

Economics of security

Individual Assignment

Manish Kumar (s1858882)

Final Paper

Date: Nov 16, 2016

Abstract

This paper sheds light on a rapidly growing issue Distributed denial-of-service (DDoS) especially the ones caused by spoofed IP packets. This paper further tries to proof a relationship between the AS and IP spoofing by analyzing many factors like size and type etc of the ASNs. The multitude and variety of both the attacks and the defense approaches are overwhelming. The key findings of this paper are a survey on the problem of denial-of-service (DoS) and Distributed Denial of Service (DDoS) attacks and proposed ways to deal with it. Further this paper describes the nature of the problem and looks for its root causes and suggested approaches for defending against DDoS. i.e ingress filtering. The analyses done in this paper are solely based on the data collect only from netherlands. The collective analysis of global situation can farm a totally different picture. Which i propose for future researchers.

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 but attackers continue to employ IP spoofing for their benefits and it remains one of the most common forms of online camouflage.

Massive East Coast Internet Outage[1], A repel massive DDoS attack on 5 major Russian banks[2][3] and largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices[4] in september are just few examples in last two months. In recent months DDoS attacks are increasing exponentially. And it's always very complex, expensive and tedious task to analyse the exact lose by such attacks.

These attacks are happening because the Internet forwards packets according to the IP destination address, packet forwarding typically takes place without inspection of the source address. In result of which malicious attacks have been launched using those spoofed source addresses.

IP Spoofing designates the alteration of the source address in IP packets, in order to fake the sender's identity or at time also amplify the attack with DNS amplification.

DNS Amplification Attacks are a way for an attacker to magnify the amount of bandwidth they can target at a potential victim. Imagine you are an attacker and you control a botnet capable of sending out 100 Mbps of traffic. While that may be sufficient to knock some sites offline, it is a relatively trivial amount of traffic in the world of DDoS.

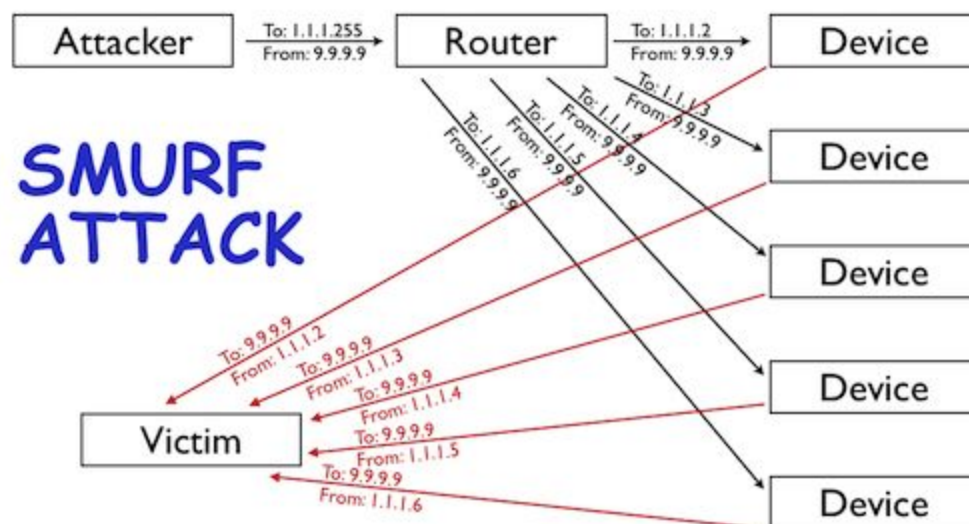
In order to increase your attack's volume, you could try and add more compromised machines to your botnet. That is becoming increasingly difficult. Alternatively, you could find a way to amplify your 100Mbps into something much bigger.[5]

And that's where the ip spoofing comes in handy. Like A SMURF attack involves an attacker sending ICMP requests (i.e., ping requests) to the

network's broadcast address (i.e., X.X.X.255) of a router configured to relay ICMP to all devices behind the router.

The attacker spoofs the source of the ICMP request to be the IP address of the intended victim. Since ICMP does not include a handshake, the destination has no way of verifying if the source IP is legitimate.

