Economics of Security

Final Assignment - Source Address Validation

University of Twente

Vasileios Merdis (s1789309)

Abstract

This paper explains the importance of IP address spoofing and the need to implement Source Address Validation (SAV) for preventing threats. The discovery and analysis of the Dutch ASes and the correlation between the size of them, gives us the opportunity to answer the research question if there is significant correlation concerning the level of the AS in the Internet Topology. In order to extract some results we assumed two hypotheses regarding the degree of the ASes and the number of spoofable/non-spoofable IPs they are related to, and we analyzed the data that we grabbed from CAIDA. We conclude that the Dutch ASes are protected in their majority, but due to the lack of sufficient data we cannot broach the subject.

1. 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. IP spoofing is the enabling force behind Denial of Service (DoS) attacks observed in operational provider networks.

As described in the previous papers, the Network providers are the prime owners of the problem as they are in the empowered state of taking decisions which can lead to mitigate the risks. However, there are some other actors that can be influenced by the security issue. These are the countries and the victims who basically pay all the losses and bear the cost of DDoS attacks. There are many risk strategies that the actors can adopt to tackle the problem of spoofing-based denial of service (DoS) attacks. The strategies can have many positive incentives to the actors, especially for the victims. However, there are also some costs of implementing Source Address Validation (SAV); all mentioned in previous researches.

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 opensource tool "Spoofer" from CAIDA that was developed to assess and report on the deployment of source address validation (SAV) best anti-spoofing practices. Focused on the data from the Netherlands we will make a research regarding the networking system and conclude some results based on the data analysis.

2. Literature Review

Critical infrastructure protection and Internet interconnection resilience have been studied during the past decades. There are some previous research papers that are relevant to the subject we focused on, IP address spoofing, and the importance of implementing Source Address Validation (SAV).

In the paper "Source Address Validation: Architecture and Protocol Design" [1] the authors have proposed a Source Address Validation Architecture for IPv6 network to ensure that every packet received and forwarded should hold an authenticated source IP address. The architecture supports a step by step deployment and is beneficial even if it is deployed only in a single AS of the Internet. SAV filtering is a major issue as it is presented in the paper

"Understanding the Efficacy of Deployed Internet Source Address Validation Filtering" [2], published in 2009. Significant surveys have been taken place testing the provider's source address filtering and the outcoming results are of big importance. Their analysis provided an empirical basis for evaluating incentive and coordination issues surrounding Internet packet authentication strategies.

Another research on the security issue is done by R. Beverly and S. Bauer and published with the title "The Spoofer Project: Inferring the Extent of Source Address Filtering on the Internet" [3]. This paper presents an Internet wide active measurement spoofing project. Their results based on UDP packets designed to inter filtering policies revealed that some ASes permit spoofing. This means that a large portion of the Internet is vulnerable to spoofing even after filtering and that spoofing attacks, such as DDoS attacks, are a serious concern. Based on this idea the SANS Institute published an article named "Spoofed IP Address Distributed Denial of Service Attacks: Defense-in-Depth" [4], where the main point was to look at a defense-in-depth approach to spoofed IP addresses DDoS attacks including techniques like ingress and egress filtering.

Finally, the research project "Discovery and Mapping of the Dutch National Critical IP Infrastructure" [5] based on the mapping of Dutch critical infrastructure organisations, provided a list of important results concerning the Dutch links and ISPs and the connection between them. Based on these results and the data collected from CAIDA regarding to ASes in the Netherlands we will try to answer the research question on the security issue that is described below in the next section.

