Assignment Block 4
GROUP 2

Akbar Aryanto*, Amit Gupta*, Jonathan Quigley * Manish Kumar* and Vasileios Merdis *
* *Economics of security Course 2016, University of Twente, Enschede, The Netherlands*

Introduction

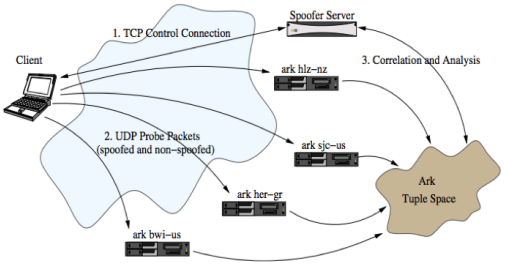

Figure 1. Spoofer test operation.

1) Clients receive test scenario from control server.
2) Scenarios involve sourcing a series of spoofed and non-spoofed UDP probe packets to ark nodes across the Internet.
3) Control server disambiguates and analyzes the results

1. Actors involved in the security issue

During our previous assignment, we have focused on identifying the problem owner, as well as, other actors that play a significant role in the security issue of IP address spoofing.

We identified the problem owner as the *Network Operators*, because they have the ability to implement some solutions, and specifically, Source Address Validation (SAV) to prevent IP spoofing. However, they are not the only impacted actors of this issue, which are more likely DDoS attacks using spoofing.

Another actor, that can be influenced by the security issue and was described in the last assignment, is *the country*. A countrys reputation can be easily affected by an attacker who is using IP spoofing, in that country, to carry out a denial of service (DoS) attack. On the one hand, countries can gain a lot of benefits from implementing SAV to mitigate the risk, but on the other hand, the cost of such an implementation can be harmful for them.

Finally, the last actor that can be influenced by the security issue is *the victim*. And a victim can be considered both the the target IP and also the IP that the attacker uses in order to hide his own. The victims can also proceed to some solutions in order to mitigate or transfer the risk. But, first, they have to estimate the benefits and the costs of the potential solutions.

1.1. One concrete countermeasure that could take to mitigate the security issue

Having so many diverse actors involved in a security issue always makes it difficult to find a common concrete countermeasure that all of them can take. Not to mention in SAV the one who bears the cost doesnt fully reap the benefits.

However, considering a counter measure where all the actors can at least benefit the mitigation of the security issue opens the window for many risk strategies that can be deployed mainly at Network Providers end.

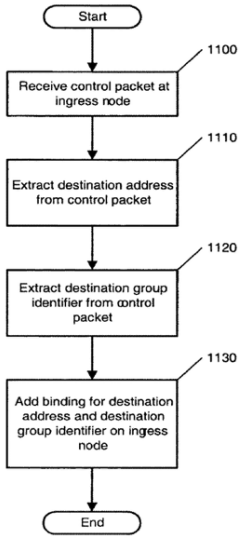

Figure 2. Ingress Filtering process.

And the one we will focus during this assignment is **Ingress Filtering** which can solve the root cause and give solution as well to other actors. Now it can be debated that ingress filtering is a very old technique to do source address validation. But its still wildly deployed.

New techniques like Unicast Reverse Path Forwarding, or uRPF which are prefered to use today or also the automation of Ingress Filtering implementation. Which are further explained below.

The Network Providers (our problem owners) will need to implement ingress filtering rules, which check the source IP field of the IP packets it receives. If the source IP address is not within a range of legitimately advertised prefixes, a router will drop the packet.