The router receives the request and passes it on to all the devices that sit behind it. All those devices then respond back to the ping. The attacker is able to amplify the attack by a multiple of how ever many devices are behind the router (i.e., if you have 5 devices behind the router then the attacker is able to amplify the attack 5x, see the figure 1 below).



Figure[1] Diagram Explaining SMURF/DNS Amplification attack. [5]

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.

Researchers have been continuously putting their effort to enhance the Internet with applying source address validation techniques over IPV4 and IPV6.

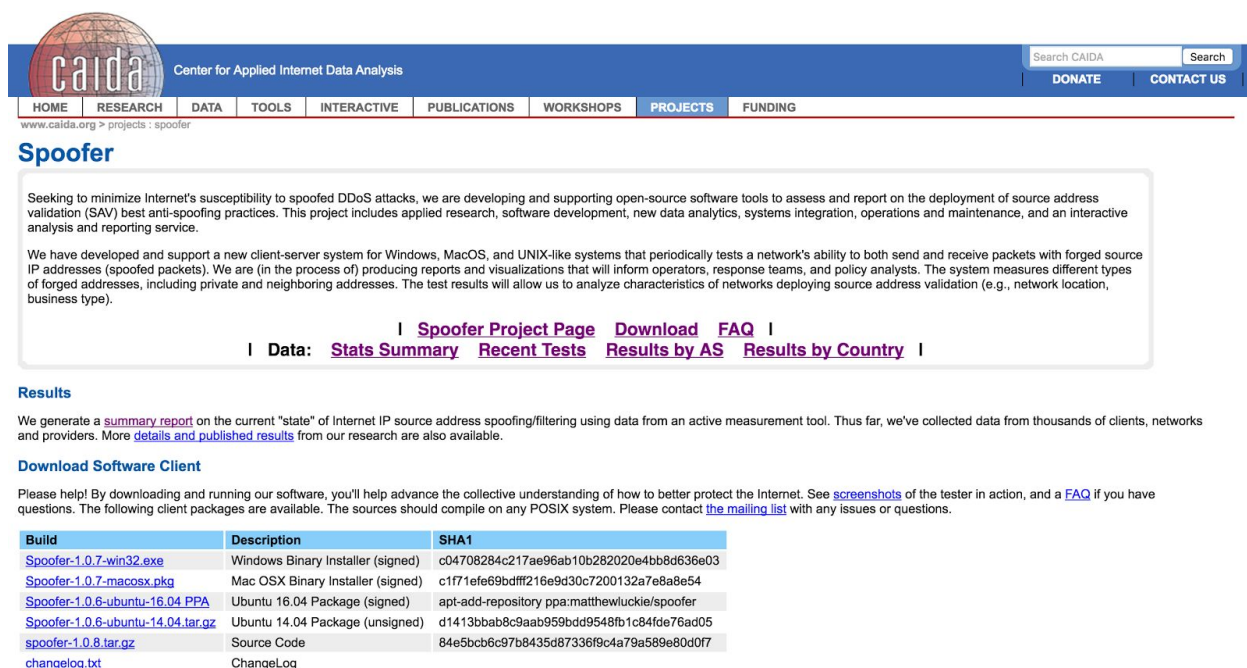
There have been many efforts in the research to evaluate mechanisms, and that's the purpose of this report as well. If and what are they methods to

stop or decrease the IP Spoofing, and what is feasibility to deploy them in real world.

In this report we are using the data provided from an opensource tool "Spoofers" and "As Rank" from CAIDA that was developed to assess and report on the deployment of source address validation (SAV) best anti spoofing practices.[6][7]

Which was built in an effort to enhance the Internet with IP source address validation and seeking to minimize Internet's susceptibility to spoofed DDoS attacks.

This project includes applied research, software development, new data analytics, systems integration, operations and maintenance, and an interactive analysis and reporting service. [6]



CAIDA Center for Applied Internet Data Analysis

Search CAIDA

[DONATE](#) [CONTACT US](#)

[HOME](#) [RESEARCH](#) [DATA](#) [TOOLS](#) [INTERACTIVE](#) [PUBLICATIONS](#) [WORKSHOPS](#) [PROJECTS](#) [FUNDING](#)

[www.caida.org](#) > projects : spoofers

Spoofers

Seeking to minimize Internet's susceptibility to spoofed DDoS attacks, we are developing and supporting open-source software tools 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.