3. Research Question, Objective and Hypothesis

The main goal of this research project can be summarised in the following question: ***Can we discover a correlation concerning the level of the AS in the Internet Topology?***

The ASes which are present in our dataset have different positions in the global architecture of the Internet. While some of them are directly providing access to the end user, others have a role of transit deeper in the network. It seems natural to think that networks on the edge of the topology should be the first actors in the process of Source Address Validation. Indeed, the closer you get to the source of the traffic, the easier it becomes to filter it. Mainly because there is less prefixes to check. Thus, SAV becomes ineffective if it is done by ASes in the

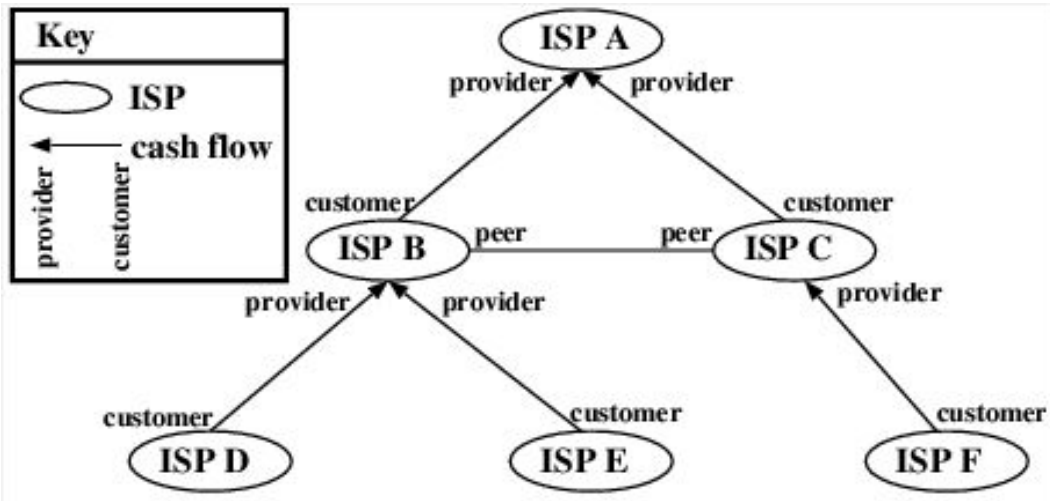
core of the network. Either it creates false positives, or it is unable to detect spoofed traffic.

According to the above we can also set additional goals defined in the following two hypothesis:

- H_0: The security performance is correlated to the level of the AS in the topology.
- H_1: The security performance is independent of the level of the AS in the topology.

4. Methodology

We considered all ASes from the Netherlands for which we have data, and collected the degree of each one. The degree is related to the number of neighbours the AS has. Consequently, we can infer that the higher the degree is, the higher is the level of the AS in the Internet topology. As we can see ASes on the edge of the network usually have one or more provider(s), and often no peering relations. They have a low degree and most of the time 0. On the other hand, ASes in the core are connected with numerous others, often by means of peering agreements, can have a high degree. Thus, we can consider ASes which have the higher number of relations, or the higher degree, as the deeper in the global network.



Example of relationships between ASes.

We will analyze the data that we have, provided by CAIDA, using the SPSS Statistics software. Although the data is limited, we will try to find a correlation between the two variables (ASes that are spoofable and non-spoofable and their degrees) and consequently to answer the research question using the hypothesis.

	Degree	
ASN	Unspoofable	Spoofable
1128 (TUDELFT-NL)	0	
20857 (TRANSIP-AS)	0	
196752 (TILAA)	0	
198203 (ASN-ROUTELABEL)	0	
199664 (NLNETLABS)	0	
200130 (DIGITALOCEAN-ASN-1)	0	
200837 (PCEXTREME-UK)		0
202018 (DIGITALOCEAN-ASN-3)	0	
202109 (DIGITALOCEAN-ASN-2)	0	
1133 (UTWENTE-AS)	0	
57043 (HOSTKEY-AS)	0	
57062 (SERVERCLUB-AS)	0	
59743 (EliteHosting)	0	
60117 (HS)	0	
63473 (HostHatch-NA-AS)	0	
57771 (STEFFANN-AS)	2	
35017 (SWIFTWAY-AS)	4	
56611 (REBACOM-AS)	4	
49349 (DOTSI)	5	
60144 (THREE-W-INFRA-AS)		6
4608 (APNIC-SERVICES)	9	
48635 (PCEXTREME)	21	
49981 (WorldStream)		60
29073 (QUASINETWORKS)		66
47869 (NETROUTING-AS)		89
31216 (BSOCOM)		98
43350 (NFORCE)		98
49544 (INTERACTIVE3D)	106	
50673 (Serverius-as)	110	