There are at least five ways to implement ingress filtering technique in network operator :

1) **Ingress Access List**
   An Ingress Access List will filter and checks the source address of every message received on a network interface against a list of acceptable prefixes, then dropping any packet that does not match the filter.
2) **Strict Reverse Path Forwarding**
   It is conceptually identical to using access lists for ingress filtering, with the exception that the access list is dynamic
3) **Feasible Path Reverse Path Forwarding**
   Feasible Path Reverse Path Forwarding (Feasible RPF) is an extension of Strict RPF. The source address is still looked up in the RPF-specific table but instead of just inserting one best route there, the alternative paths (if any) have been added as well, and are valid for consideration.
4) **Loose Reverse Path Forwarding**
   Loose Reverse Path Forwarding (Loose RPF) is algorithmically similar to strict RPF, but differs in that it checks only for the existence of a route (even a default route, if applicable), not where the route points to. Practically, this could be considered as a "route presence check"(loose RPF is a misnomer in a sense because there is no "reverse path"check in the first place).
5) **Loose Reverse Path Forwarding ignoring default routes**
   The fifth implementation technique may be characterized as Loose RPF ignoring default routes, i.e., an "explicit route presence check". In this approach, the router looks up the source address in the route table, and preserves the packet if a route is found. However, in the lookup, default routes are excluded. Therefore, the technique is mostly usable in scenarios where default routes are used only to catch traffic with bogus source addresses, with an extensive (or even full) list of explicit routes to cover legitimate traffic.

By implemented ingress filtering it will not only mitigate the security issue and provide benefits to the problem owner (network provider) but as well as all the rest of the actors mentioned above.

Countries have better reputation and less malicious network. The victims all around the world have few less computers to worry about. It will reduce DDoS attack which use forged IP addresses to propagated from an Internet Service Provider (ISP).

And ASNs or the network providers on other hand have big raise in quality of service by having all the bandwidth and less malicious network for their customers. There are many more factors but some of the cost distribution and benefits are explained in detail, down below.

1.2. The distribution of costs and benefits among the different actors that the deployment of the countermeasure would entail.

An important factor determining the uptake and deployment of ingress filtering (BCP 38) methods is how the costs (capex and opex) are addressed. Network Providers operate in a highly competitive and tough market with relatively small margins.

They invest their money in services such as VPN and content hosting, as these are services people expect to get charged for, rather than for inter-domain routing security or the source address validation, for which no direct charges are made.

Investments in security are lagging behind as many NP are not able to justify business investments, as the costs of successful attacks are currently not measured. Should these costs be made clear, investments would be more easily justified.

Nonetheless, form the actors we are focusing in this assignment the solution can only be deployed at Network Providers end. So all the direct cost is beared by them. They have some incentives but not as much as to victims.

Mainly for better understanding, we have divided the cost into three categories (parts).

- **Capital expenditure** or capital expense (CapEx) only if the equipment NP already use doesn't support **RPF**. These are the one time cost.
- **Operating Expense** or operating expenditure (OpEx) which are the recurring cost. Some of these can be. deployments, installation costs trainings, manpower, energy consumption, support and maintenance etc.
- **Opportunity Cost** These are the losses from those customers who don't like or want filtering or the solution implemented for that matter and move on to another NP who doesnt filter.

Other than just costing money the practice have multiple of benefits to all the actors including victims and network providers among others.

1) **The Victim**
   - No Solution Deployment Cost. (Ingress Filtering)
   - No extra firewall cost to prevent or stop a DDoS attack.
   - No disaster recovery plans.
   - No man power to make the plans

- No down time.
- Financial impact of being offline for a period of time
- No Brands value loss
- No extra bandwidth cost
- No DDoS prevention or safety services
- No frauds or data breaches
- More Threat Free network
- Good Reputation

2) **The NetWork Provider**

- Bandwidth Cost
- Reputation
- Better Customer Protection (IP theft. Or IP Logins. Man-in-the-Middle)

3) **The Country**

- Competitive image in tech market.
- If marketed properly, it can attract lots of Tech Companies.
- Specifically the companies who need their Data Centers.
- Hosting providers and others directly related to networks.
- Which can raise the economy and job ratio.

So to sum to up, We found that the major cost is with Network Providers end if we go for Ingress filtering. But to solve this at the consumer CPE level would remove 90-95 percent of the problem at zero hardware cost, a very small software cost, and a very small support cost and probably make us stop talking about this issue all together.