We have developed and support a new client-server system for Windows, MacOS, and UNIX-like systems that periodically tests a network's ability to both send and receive packets with forged source IP addresses (spoofed packets). We are (in the process of) producing reports and visualizations that will inform operators, response teams, and policy analysts. The system measures different types of forged addresses, including private and neighboring addresses. The test results will allow us to analyze characteristics of networks deploying source address validation (e.g., network location, business type).

[| Spoofers Project Page](#) [Download](#) [FAQ](#) [|](#)

[| Data:](#) [Stats Summary](#) [Recent Tests](#) [Results by AS](#) [Results by Country](#) [|](#)

Results

We generate a [summary report](#) on the current "state" of Internet IP source address spoofing/filtering using data from an active measurement tool. Thus far, we've collected data from thousands of clients, networks and providers. More [details and published results](#) from our research are also available.

Download Software Client

Please help! By downloading and running our software, you'll help advance the collective understanding of how to better protect the Internet. See [screenshots](#) of the tester in action, and a [FAQ](#) if you have questions. The following client packages are available. The sources should compile on any POSIX system. Please contact [the mailing list](#) with any issues or questions.

Build	Description	SHA1
Spoofers-1.0.7-win32.exe	Windows Binary Installer (signed)	c04708284c217ae96ab10b282020e4bb8d636e03
Spoofers-1.0.7-macosx.pkg	Mac OSX Binary Installer (signed)	c1f71efe69bdf216e9d30c7200132a7e8a8e54
Spoofers-1.0.6-ubuntu-16.04 PPA	Ubuntu 16.04 Package (signed)	apt-add-repository ppa:matthewlueckie/spoofers
Spoofers-1.0.6-ubuntu-14.04.tar.gz	Ubuntu 14.04 Package (unsigned)	d1413bbab8c9aab959bdd9548fb1c84fde76ad05
spoofers-1.0.8.tar.gz	Source Code	84e5bcb6c97b8435d87336f9c4a79a589e80d0f7
changelog.txt	ChangeLog	

Figure[2] Spoofers Project from Caida [6]

Literature Review

As mentioned, Researchers have been continuously putting their effort to enhance the Internet with applying source address validation techniques over IPV4 and IPV6. Following are some of their efforts and insights about IP spoofed DDos Attack, Source Address Validation and other techniques.

The literature review brought light over a lot of valuable approaches towards the problem, and introduced new evidences for the types of variables selected. It introduced with plenty of effective approaches for detection and some unique insights and angles on prevention techniques. Like one paper would suggest a multilayer protection strategy and an other claims their solution to be 20% cheapest of the available solutions in market let alone their accuracy claim is to be 90%.

It also proves that the major improvement in this area still remains to be done to prevent IP Spoofed DDoS attacks. Here below is my details literature review each paper wise.

1. Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches by Darshan Lal Meena and Dr. R. S. Jadon[8]

Starting with a paper published in 2014, Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches by Darshan Lal Meena and Dr. R. S. Jadon

This paper was a survey on the problem of Distributed Denial of Service (DDoS) attacks and proposed ways to deal with it. It expends on describing the nature of the problem and look for its root causes, further presenting brief insights and suggested approaches for defending against DDoS.

It not only points out positive but also negative sides of each potential solution. Further this paper, also presents a classification of available mechanisms that are proposed in literature on preventing Internet services

from possible DDoS attacks and discuss the Five Principal for DDos defense to build an effective solution

This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention mechanisms for fighting against DDoS threat.