Data received from CAIDA[1]

[1] https://spoofer.caida.org/summary.php

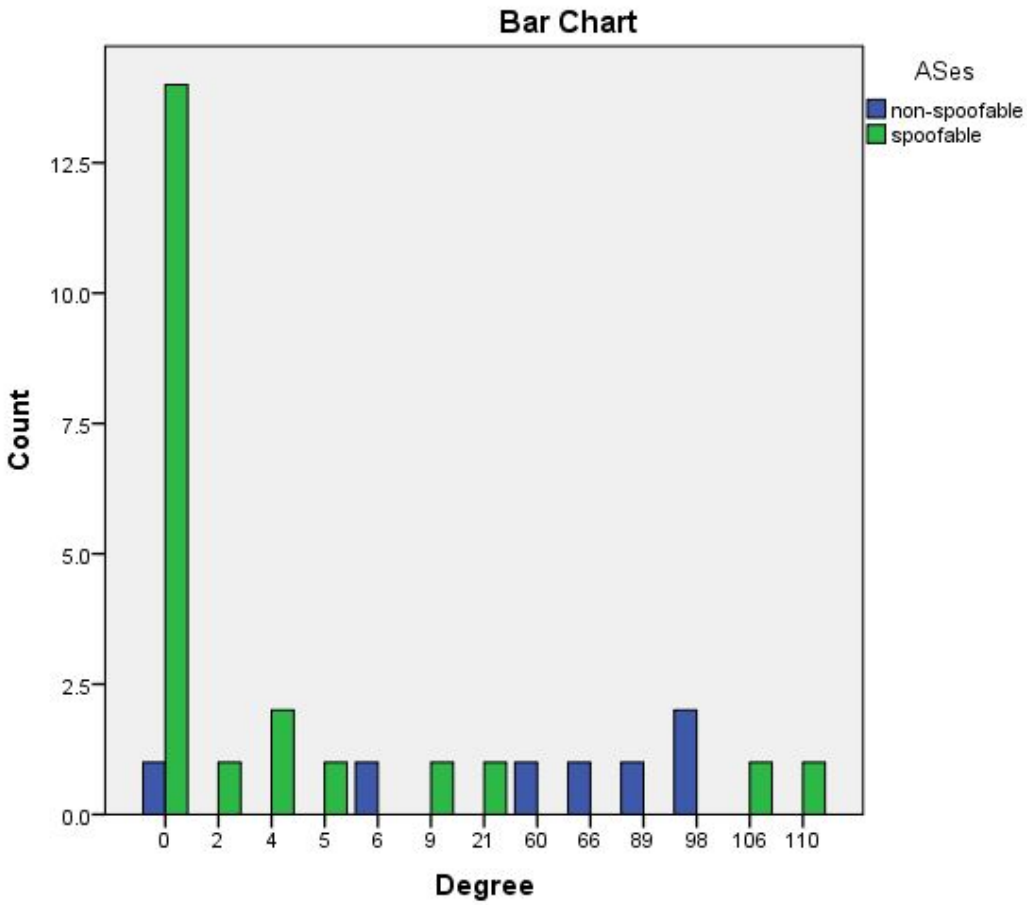
5. Results

ANOVA

ASes

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.377	12	.365	6.253	.001
Within Groups	.933	16	.058		
Total	5.310	28			

The degree of each AS differed significantly among the spoofable and non-spoofable ASes, $F(12,16) = 6.253$, $p < 0.05$. The p value (denoted by "**Sig.**") is 0.001. This means that if the spoofable and non-spoofable ASes are exactly equal, we only have a 1% chance of finding the differences that we observe in our sample. So we conclude that the number of spoofable and non-spoofable ASes, as well their size, is not equal.