Companies like Apple, Google, Cisco, linksys and tenda who make the routers will have to bear that small cost. And in return they can reap many benefits. And market the feature to sell their products as **"not letting hackers use your devices."**

1.3. The actors which have an incentive to take the countermeasure

Each actor has their own motivation to find the best countermeasures. Ingress filtering is the countermeasure that will be a concrete countermeasure which applies to all actors. With this countermeasure, its will be fitted and bring the benefit to the actors.

The network operator, one of the actor, is the most important node to implement this solution. Because network operator as a root cause of this case, when DDoS attack can be reduce from this side, will bring positive result to other actors. Even though there are no direct benefits to Internet Service Provider when implemented ingress filtering, but there are some incentives and benefits to network operators.

Network Provider

1) **[Positive] Better Customer Protection (IP theft, IP Logins, MITM)**
Implementing ingress traffic filtering of Internet connected networks will reduce the effectiveness of source address spoofing denial of service attacks. Internet Providers and network operator which implement ingress filtering, will lessen the opportunity for an attacker to use forged source addresses as an attack methodology. Number and frequency of attacks in the Internet as a whole will be reduced, customer will gain the benefit of it countermeasure.

2) **[Positive] Reputation**
The reputation of network operator will increase because they implement the countermeasure.

3) **[Positive] Customer Satisfaction**
Each client has different purposes while using the service from the service provider. they will feel safe running their business using it because the good neighborhood of the internet they used.

4) **[Negative] Side Businesses**
There are many organizations, Specifically the ones we are studying in our report. All the organizations which owns the ASes that allow sending of spoofable packets outside also happen to provide services like DDoS prevention.
So by implementing the countermeasure they might lose that business. Though its only possible in an ideal situation of full internet getting SAV. But even one AS implementing the countermeasure will also decrease the chance and resources behind the attacks. No attacks = No DDoS preventions.

5) **[Negative] Opportunity Cost**
By implementing the countermeasure, the AS can lose those customers who don‘t want filtering, or the solution implemented which prevents sending spoofed packets outside. and eventually can move on to another NP who doesn‘t filter.

6) **[Negative] Cost vs Benefits**
Though it‘s true that NP does get the benefits of implementation of SAV, but comparing it with the cost those benefits might seem to be losses, specially the recurring cost that they have to bear.

Country

1) **[Positive] Reputation**
The reputation of Country will increase as well, the number of attackers coming from Netherlands to other countries will decrease. This will make a good benefit to Country as one of a big actor.

1.4. The role of externalities around this security issue

Apart from the direct impacts of the DDoS security issue on the target, the effects are seen on multiple other external parties. In fact, the relationship is both ways, the externalities driving DDoS and effect of security threat on the externalities.

For example, applying SAV through in-house firewall servers can be costly to the network providers because of which they tend to avoid installation of ingress filters (BCP38) on their servers. Also because sometimes having multiple filters on the servers tends to unpredictable performance challenges, the network owners avoid SAV. This leads to IPs in the subnet being spoofed causing DDoS.

Another externality is the existence of open DNS proxies that will respond to requests from anywhere on the Internet. Many organizations run DNS proxies for use by their own people. A well-managed DNS proxy is supposed to check that requests are coming from within the same organization; but many proxies fail to check this – they're "open"and will respond to requests from anywhere.(on Security, n.d.)

Looking deeper into it, the investments to defend against targeted attacks such as hacking and distributed denial of service (DDoS) attacks cause negative externalities, whereas protections against untargeted attacks such as viruses, worms, Trojan horses and spyware generate positive externalities.(Shim, 2010)

Theories also say that, compared to the case of independent security risks, in the presence of positive externalities firms purchase less or equal insurance coverage while in the presence of negative externalities firms purchase equal insurance coverage. It is concluded that the adoption of cyber insurance can at least partially solve the overinvestment problem whereas the underinvestment problem becomes more severe.(Shim, 2010)

We believe that the externalities can be fixed by regulations around the driving forces and personal. It is better to fix this issue without government intervention. Although the reputation of a country is on stake, governments have to intervene when they are really threatened.

2. Type of actor whose security performance is visible in the metrics

Considering our previous assignments, findings and data analyses, there are two major actors whose security performance is visible in the metrics we have selected.