1. DDoS is a distributed attack and because of high volume and rate of attack packets, distributed instead of centralized defense is the first principle of DDoS defense.
2. High Normal Packet Survival Ratio (NPSR) hence less collateral damage is the prime requirement for a DDoS defense.
3. A DDoS defense method should provide secure communication for control messages in terms of confidentiality, authentication of sources, integrity and freshness of exchanged messages between defense nodes.
4. As there is no centralized control for autonomous systems (AS) in Internet, a partially and incrementally deployable defense model which does not need centralized control will be successful.
5. A defense system must take into account future compatibility issues such as interfacing with other systems and negotiating different defense policies.

2. Spoofed IP Address Distributed Denial of Service Attacks: Defense-in-Depth[9] by SANS Institute InfoSec Reading Room.

Second paper that I reviewed is Spoofed IP Address Distributed Denial of Service Attacks: Defense-in-Depth by SANS Institute InfoSec Reading Room.

This paper also sheds more light on the my research question and is related to the paper discussed earlier but it differs because it looks at a defense-in-depth approach for only spoofed IP address DDoS attacks, including known defenses, new techniques, and recent developments but all of it without creating limitations in performance or scalability.

The paper particularly talks about solutions like, Ingress Filtering, Ingress Filtering on Cisco Routers, Ingress Filtering on Juniper Routers, Ingress Filtering Verification, Traceback, Intelligent Network Management, Backbone-Layer Security, Egress Filtering, Egress Filtering on Cisco Routers, Host-based Defense, Host-Based Anti-Tools and Recent Developments with Windows XP.

The paper further presents that the Defenses against DDoS attacks depend upon the Internet community working together. With ISP's, customer network administrators, hardware and software manufacturers, and Internet security professionals implementing defense in depth best practices, together we can reduce and/or hopefully stop DDoS attacks. Which we believe is true because it resonates with the findings we have had during our course assignments.

3. DDoS Attacks Impact on Network Traffic and its Detection Approach[12]

This paper was not strongly related to IP Spoofed attacks but it has one very unique aspect over other papers that i've reviewed for this report. The aspect is that it's talks about the impact on network traffic from DDoS attacks. Which i found very helpful in relation to the benefits that network providers can get by implementing source address validation or any other solution for that matter. Because those are the ones who bear the cost behind the solutions.

Further after reading the paper i found out that, This paper has studied a DDoS attack to analysis the distribution of network traffic to recognize the normal network traffic behavior. It has also discussed flooding attacks along with the EM algorithm which approximates the distribution parameter of gaussian mixture distribution model.

It further goes on discussing a method to recognize anomalies in network traffic, based on a non restricted α - stable model and statistical hypothesis testing.

4. Distributed Denial of Service Prevention Techniques by B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE [10]

This third paper talks about the significance of the DDoS problem and the increased occurrence, sophistication and strength of attacks, which has led to the dawn of numerous prevention mechanisms.

Each proposed prevention mechanism in this paper had some unique advantages and disadvantages over the others. Also this paper, presents a classification of available mechanisms that are proposed in literature on preventing Internet services from possible DDoS attacks and discuss the strengths and weaknesses of each mechanism.

The paper also proposes one interesting direction to develop a comprehensive solution that encompasses several defense activities to trap variety of DDoS attack. If one level of defense fails, the others still have the possibility to defend against attack. A successful intrusion will requires all defense level to fail.

5. Detecting and Preventing IP-spoofed Distributed DoS Attacks from International Journal of Network Security 7 · January 2008[11]

This paper also explores more on mechanisms for defending against Distributed Denial of Service (DDoS) attacks but the reason I selected this is that it's specifically focusing on the prevention of my research topic — the most harmful and difficult to detect DDoS Attacks, those that use IP address spoofing to disguise the attack flow.

It proposes a novel scheme for detecting and preventing the attack. Their scheme is based on a firewall that can distinguish the attack packets (containing spoofed source addresses) from the packets sent by legitimate users, and thus filters out most of the attack packets before they reach the victim.

Unlike other packet-marking based solutions, that i've studied during my research, their scheme has a very low deployment cost; They estimate that an implementation of this scheme would require the cooperation of only

about 20% of the Internet routers in the marking process. Which i found very impressive.

The scheme allows the firewall system to configure itself based on the normal traffic of a Web server, so that the occurrence of an attack can be quickly and precisely detected.

