Economics of security

Assignment block 4 – Group 2

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

Draft Paper

Date: Oct 24, 2016

Introduction

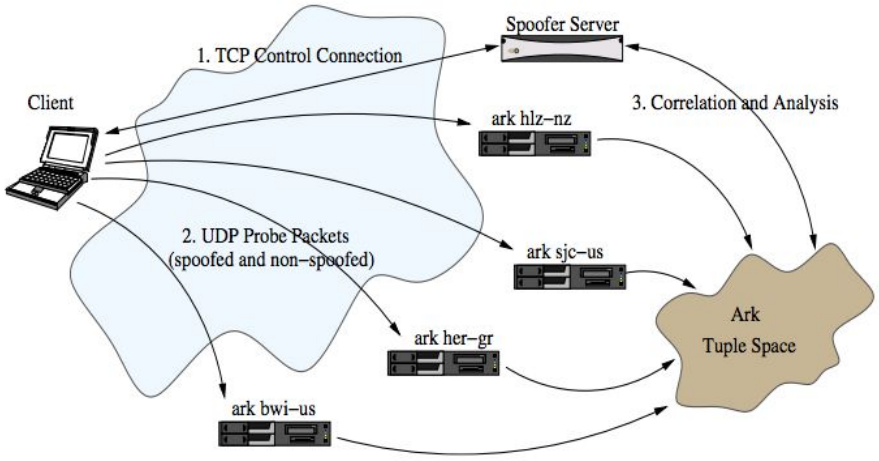


Figure: Spoofer test operation: 1) Clients receive test scenario from control server. 2) Scenarios involve sourcing a series of spoofed and non-spoofed UDP probe packets to ark nodes across the Internet. 3) Control server disambiguates and analyzes the results

1. **Select 3 actors (including the problem owner) involved in the security issue (you can draw on the previous assignment)**

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.

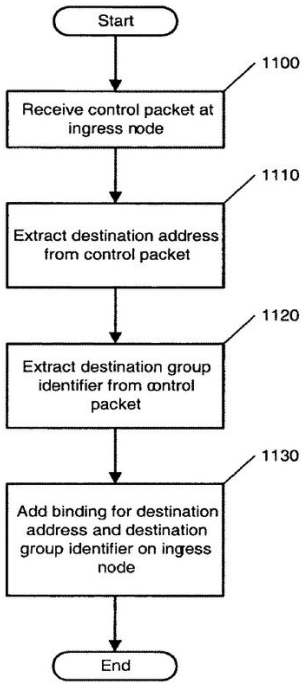
Another actor, that can be influenced by the security issue and was described in the last assignment, is *the country*. A country's reputation can be easily affected by an attacker who is using IP spoofing, in that country, to carry out a denial of service (DoS) attack. On the one hand, countries can 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. Identify one concrete countermeasure that they 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 doesn't 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.



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 it's 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. Analyze 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 doesn't filter.

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

- **The Victim**
    - Monetary Benefits
        - 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 reputation loss
        - No extra bandwidth cost.
        - No DDoS prevention or safety services

        - No frauds or data breaches
    - Other Benefits
        - More Threat Free network

- **The NetWork Provider**
    - Monetary Benefits
        - Bandwidth Cost
    - Other Benefits
        - Reputation
        - Better Customer Protection (IP theft. Or IP Logins. Man-in-the-Middle)

- **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% 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. Analyze whether the actors 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

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

  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.

- Reputation

  The reputation of network operator will increase because they implement the countermeasure.

- 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.

Country

- Reputation

  The reputation of Country will increase as well, the number of attackers came from Netherlands to other countries will decrease. This will make a good benefit to Country as one of a big actor.

1.4. Briefly reflect on 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. [1]

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[2]

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.[3]

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.