1) ASes (The network Providers)
2) Countries

Mainly 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.

In this assignment, we will focus on the differences in behavior of ASes regarding IP Spoofing.

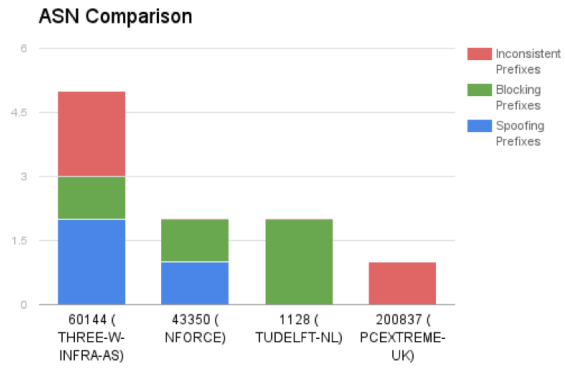

Figure 3. Comparison of 4 ASes in terms of prefixes.

2.1. Different factors causing the variance in the metric

The metric that will be used is the resistance of an AS against forged routable IPv4 addresses, as it is the most representative parameter of the security issue. 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.

To explain these differences in security performances, we analysed several factors.

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 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. We can then make these two hypothesis:

H0: The security performance is correlated to the level of the AS in the topology

H1: The security performance is independent of the level of the AS in the topology

Number of prefixes owned by the AS

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. This will materialize by larger ACLs on its edge routers. Therefore, we could infer that if an AS has a large number of prefixes, the implementation of SAV will cost him more than with just a few ones.

On the other hand, if a network owns numerous prefixes, it should mean its size is important, and its financial resources as well. Then, the cost of implementing a protection

against spoofing should not be a strong barrier. Here are two hypothesis:

H0: The security performance is correlated to the number of prefixes of the AS

H1: The security performance is independent of the number of prefixes of the AS

Type of network

ASes can be associated with different types depending on their function. For instance, a transit AS has the purpose to provide to smaller neighbours connectivity to the rest of the network. Conversely, an enterprise or educational AS is more likely a leaf of the topology, hosting end users. This difference in purpose could reflect on security performance, as we could expect networks from ISP to be more secure, because they should be aware of the issue of spoofing. Unfortunately, we were unable to find a reliable source of data for this factor. There is a project from CAIDA(CAIDA, n.d.) which classifies ASes in three categories (Access/transit, Content, Enterprise), but it is not accurate enough to exploit its results.

2.2. Collect data for one or several of these factors

Level of the AS in the Internet Topology

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 an 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.

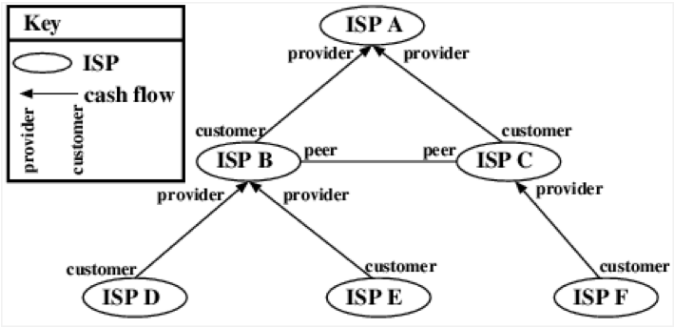

Figure 4. Example of relationships between ASes.

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

On figure 5, we can observe the degree of all ASes we have data on, 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.

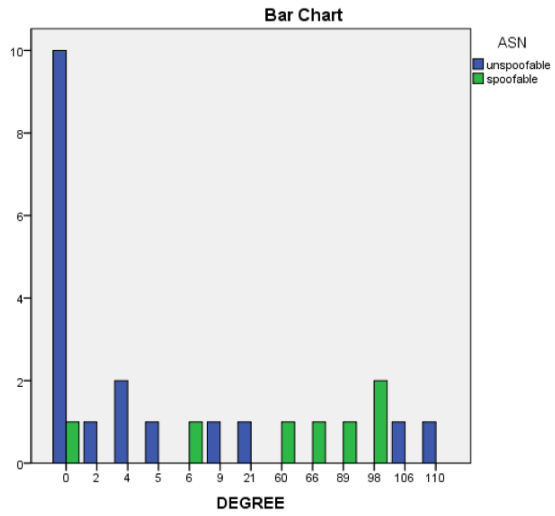

Figure 5. number of spoofable and unspoofable ASes function of their degree.

