 38 can now be supported by a majority of routers ISP use². Still it costs money, albeit a very small amount. That’s why not all the network operators are willing to install filters. The argument of buying new equipment can yet apply to some ISP which reuse their old reconditioned equipment.

1

https://www.caida.org/publications/presentations/2016/software_systems_surveying_spoofing_ausnog/software_systems_surveying_spoofing_ausnog.pdf

2

<http://www.internetsociety.org/deploy360/blog/2014/07/anti-spoofing-bcp-38-and-the-tragedy-of-the-commons/>

The main problem is the inadequate business case. ISPs don't think that they will benefit directly by deploying anti-spoofing mechanisms that overdraw the costs and the risks related to them. For example, even if a network uses ingress filtering to prevent spoofing, it still can be used by attackers to accomplish their missions. So, even if a network operator will install an anti-spoofing filter, it will not guarantee 100% safety.

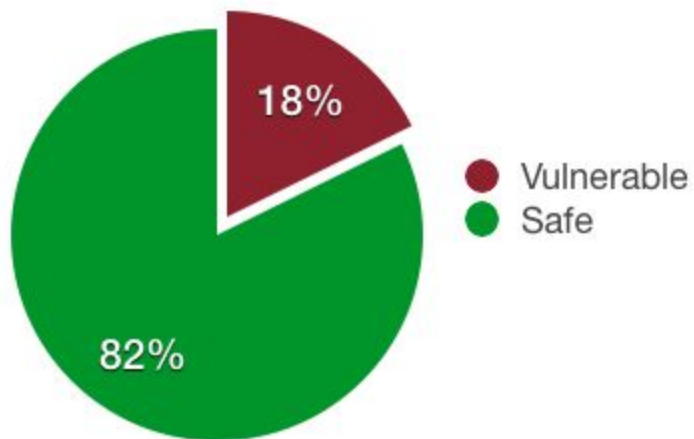
Define Metrics

Current condition ASN in Netherlands

We analyse 192 IP address from the dataset since 9 February 2016 until 30 September 2016. We find the result 158 IP address is safe and can't be spoofed in the networks, on the other hand, we find 34 IP address is vulnerable because the result that IP address can be spoofed in the networks. From the graph below we can see 82 percent of ASN in Netherland safe from the spoofed.