[1] https://www.schneier.com/blog/archives/2013/04/security_extern.html

[2] Interdependent Risk and Cyber Security: An Analysis of Security Investment and Cyber Insurance, Shim, Woohyun, 2010 Michigan State University, http://eric.ed.gov/?id=ED523218

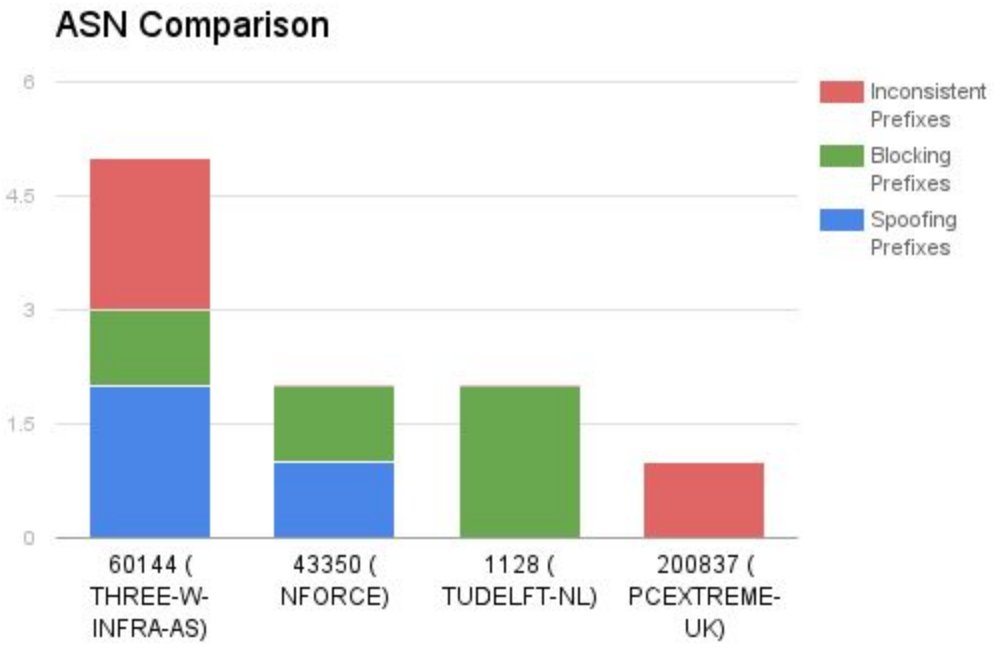
[3] Interdependent Risk and Cyber Security: An Analysis of Security Investment and Cyber Insurance, Shim, Woohyun, 2010 Michigan State University, http://eric.ed.gov/?id=ED523218

2. Identify the type of actor whose security performance is visible in the metric(s) you selected (e.g. ISPs, software vendors, countries). Note that this is not necessarily the problem owner, rather is the unit of analysis in your metric.

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. ASN (The network Providers)
2. Countries

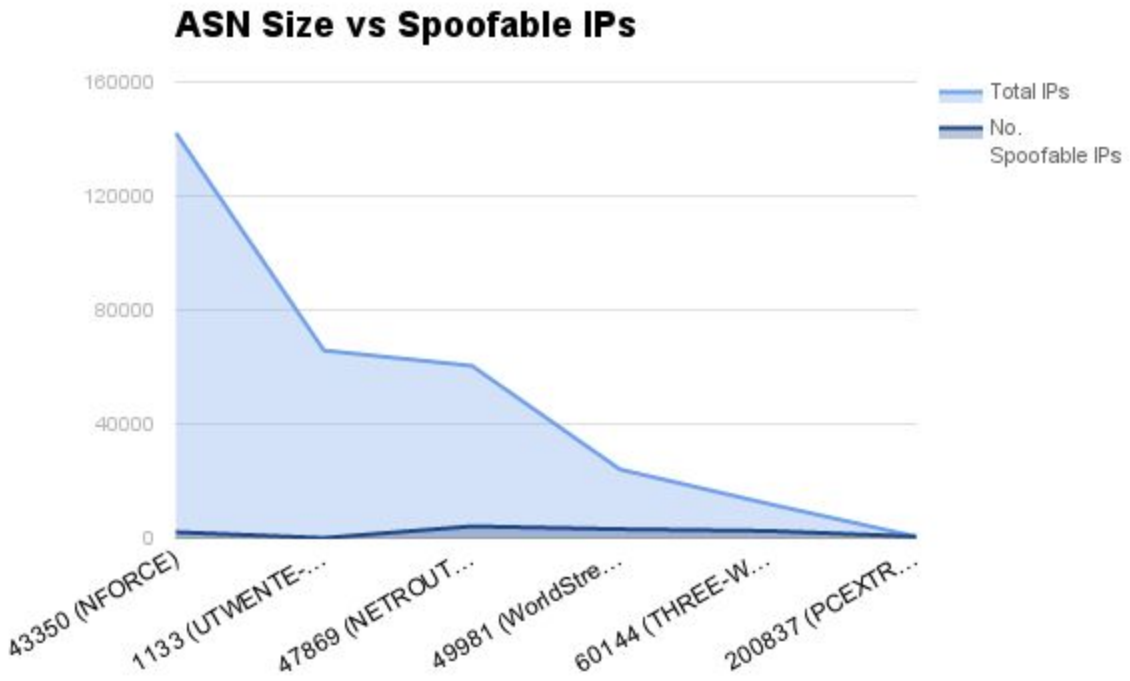
Mainly the metrics shows how any ASN is vulnerable (open to be spoofed) compared to other ASNs within their country and beyond. As well as how their architecture can allow attacker to use the IPs from neighbouring AS or netblocks.



