# Economics of security
# Assignment block 3 – Group 2

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

Draft

# Problem Owner

In the previous assignment, we looked for metrics which could describe the security issue of IP spoofing, and provide the networks operators some insights to remediate to it.

The metrics we produced were based on the tests of the Spoofer project, which allows any and end-user to test his operator's network. Our metrics measured the percentage of positive and negative tests for all Autonomous Systems of Netherlands, and then by AS. Here, we suggest to use a metric based on the percentage of spoofable addresses in an AS compared to its size.

In this assignment, we will focus on the actors impacted by this security issue, and especially on the problem owner. We identified the problem owner as the network operators, because they have the ability to implement Source Address Validation (SAV) solutions to prevent IP spoofing. However, they are not the main impacted actors of the issue, which are more likely victims of DDoS attacks using spoofing.

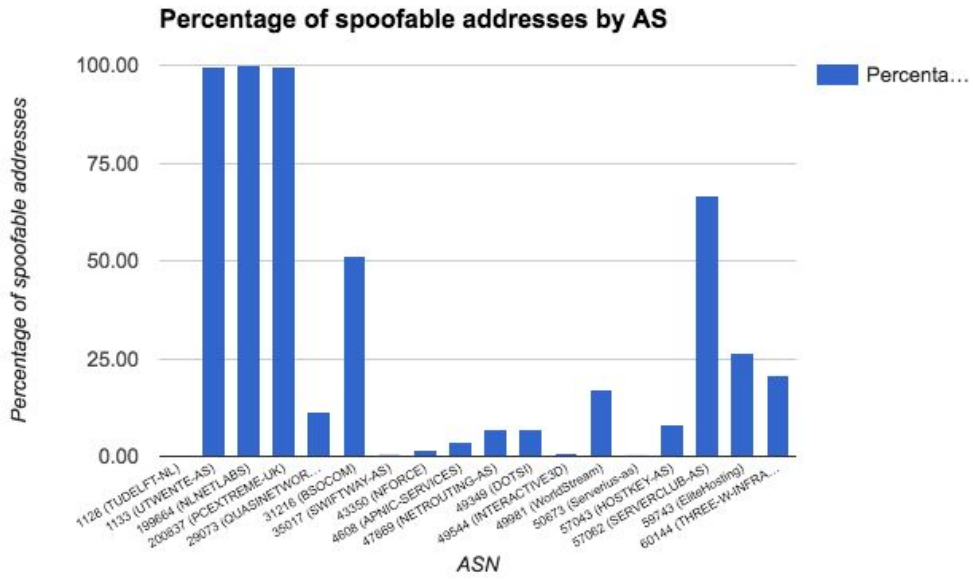
# Differences in security performances

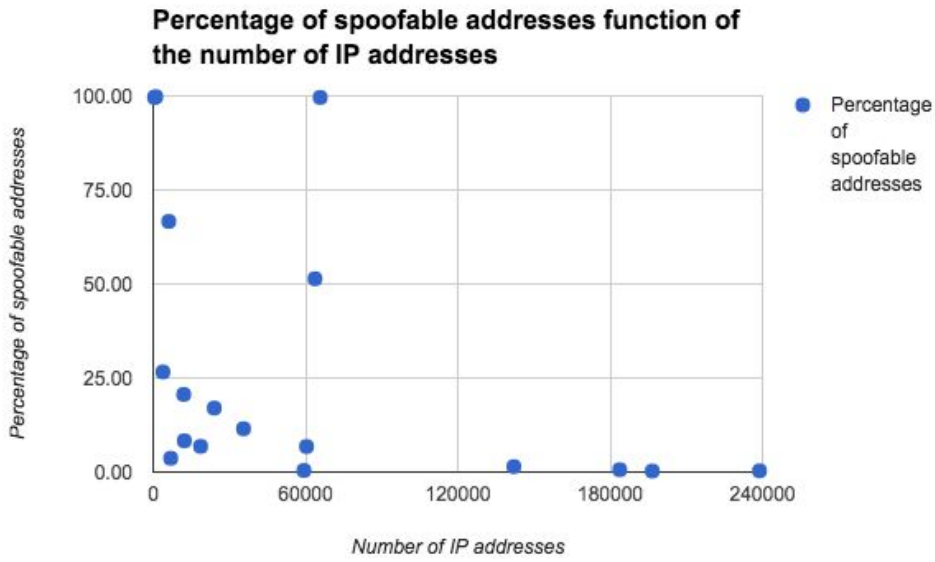
An interesting metric would be the evolution over the years of the number of AS which allowed spoofing and those who implemented SAV.

Unfortunately, we only have data from the past few months, which is not sufficient to draw a trend in security performances. Nonetheless, we produced a metric which is the percentage of spoofable IP addresses within an AS, function of its size (in terms of number of IP addresses).

Because the information is not directly present in the dataset, we had to manually collect it, and therefore we only focused on AS from the Netherlands. This means the data is maybe not fully representative of the situation in other countries.

Here are two graphs, projecting the percentage of spoofable addresses, first by AS, and then function of the size of the AS.




The first assumption we could make from this metric is that larger ASes are more likely to implement Source Address Validation, as they have more resources than smaller ones.
However, we would have to confirm this trend with larger data to make some reliable observations. For networks operators, this metric could tell them how they behave compared to their pairs, and produce some kind of shame effect if they do not conform to the others' standarts.