ASN in Netherlands

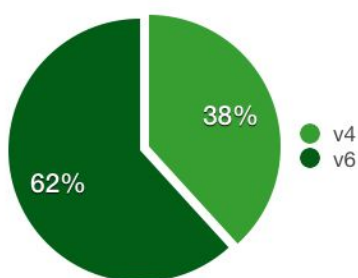
TOTAL	
Vulnerable	34
Safe	158



Safe and Vulnerable ASN in Netherland based on IP version

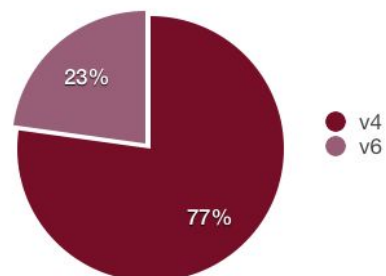
Safe ASN

IP VERSION	TOTAL
v4	13
v6	21



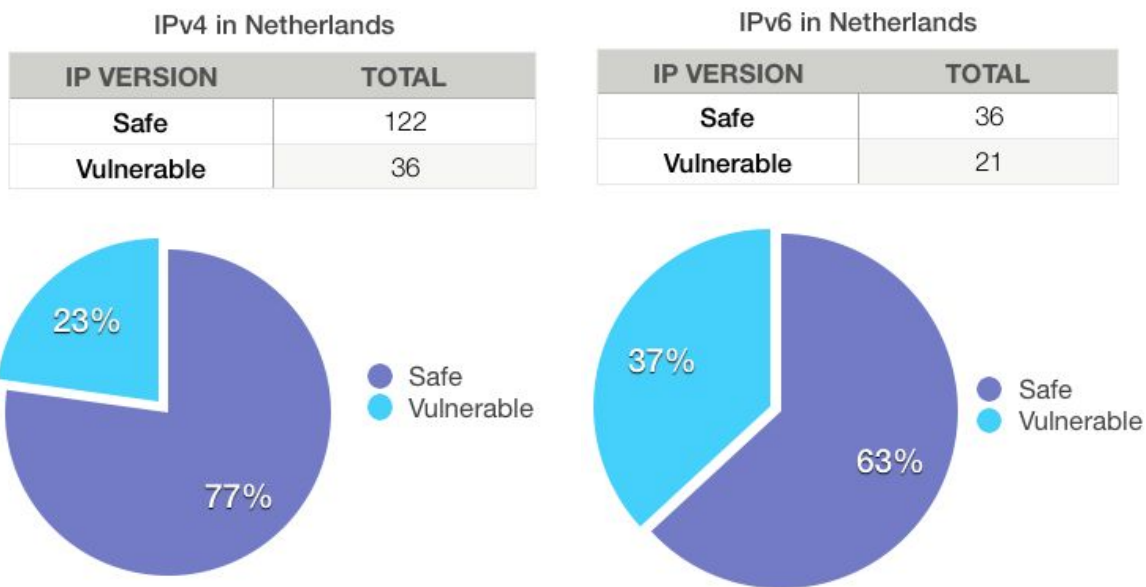
Vulnerable ASN

IP VERSION	TOTAL
v4	122
v6	36



Comparison IPv4/v6

The Spoofer client provides tests using IPv6, if the operator's network allows it. We decided to check if ISP which implemented SAV on their network for IPv4 did it for IPv6 as well. We measured the number of positive and negative tests for both versions, in order to compare them. As IPv4 is still the most used protocol (about 90% of the Internet users) and the oldest in place, we could expect it to be safer than its newer version. This supposition appears to be true, as only less than one quarter of the tests are positive with IPv4, versus 37 percent for IPv6. This can be explained by the relative novelty of the version 6. For instance, ISP which implemented SAV could have begun to use IPv6 later, and forgot to deploy it for this version too.



Comparison ASN in the Netherlands

We make a ranking of ASN based on the number of customer from CAIDA website, and then we sort for top 10 safe ASN and top 10 vulnerable ASN based on their rank.

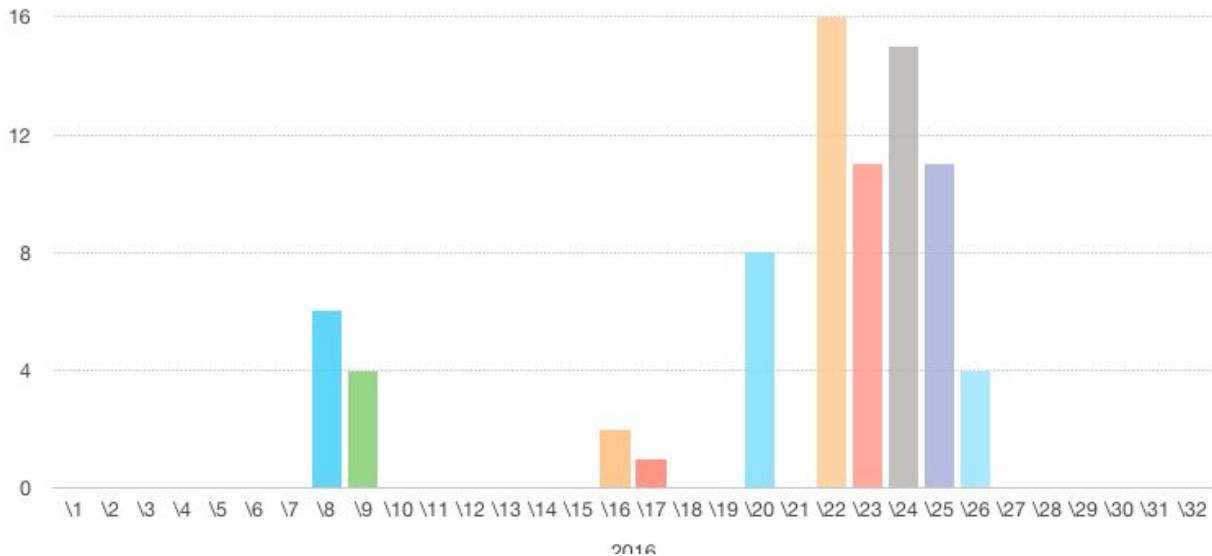
Safe ASN Rank		Vulnerable ASN Rank	
Ranking	ASNs	Ranking	ASNs
8	6939 (HURRICANE)	685	49544 (INTERACTIVE3D)
28	7922 (COMCAST-7922)	770	43350 (NFORCE)
294	42708 (PORTLANE)	982	31216 (BSOCOM)
362	50673 (Serverius-as)	1003	47869 (NETROUTING-AS)
553	1136 (KPN)	1871	48635 (PCEXTREME)
685	49544 (INTERACTIVE3D)	2543	29073 (QUASINETWORKS)
882	1103 (SURFNET-NL)	3352	49981 (WorldStream)
1003	47869 (NETROUTING-AS)	3513	60144 (THREE-W-INFRA-AS)
1871	48635 (PCEXTREME)	4456	4608 (APNIC-SERVICES)
2543	29073 (QUASINETWORKS)	7836	57062 (SERVERCLUB-AS)
3223	35017 (SWIFTWAY-AS)	9419	59743 (EliteHosting)
3352	49981 (WorldStream)	9872	200837 (PCEXTREME-UK)
1041	TOTAL AVERAGE	3859	TOTAL AVERAGE