As far as country is concerned we could see how one country is doing compared to another, considering the number of tests have been run along with the total number of AS in that country.

Mainly for a country the security performance and differences can translate into better reputation and opportunities for many tech companies getting attracted for investment.

Apart from these two actors the variance we are focusing in this assignment from our previous matrices is quite simple we found that mainly the bigger an AS gets in size the smaller the percentage of spoofable IPs they have. It's reflected into the following graph as well.



There can be many reason behind this, some of them are discussed below but provided the fact that this trend can only be scene from the data available. If we could some how get the full picture of a country the end picture can be very different.

2.1. Identify different factors explaining (causing) the variance in the metric

Premise:
Based on the analysis of the data from the Spoofer, it was clear that the there is a trend in the variance on the basis of metric. It appears that the network providers with relatively more number of consumer IPs tend to have lesser number of spoofable end points.
,i.e., within limits, for a network provider (NP) we can define,

Size of the network provider, S, could be defined by the number of IPs in its subdomain.
Number of IPs in the network = N
Number of Spoofable IPs in the network = SP
Number of Non-spoofable IPs in the network = NSP
Number of IPs whose information is unknown = UP,
Then, N = SP + NSP + UP.
And,

$$N \propto 1/SP$$

1. The larger the network provider is, the more revenue it generates by providing services to the customers
2. It is understood that a NP insists to give uninterrupted, good QoS of network service to its customers
3. **Investments:** If the network provider has high revenues, it is capable enough to invest in security risk management teams, tools and techniques, e.g, have dedicated security analysts and blue teams

a. **Firewalls:** The smaller NP on the other hand does not have enough funds to buy expensive network filters and firewalls. Because it needs to sustain the small segment of customers that it has and survive its venture at the same time, probably QoS is marked second on the importance list. E.g. stronger firewalls, in order to preserve its QoS for the clients

4. **Code of conduct:** It is highly likely that a bigger network provider company would insist in having more stringent ethical code of conduct, so it does invest in strategies that might not have direct impacts in the monetary profits for the company but are ethically good.
5. **Foreseen threat:** NPs with relatively more number of served IPs is more likely to be compromised over DDoS, than the smaller NPs with only limited size, S.

2.2. Collect data for one or several of these factors

All businesses must now expect DDoS attacks, rather than consider them remote possibilities, and prepare accordingly. One recent study found that in just one year, a whopping **38%** of companies providing online services (such as e-commerce, online media and others) had been on the receiving end of an attack.[4]

It has been a constant effort from the network service providers to make sure that the traffic they handle are pure and the precious bandwidth is handled with care. As mentioned in 2.1, the small players and the big NPs have a statistically visible variation in the way they take care of the security configurations on their servers. Studies reveal that the NPs have been investing in some of the security initiatives to secure their servers from uncontrolled DDoS. Overall there are three kinds of solutions against DDoS that are adopted in today's market[5]:

a. **Cloud scrubbing Technologies:** Some of the NPs in Netherlands, for example NFORCE (mentioned in point 2) invests in cloud scrubbing technologies. [6] When the customer's web applications tend to receive high volumes of traffic, it is likely that a part of it could be malicious. The potential malicious traffic is transferred to the company's cloud traffic scrubbing centers. As traffic enters a scrubbing center, it is triaged based on a various traffic characteristics and possible attack methodologies. Traffic continues to be checked as it traverses the scrubbing center to confirm the malicious traffic has been fully removed. Clean traffic is then returned through your website with little to no impact to the end user.