# Possible risk strategies

According to the general model, there are four options for the possible strategies: avoid, accept, reduce and transfer. As we mentioned before, Network Providers are the main problem owners. Thus, the possible strategies that they can follow in order to prevent IP address spoofing and by extension DDoS attacks, minimized in two categories. They cannot avoid or accept this security issue.

Conversely, they are responsible for reducing and transferring the problem. This can be done in many ways, for example, installing ingress[1] firewalls for preventing the wider Internet from accessing services in possibly malicious ways.

There is another type of firewall called an egress[2] firewall, or a firewall that filters outbound connections from a machine to the internet. Another possible strategy for Network Operators should be to deploy SAV to ensure that every packet received and forwarded hold an authenticated source IP address.

[1] https://en.wikipedia.org/wiki/Ingress_filtering
[2] https://en.wikipedia.org/wiki/Egress_filtering

# Other actors related to the issue

There are other actors that can be influenced by the security issue we are focusing (spoofing-based denial of service (DoS) attacks). Such as

1. **The Country,** because their reputation is on stake.
2. **The Victim,** who basically pays all the losses and bear the cost of a DDoS attack and their Preventions in some cases.
3. **The End User/Payer**, who pays and loses the bandwidth of it's network.

**The Domain Name System (DNS)** is a another such actor and a critical element of the Internet infrastructure can be influenced by the security issue we are focusing (spoofing-based denial of service (DoS) attacks).

Even a small part of the DNS infrastructure being unavailable for a very short period of time could potentially upset the entire Internet and is thus totally unacceptable.

Unfortunately, because DNS queries and responses are mostly UDP-based, it is vulnerable to spoofing-based denial of service (DoS) attacks, which are difficult to defeat without incurring significant collateral damage. The key to prevent this type of DoS attacks is spoof detection, which enables selective discarding of spoofed DNS requests without jeopardizing the quality of service to legitimate requests.

# Risk Strategies that other Actors can adopt

### The Domain Name System (DNS)

There are two possible DoS attack strategies against DNS servers. The first is to send a large number of requests to a DNS server to overload it. Because a standard DNS server cannot distinguish between spoofed and non-spoofed requests, it has no choice but to handle all of them when it can, and starts to drop requests indiscriminately when it becomes overloaded.

The other attack strategy is to exploit DNS servers to amplify attack traffic. The attacker crafts a DNS request that gets a response significantly larger than the request itself, e.g., a 50-byte request for a

500-byte response. The amplified response is replied to a spoofed third-party victim machine. Under this attack, both the amplifying DNS server's upstream bandwidth and the third-party machine's downstream bandwidth could be exhausted. Due to traffic amplification, an attacker can starve the bandwidth of its victims even if his bandwidth is 10 times smaller.

These the following strategies being used in practice by DNS server. In all these strategies, a DNS server sends a distinct cookie to each requesting host, and the requester associates each request it sends to the DNS server with the server's corresponding cookie. By checking the cookie that comes with each incoming request, it is possible to determine if a DNS request indeed originates from source address indicated in the packet. However, how to introduce these cookies in a way that is transparent to the existing Internet infrastructure and incurs minimal performance overhead is the design challenge.

1. **DNSSEC**

The DNS Security Extensions, it's much easier. DNSSEC stores cryptographic keys and digital signatures in records in the namespace. These are positively enormous.

2. **Hop count based mechanism called HCF to detect spoofed packets.**

Servers can learn the normal distance (hop count) of their clients. It is assumed that there is no easy way for an attacker to learn the distance between a server and its clients, thus the server can detect spoofed packets because of the incorrect hop count in the packet.

3. **TTL to detect spoofing.**

Overall this is a good solution. But some drawbacks may hinder its application to DNS because of the false negative ratio and hop count learning issue.

4. **Ingress Filtering**

It deploys filters at the edge of the network to discard packets whose source IP is not in the edge network. Unfortunately, its effectiveness depends on the universal deployment. In reality, the deployment is slow due to administrative burden, lack of incentive and so on.

5. **The Pushback Mechanism**

It allow routers to limit attack traffic to some destinations.

Following are some other strategies in practice by Victims not specific to DNS.

1. **Blackholing**

Blackholing describes the process of a service provider blocking all traffic destined for a targeted enterprise as far upstream as possible, sending the diverted traffic to a "black hole" where it is discarded in an effort to save the provider's network and its other customers. Because legitimate packets are discarded along with malicious attack traffic, blackholing is not a solution. Victims lose all their traffic-and the attacker wins.

2. **Router filtering**
    a. **Access control lists (ACLs)**

        In general, although router ACLs do provide a first line of defense against basic attacks, they are not optimized to defend against the following sophisticated types of DDoS attacks: SYN, SYN-ACK, FIN, etc

3. **Firewalls**
4. **Intrusion Detection System (IDS)**
5. **Manual Responses to DDoS Attacks**

Typically to ask the closest upstream connectivity provider-an Internet service provider (ISP), a hosting provider, or a backbone carrier-to try to identify the source. With spoofed addresses, this can be a long and tedious process that requires cooperation among many providers. And though a source might be identified, blocking it would mean blocking all traffic-good and bad.

6. **Over Provisioning**

that is, buying excess bandwidth or redundant network devices to handle any spikes in demand. Such an approach is not particularly cost effective, especially because it requires the addition of redundant network interfaces and devices. And regardless of the initial effect, attackers merely need to increase the volume of the attack to defeat the extra capacity.