The paper also talks about their extensive testing of the scheme by simulating DDoS attacks with up to several thousand attackers and the experimental results show that more than 90% of attack packets can be effectively filtered-out without much affecting the flow of legitimate packets to the victim Web-server.

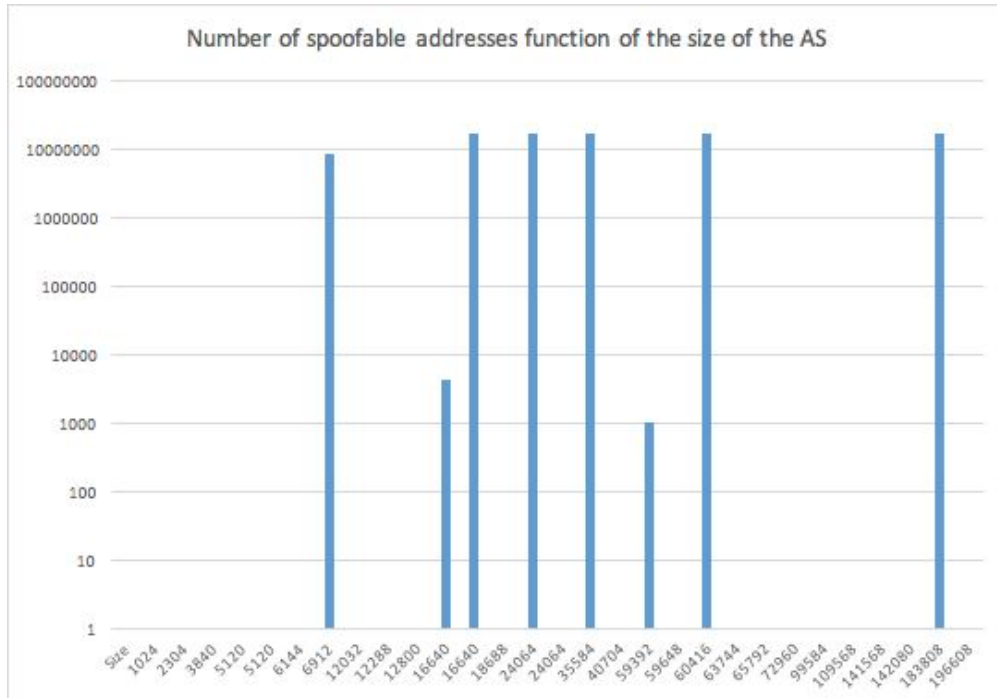
They call the scheme MDADF, which is composed of two parts: first one is marking process and other is filtering process. The number are quite impressive but at the end it's simulation based, we have to see how it performs in the real world.

Research Question, Objective and Hypothesis

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. The data source of this research is spoofer project from caida[6] refer to introduction of this report for more information on spoofer project.

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

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.



Figure[3] Number of spoofable addresses (function of the size of AS)

The hypotheses I propose considering the above metrics is that the higher the size of an AS goes the lower its chances of allowing spoofable packets becomes.

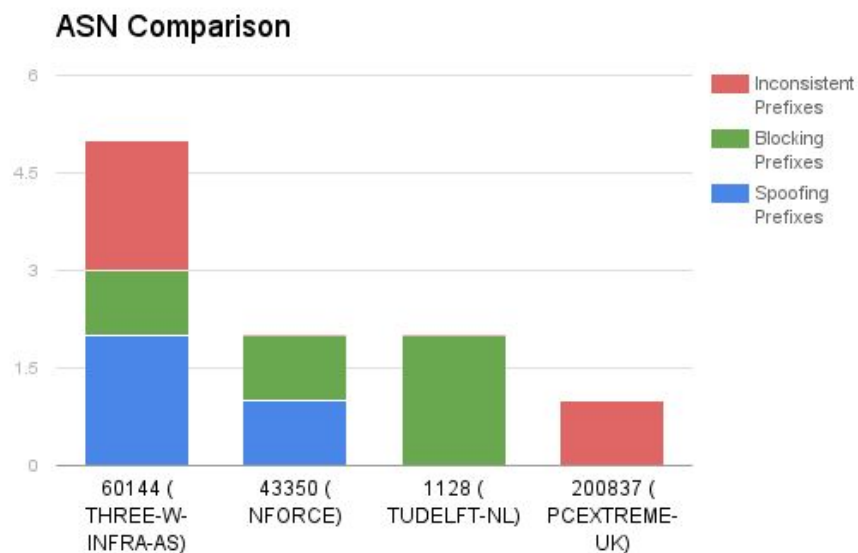
As from the literature review some of the papers suggests that the number of IP prefixes an AS owns will increase the number of tests he has to run to check the validity of the traffic source. I believe it's strongly related to the literature review. This hypotheses will materialize by larger ACLs on its edge routers. Therefore I conclude that it could infer, if an AS has a large number of prefixes, the implementation of SAV will cost the AS more than with just a few ones.