b. **CDN:** A content delivery network (CDN) is a system of distributed servers (network) that deliver webpages and other Web content to a user based on the geographic locations of the user, the origin of the webpage and a content delivery server.This service is effective in speeding the delivery of content of websites with high traffic and websites that have global reach. The closer the CDN server is to the user geographically, the faster the content will be delivered to the user. CDNs also provide protection from large surges in traffic.[7]

c. **Customer on Premises Equipment (Appliances):** This kind of investments is often one of the expensive deals and are taken up by the network providers who are more than small in scale. With increased number of served IPs, the responsibility to manage the security of the network is also high, so it's important for the NPs to invest in the inhouse solutions like CISCO Guard XT Suit[8].

---

[4] https://devcentral.f5.com/articles/scrubbing-away-ddos-attacks
[5] https://devcentral.f5.com/d/firewall-201-ddos-protection-with-f5-223
[6] https://www.nforce.com/ddosprotection
[7] http://www.webopedia.com/TERM/C/CDN.html
[8] http://www.networkworld.com/article/2333552/lan-wan/cisco-details-strategy-for-catalyst-firewall-services-module-and-anti-ddos-gear.html

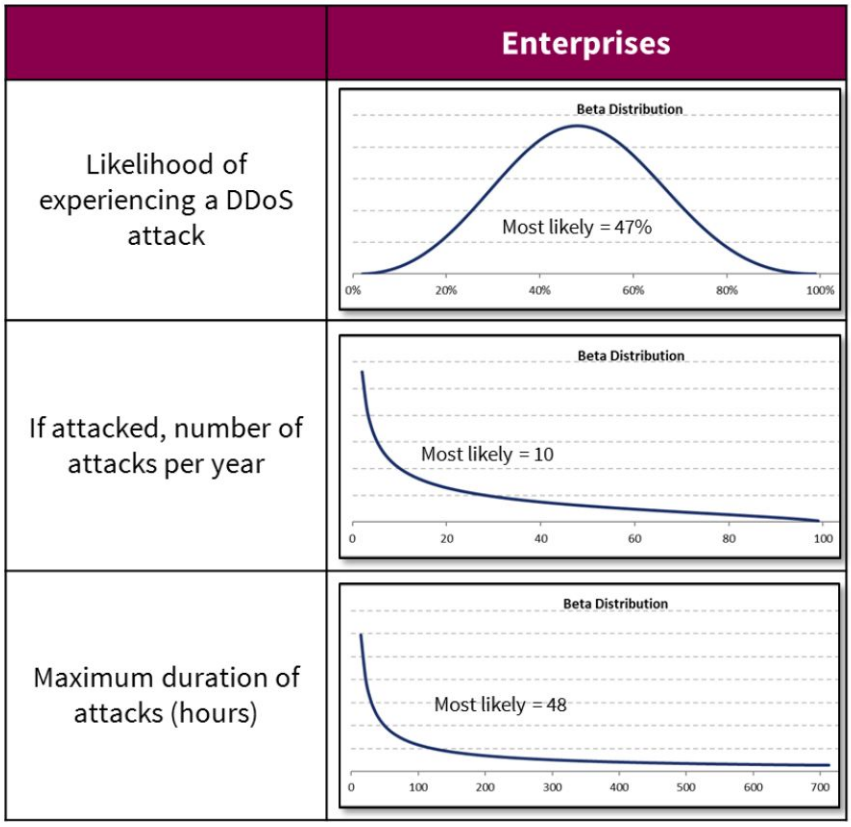


Fig: Empirical Data Shows the Likelihood, Frequency, and Duration of DDoS Attacks Against Traditional Enterprises [9]