On the other hand we make a sort the rank based on the total number of client test from the dataset.

Top 10 Safe ASN in Netherlands				Top 10 Vulnerable ASN in Netherlands			
No	ASN	Test	Result	No	ASN	Test	Result
1	199664 (NLNETLABS)	14	100%	1	1140 (SIDN)	10	0%
2	1128 (TUDELFT-NL)	11	100%	2	43350 (NFORCE)	1	0%
3	198203 (ASN-ROUETELABEL)	10	100%	3	31216 (BSOCOM)	1	0%
4	63473 (HostHatch-NA-AS)	10	100%	4	200837 (PCEXTREME-UK)	3	33%
5	202109 (DIGITALOCEAN-ASN-2)	6	100%	5	60144 (THREE-W-INFRA-AS)	9	44%
6	35017 (SWIFTWAY-AS)	6	100%	6	49981 (WorldStream)	2	50%
7	49349 (DOTSI)	5	100%	7	47869 (NETROUTING-AS)	2	50%
8	1133 (UTWENTE-AS)	5	100%	8	59743 (EliteHosting)	4	50%
9	1136 (KPN)	5	100%	9	57062 (SERVERCLUB-AS)	12	50%
10	202018 (DIGITALOCEAN-ASN-3)	5	100%	10	4608 (APNIC-SERVICES)	16	56%

Range of spoofable neighbouring addresses

Another test of the client allows to measure the number of adjacent addresses you are able to spoof. This is a relevant metric as sometimes spoofed traffic sent by the client does not reach the servers from CAIDA, but the client's network can still be used for spoofing. This happens when the traffic is blocked by another AS on the path of the packets, but not by the previous ones. We measured the percentage of each range of spoofable addresses in the following graph. We can then observe that a majority of spoofable ranges are between /20 and /26, which already represents a relative large amount of machines.



Conclusion

Within this study, we analysed the economical situation of Source Address Validation, by identifying the actors and the issues involved. We looked for the ideal metrics which could help decision makers of an ISP to invest in solutions against spoofing on their network.

We observed that this security issue is an example of the tragedy of the commons, as the implementation of SAV would only benefit the community, and represent a cost for the ISP. However, the costs of solutions like BCP 38 are constantly decreasing, and can now no more be used as an argument for not deploying it.

Finally, we exploited the dataset of results from the Spoofer project, which permits end users to test their operator's network by sending spoofed traffic. We defined metrics to analyse the behaviour of ISP given certain parameters, like their size or their type. Unfortunately, we lacked time to finish this study, in particular for the exploitation of the dataset. For instance, we first decided to focus our metrics on a few countries, but due to the short time remaining, we could only study data from Netherlands.