Methodology

As mentioned earlier in the report I'll be using statistical analysis methodologies on the data taken from Spoofer project from CAIDA in order to deduce the relationship between the hypotheses I proposed. The higher the size of an AS goes the lower its chances of allowing spoofable packets becomes. For the analysis of the influence of the position of an AS on its security performance, each AS degree will be sampled.

Orderly, I tried to Identify concrete countermeasures that the network operators could take to mitigate the security issue. Based on the available artifacts, it was found that ingress filtering was one the impactful choices. Moving further, I tried to analyze the distribution of costs and benefits that the decision makers had to take up, incase they tried to implement ingress filtering on their network nodes. Digging deeper, to analyze the incentives behind the decisions to implement the countermeasures.

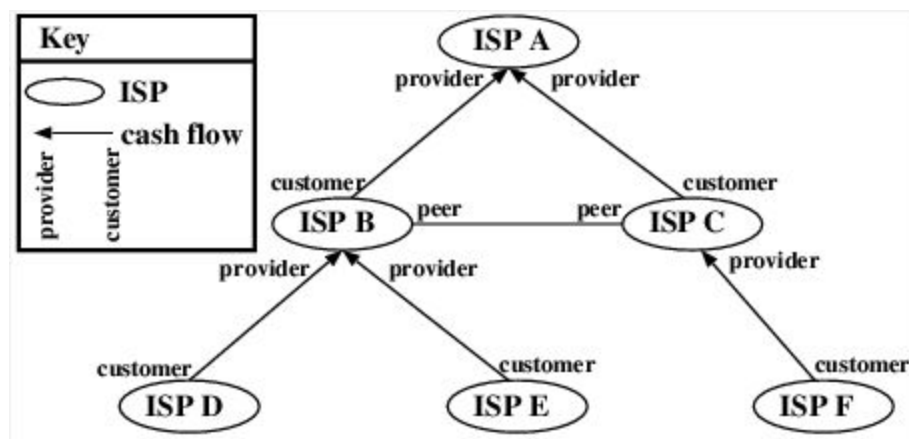
If we look at the metrics shows how any AS is vulnerable (open to be spoofed) compared to other ASes within their country and beyond. As well as how their architecture can allow attacker to use the IPs from neighbouring ASes or netblocks.



Figure[4] Comparison of 4 ASes in terms of prefixes

In this research, we will focus on the differences in behavior of ASes regarding IP Spoofing. We limited our scope to the data we have about ASes within the Netherlands. This leads us to a list of 29 networks, in which 7 let spoofed traffic flow to their neighbours.