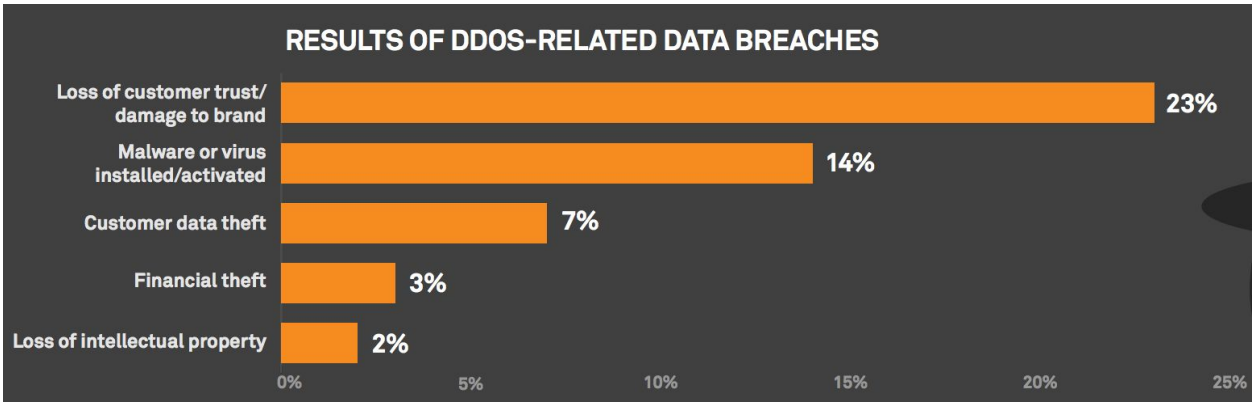


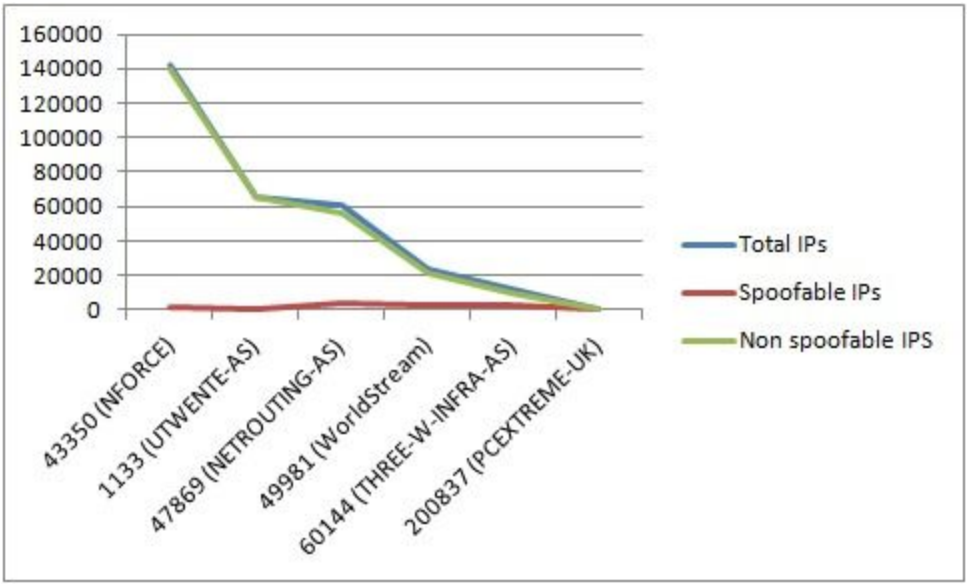
Fig: A glimpse on the losses that organizations have to face because of DDoS attacks[10]

[9] https://www.arbornetworks.com/images/documents/aberdeen-quantify-ddos-risk.pdf

[10] https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2015-us-ddos-report.pdf

2.3. Perform a statistical analysis to explore the impact of these factors on the metric.

ASNs	Total IPs	Spoofable Ips (%)	Non spoofable IPS (%)
43350 (NFORCE)	142080	1.4	98.6
1133 (UTWENTE-AS)	65792	0	100
47869 (NETROUTING-AS)	60416	6.8	93.2
49981 (WorldStream)	24064	12.9	87.1
60144 (THREE-W-INFRA-AS)	12032	20.6	79.4
200837 (PCEXTREME-UK)	512	99.6	0.4



This graph shows the ASNs with the total IPs that they have, both spoofable and non spoofable. As ws can see the bigger a ASN is, the less spoofable IPs it contains. For example, NFORCE is the bigger with the less spoofable IPs and the PCEXTREME-UK is the smaller ASN and almost all of its IPs are spoofable.