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.

Number of prefixes owned by the AS

Thanks to the data provided by CAIDA again, we collected the number of prefixes each AS from our list owns. On figure 6, we can observe the spoofability of ASes function of their number of prefixes.

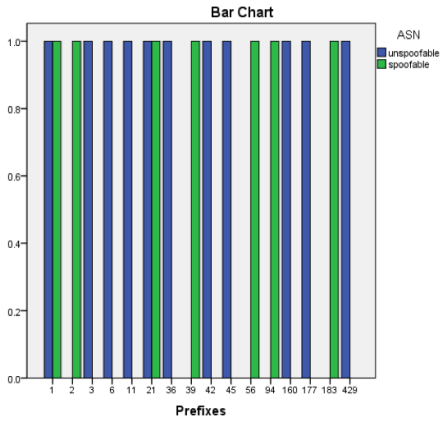

Figure 6. Spoofability of ASes function of their number of prefixes.

Clearly, no particular pattern can be defined from this graph, as spoofable ASes are divided all over the range of values. We could have expected that larger networks would have been less secure due to the difficulty of managing such amount of traffic, but it seems that with a bigger size come more resources to handle security.

2.3. Statistical analysis to explore the impact of these factors on the metric.

For this section, we have to perform a statistical analysis so several factors that can explain the variance are assessed, i.e. the percentage of spoofable and non spoofable ASNs, the type of these ASNs, the prefixes and the degree. However, the sample is too small (18 and 29) and no conclusions can be drawn from the tests.

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

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	

Figure 7.

The Pearson‘s r for the correlation between the prefixes and ASN (spoofable or not spoofable) is -0.131. When Pearsons 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.

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

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	

Figure 8.

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 Pearsons 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.

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 Cramers V value is 0.824 and the Phi is 1.165.

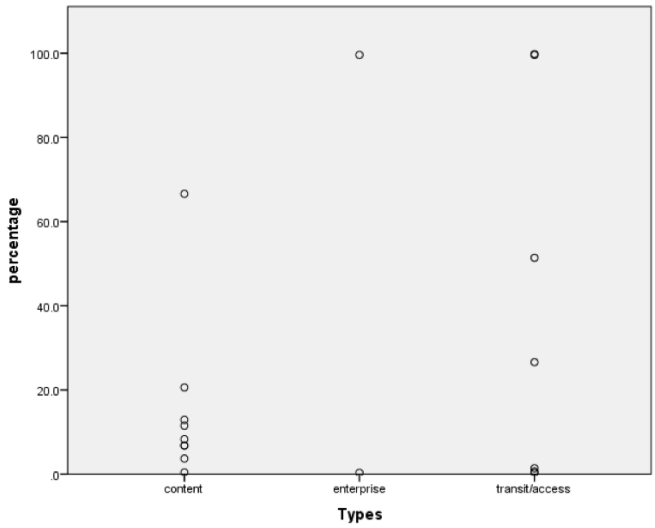

Figure 9.

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).

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	

Figure 10.

The Pearson‘s r for the correlation between the ASNs (spoofable and unspoofable) 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.

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.

3. Conclusion

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 part 2.3 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 that we have, the rest of factors we did not find any relation.

References

CAIDA. (n.d.). *As classification.* Retrieved from `http://www.caida.org/data/as-classification/`

on Security, S. (n.d.). *Security externalities and ddos attacks.* Retrieved from `https://www.schneier.com/blog/archives/2013/04/security_extern.html`

Shim, W. (2010). Interdependent risk and cyber security: An analysis of security investment and cyber insurance. (1), 149.