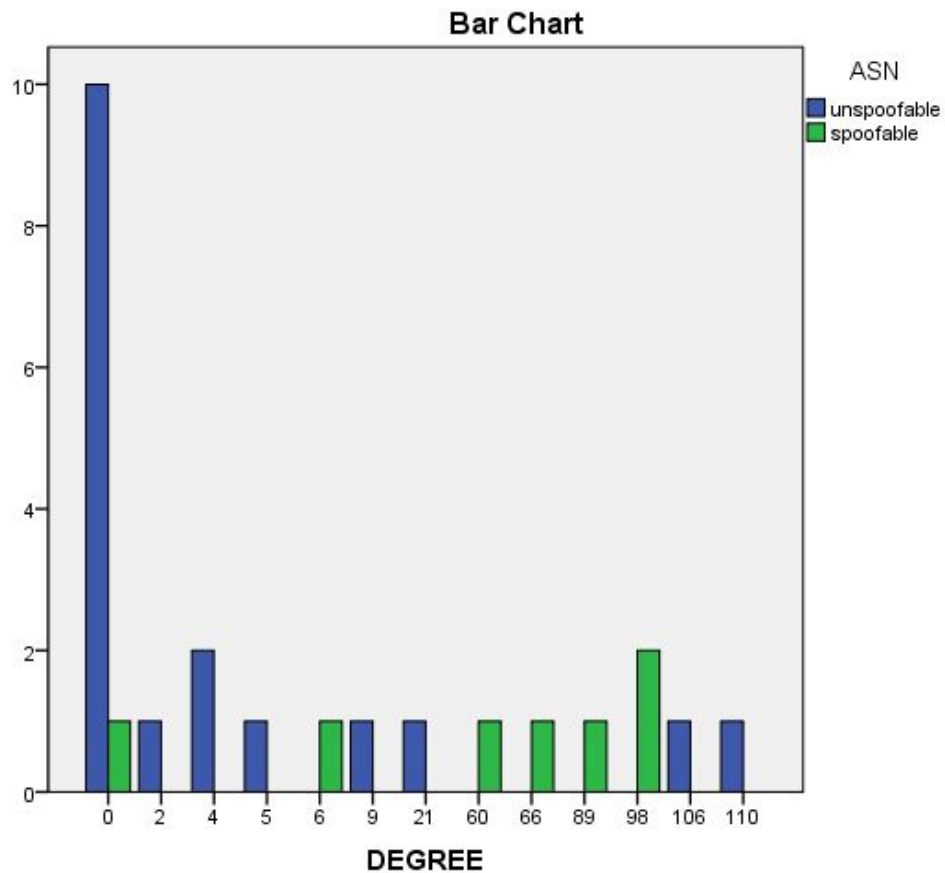
We considered all ASes from Netherlands for which we have data, and collected the degree of each one. The degree is related to the number of neighbours one AS has. Consequently, we can infer that the higher the degree is, the higher is the level of the AS in the Internet topology. As we can see on figure 4, ASes on the edge of the network usually have one or more provider(s), and often no peering relations. They have a low degree, most of the time 0. On the other hand, ASes in the core are connected with numerous others, often by means of peering agreements, and have a high degree.



Figure[5] Example of relationships between ASes

Thus, we can consider ASes which have the higher number of relations, or the higher degree, as the deeper in the global network.

A trend is remarkable 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.



Figure[6] number of spoofable and non spoofable ASes function of their degree

Then, we can infer about our hypothesis from the previous step. It seems that there is a correlation between the degree of an AS and its security performance. The higher in the topology, the less SAV is deployed. This could be explained by the fact that ASes in the core of the network do not usually provide direct access to end users, but rather transit to smaller ASes. By consequence, it is not their role to check the validity of the source of the traffic originating from one of their customers.

Results

Correlations			
		Prefixes	ASN
Prefixes	Pearson Correlation	1	-0.131
	Sig. (2-tailed)		0.604
	N	18	18
ASN	Pearson Correlation	-0.131	1
	Sig. (2-tailed)	0.604	
	N	18	29

The Pearson's for the correlation between the prefixes and ASN (spoofable or not spoofable) is -0.131. When Pearson's r is close to 0 means that there is a weak relationship between the two variables. And when the Pearson's r is negative means that as one variable increases in value, the second variable decreases in value. In our case there is a weak relationship between ASNs and the number of prefixes and also a negative correlation.

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	0.875	0.541
	Cramer's V	0.875	0.541
	Contingency Coefficient	0.659	0.541
N of Valid Cases		18	

Sig (2-Tailed) value is the value which tells us if there is a statistically significant correlation between our two variables. In our example, our Sig. (2-tailed) value is 0.604 and it is bigger than the value 0.05 (the acceptable probability of error). We can conclude that there is no statistically significant correlation between our two variables. That means, increases or decreases in one variable do not significantly relate to increases or decreases in the second variable.