On the above figure, we can observe the degree of all ASes, and their spoofability, represented by the colour of the bar. Among all those which have a null degree, only one is spoofable. A trend is remarquable on the graph, as we can see that most of the ASes with a low degree are not allowing spoofing. Conversely, all ASes with a degree between 50 and 100 are spoofable.

Correlations

		ASes	Degree
ASes	Pearson Correlation	1	-.529**
	Sig. (2-tailed)		.003
	N	29	29
Degree	Pearson Correlation	-.529**	1
	Sig. (2-tailed)	.003	
	N	29	29

**. Correlation is significant at the 0.01 level (2-tailed).

The Pearson's r for the correlation between the ASNs (spoofable and non-spoofable) and the degree of them is -0.529. That means that there is a relative strong relationship between these two variables, as the value of the Pearson's r is closer to 1. Furthermore, the Pearson's r value is negative which means that as the one variable increases in value, the second variable decreases in value, i.e. increasing the degree of ASNs, we decrease the non-spoofable IPs connecting to them. In this case, the Sig. (2-tailed) value is 0.003 which is smaller than the value 0.05. We can conclude that there is statistically significant correlation between our two variables. That means, increases or decreases in one variable, significantly relate to increases or decreases in the second variable.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	.908	.021
	Cramer's V	.908	.021
	Contingency Coefficient	.672	.021
N of Valid Cases		29	

According to the Symmetric Measures and the Phi and Cramer's V tests we can see that the strength of association between the variables is very strong. The Cramer's V and the Phi value is 0.908, very close to 1.

6. Limitations

This research will primarily help the Internet Service Providers (ISP), as well as the other actors that play a role in the security issue, 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 internetworks.

In particular what this paper is focused on, is to produce useful reports and visualizations of the metrics that can help decision makers to pinpoint the best area to invest. A future work should be focused on implementing a countermeasure where all the actors can at least benefit the mitigation of the security issue. This countermeasure should be ingress filtering, as analyzed in previous papers. Future researchers should take into consideration the research that made upon the Dutch ASes and by giving them more sufficient data they will be able to mitigate the risks of IP spoofing based on DDoS attacks.

7. Conclusions

In this paper we mentioned the importance of the Source Address Validation (SAV) against the IP spoofing. 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.

After the statistical analysis of the data that we got from CAIDA, we can verify the null hypothesis that the security performance is correlated to the level of the AS in the Internet topology. Furthermore, we proved that the most of the ASes with a low degree are not allowing spoofing. Although, due to limited data we are not in a position to conclude safe results, we partially answered the research question concerning the security issue. A significant correlation concerning the level of the AS in the Internet Topology was discovered.

A clear conclusion is that the Network Providers, who are the problem owner of this security issue, should implement ingress filtering in order to mitigate spoofed IP address DDoS attacks in the future.

References

[1] Jianping Wu, Gang Ren, Xing Li. *Source Address Validation: Architecture and Protocol Design* (2007)

[2] Robert Beverly, Arthur Berger, Young Hyun, k claffy. *Understanding the Efficacy of Deployed Internet Source Address Validation Filtering* (2009)

[3] Robert Beverly, Steven Bauer. *The Spoofer Project: Inferring the Extent of Source Address Filtering on the Internet* (2005)

[4] SANS Institute InfoSec Reading Room. *Spoofed IP Address Distributed Denial of Service Attacks: Defense-in-Depth* (2001)

[5] Fahimeh Alizadeh, Razvan C. Oprea. *Discovery and Mapping of the Dutch National Critical IP Infrastructure* (2013)