ASNs				
	49981 (WorldStream)	*60144 (THREE-W-INFRA-AS)*	*200837 (PCEXTREME-UK)*	**TOTAL**
spoofable IPs (%)	12.9	20.6	99.6	133.1
non spoofable IPs (%)	87.1	79.4	0.4	166.9
TOTAL	100	100	100	300

H_0 = ASNs and IPs (size) are independent
H_1 = ASNs and IPs (size) are not independent

E_{11} = 300*(133.1/300)*(100/300) = 300*0.4*0.3 = 36
E_{12} = 300*(133.1/300)*(100/300) = 300*0.4*0.3 = 36
E_{13} = (133.1*100/300) = 44.4
E_{21} = (166.9*100/300) = 55.6
E_{22} = (166.9*100/300) = 55.6
E_{23} = (166.9*100/300) = 55.6

$$\chi^2 = \sum_{i=1}^{2}\sum_{j=1}^{3}\frac{(Oij-Eij)^2}{Eij} = \frac{(12.9-36)^2}{36} + \frac{(20.6-36)^2}{36} + \frac{(99.6-44.4)^2}{44.4} + \frac{(87.1-55.6)^2}{55.6} + \frac{(79.4-55.6)^2}{55.6} + \frac{(0.4-55.6)^2}{55.6}$$

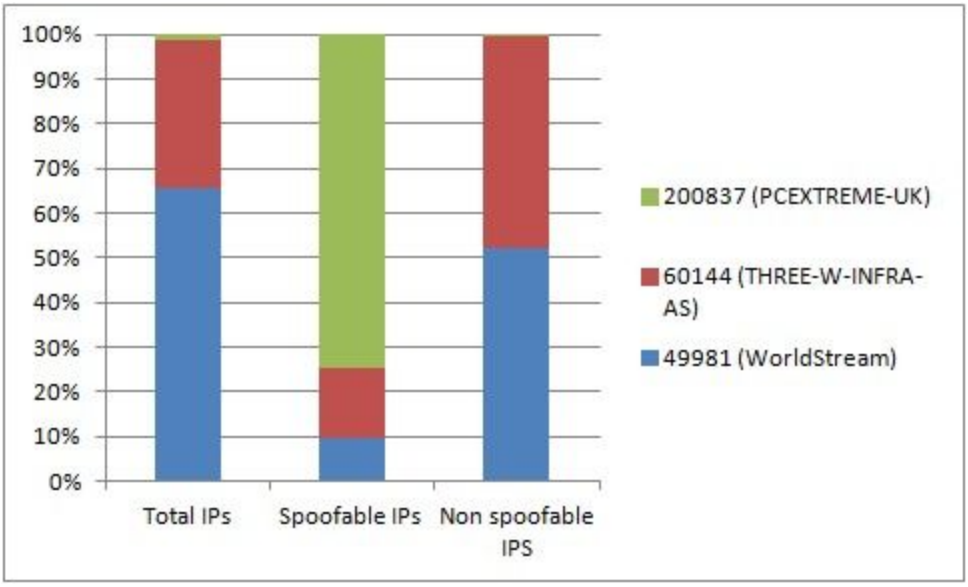
χ^2 = 14.8+6.6+68.6+17.9+10.2+54.8
χ^2 = 172.9

df = (3-1)*(2-1) = 2

$\chi^2_{2,\ 0.05}$ = 5.991 < χ^2 = 172.9
So we reject the H_0 and we accept the H_1 that ASNs and IPs are dependent.

$$V = \sqrt{\frac{172.9/300}{min\{1,2\}}} = \sqrt{0.6} \approx 0.77$$

Cramer's V varies between 0 and 1. Close to 1 it shows a strong association between the variables.



This graph indicates the three ASNs that we analyzed above to prove the relation between and ASNs and the size of IPs. The analysis was done by Pearson chi-square test and the strong association was done by Cramer's V. After all, we can say for sure that the bigger the ASN is, the less spoofable it is.