Phi and Cramer's V are both tests of the strength of association. We can see that the strength of association between the variables is very strong (0.875), as it is closer to 1.

Correlations

		type	percentage
type	Pearson Correlation	1	-0.327
	Sig. (2-tailed)		0.186
	N	18	18
percentage	Pearson Correlation	-0.327	1
	Sig. (2-tailed)	0.186	
	N	18	18

The Pearson's r for the correlation between the type of the ASNs (content, enterprise and transit/access) and the percentage of spoofable and non-spoofable ASNs is -0.327. That means that there is a weak relationship between these two variables, as the value of the Pearson's r is closer to 0. Also, 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. the more enterprise ASNs we have, the percentage of non spoofable ASNs decreases. In our case there is a weak relationship between type of ASNs and the percentage of spoofable IPs, as well as a negative correlation.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	1.165	0.659
	Cramer's V	0.824	0.659
	Contingency Coefficient	0.759	0.659
N of Valid Cases		18	

In this case, the Sig. (2-tailed) value is 0.186 which is bigger than the value 0.05. We can conclude that there is no statistically significant correlation between our two variables. That means, increases or decreases in one variable do not significantly relate to increases or decreases in the second variable.

From Phi and Cramer's V tests we can see that the strength of association between the variables is very strong. The Cramer's V value is 0.824 and the Phi is 1.165.

Correlations			
		ASN	DEGREE
ASN	Pearson Correlation	1	0.529**
	Sig. (2-tailed)		0.003
	N	29	29
DEGREE	Pearson Correlation	0.529**	1
	Sig. (2-tailed)	0.003	
	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 positive which means that as the one variable increases in value, the second variable increases also in value, i.e. increasing the degree of ASNs, we also increase the spoofable IPs connecting to them.

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	0.908	0.021
	Cramer's V	0.908	0.021
	Contingency Coefficient	0.672	0.021
N of Valid Cases		29	

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.

From 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.

Limitations

The dataset was one of the essential element in this or any other research for that matter. So I believe the spoofer is yet a growing tool, it doesn't contain enough data to form any effective conclusion from the analyses. Sure it has enough data to give it some shape but its statistical significance is not at par.

Other than the data source and the quantity the data quality was also a limitation. A valuable metric for this analysis would have been one which contains more behavior of network operators (ASNs). For example, during our research concerning data elements was taken from another project from CAIDA AS Rank. which was referred as not as accurate. So it would have been better if AS sizes and their relation were also given from the spoofer or any other trust third party source.

Conclusions

From the analysis, this paper shows Ingress filtering as a valid countermeasure that can be implemented to all actors Network operators, the country, and victims to mitigate the security issue. The positive and negative incentive raised due to the implementation of Ingress filtering on each actor.

From the analysis in results, statistical analysis to explore the impact of these factors on the metric, we can verify the hypothesis and make a conclusion. Hypothesis Level of the AS in the Internet Topology that most of the ASes with a low degree are not allowing spoofing. There is just a correlation between degree and spoofability. Due to limited data available, the rest of factors didn't provide any promising relation.

References

1. <https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/>
2. <https://www.ddosattacks.net/sberbank-and-alfa-bank-suffer-from-botnet-based-ddos-attacks/>
3. <https://www.ddosattacks.net/5-major-russian-banks-repel-massive-ddos-attack-2/>
4. <http://thehackernews.com/2016/09/ddos-attack-iot.html>
5. <https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/>
6. <https://spoofer.caida.org/>
7. <http://as-rank.caida.org/>
8. <http://www.ijarcsms.com/docs/paper/volume2/issue4/V2I4-0056.pdf>
9. <https://www.sans.org/reading-room/whitepapers/threats/spoofed-ip-address-distributed-denial-service-attacks-defense-in-depth-469>
10. <https://arxiv.org/pdf/1208.3557.pdf>
11. https://www.researchgate.net/publication/46093769_Detecting_and_Preventing_IP-spoofed_Distributed_DoS_Attacks
12. <http://research.ijcaonline.org/volume40/number11/pxc3877332.pdf>