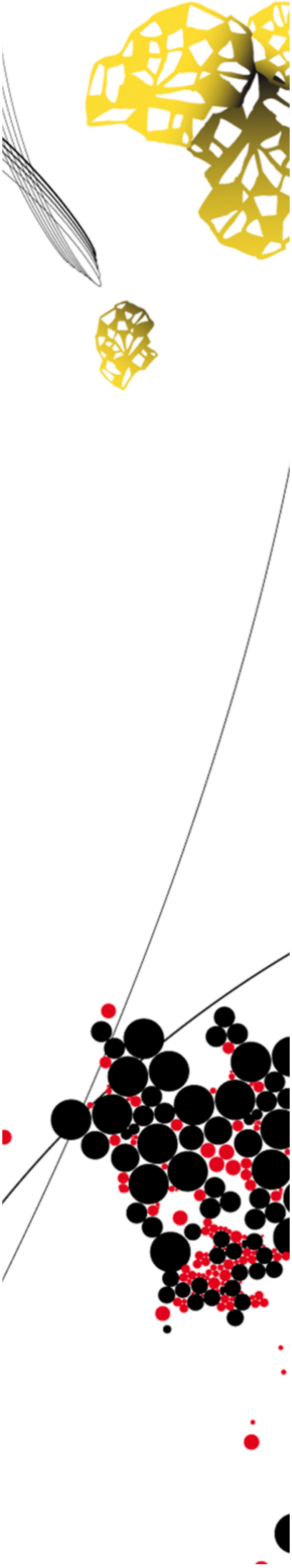

UNIVERSITY OF TWENTE.

Faculty of Electrical Engineering,
Mathematics & Computer Science

Economics of Security
Individual assignment

Jonathan Quigley
Master Computer Science
November 2016

Supervisor:
prof. dr. ir. C. H. Gañán

Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

Abstract

IP spoofing has been a major security issue for numerous years now. As it allows to conduct anonymized DDoS attacks, eradicating it would significantly decrease the number of those attacks. In fact, technical solutions have been existing for years as well, but need to be globally implemented to become efficient. However, the incentives are not strong for network operators to deploy them. Indeed, applying these solutions would only benefit the others by not allowing malicious traffic to escape their network, without any major gain for themselves. This paper aims at depicting the current situation of this security issue, and finding factors that could explain why security performance are not homogenous among all networks.

Summary

Introduction

The number of Distributed Denial of Service (DDoS) attacks is irreparably growing, and their power seems to increase as well. For instance, OVH, a French hosting firm experienced in September 2016 a record attack of 1 terabit/s. More recently, on the 8th of November 2016, five of the biggest Russian banks were hit by a DDoS attack during two days, although they managed to mitigate the attack and keep their online services up. Both were caused by botnets which include a large number of IoT devices, which is estimated to reach 150,000 in the case on the attack on OVH. These attacks obviously raise the question of security of IoT devices, but it is not the only security issue which allows DDoS attacks to happen. Indeed, in order to keep his identity secret, an attacker may use a method called IP spoofing, as pictured in figure 1. This consists in sending packets using the victim IP address as source of the traffic. The receiver will then forward its reply to the victim instead of the attacker.

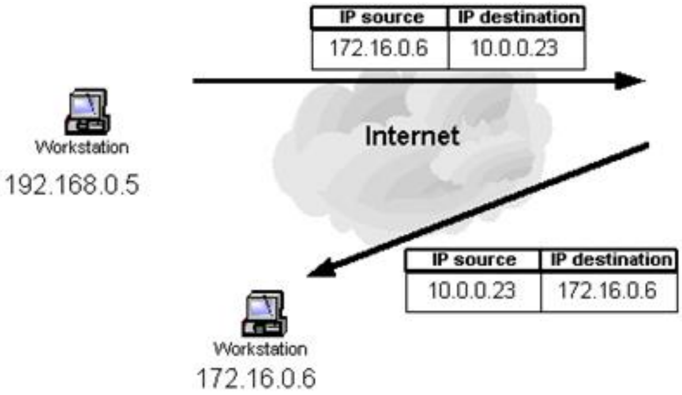

Figure 1: IP Spoofing example

This issue is key in the global problem of DDoS attacks. If spoofing was not allowed, anonymous attacks would not be possible anymore, as the originating network could be determined. Unfortunately, the Internet consists of numerous Autonomous Systems (ASs), administrated by several entities with different incentives in mitigating this security issue. In fact, in order to efficiently fight spoofing, technical controls should be implemented by the whole community. Here, the problem is that preventing IP spoofing will mainly protect others from being targeted by an attack originating from your own network. Thus, the incentives to mitigate spoofing seem to be low for network operators.

In this paper, I will try to analyze these incentives. First, by reviewing some literature about this security issue. Then, I will expand on the research question of this paper and a hypothesis. To end with, I will describe the results of this study, expand on its limitations, and draw conclusions.

Literature review

To begin with, I selected the RFC (Request for Comments) 2827, from P. Ferguson [1]. Also referred to as BCP 38 (for Best Common Practice), this document describes ingress traffic filtering, a method to block spoofed traffic. Ingress filtering consists in applying a filter on the access routers of a network, by controlling the coherence of the source address of the traffic with the prefix of its origin. For example, if an Internet Service Provider (ISP) has a customer with prefix 10.11.12.0/24, the router connected to this customer would check if all source addresses for incoming traffic fall into this range. Otherwise, the traffic would be dropped.
This does not solve completely the problem of spoofing, as a user of the customer network could use a forged address within the allowed range. However, it becomes easier to track down the origin of malicious traffic, as network administrators know which network it is originating from.

The article of F. Y. Rashid [2] shows the implication of an organism such as the Internet Society in the fight against IP spoofing. Within the MANRS (Mutually Agreed Norms for Routing Security) program, network operators are provided help to implement filtering solutions, and coordinate their efforts to reduce the cost of implementing these controls. The program produces for instance training supports and self-assessment guides for ISPs to make their network “unspoofable”. The community only counts 40 members, which seems tiny in comparison with the 50,000 Ass that compose the Internet. However, it still makes a difference, as the group effect can promote the good behavior of these ISPs and trigger a snowball effect.

Brian Krebs, author of the website krebsonsecurity.com, has been the victim of a record DDoS attack in September 2016. In his article *The Democratization of Censorship* [3], describes the circumstances of this attack, but also reports the problem of spoofing. He especially mentions the Spoofer[1] project from CAIDA, which aims at collecting data on the behavior of networks with respect to filtering. This project allows an end user to test its network provider reaction to spoofed traffic, and thereby control if it is acting against spoofing or not. Collecting all data provided by the users of the project may then be used to shame the “bad behaviors”, and convince them to help solving this issue. Unfortunately, the results of Spoofer depend on the users that run the tool, and therefore do not cover a high percentage of the whole Internet. Krebs suggest that a coalition should be formed, with the major actors like hardware manufacturers, operating systems providers and hosting firms. Working together, Krebs thinks they could deploy tools like the one from Spoofer on every host, to get more transparency on ISPs behavior.

McConachie (2014) [4] mentions that the issue around Source Address Validation (SAV) is often referred to as a Tragedy of the Commons. This means an ISP implementing SAV would only benefit the global community, and the network

[1] The project is based on a client, available for anyone, which tests the network of the user by sending spoofed traffic to CAIDA servers. https://www.caida.org/projects/spoofer/

operator would not get any personal profit. Indeed, a network operator could consider DDoS attacks are not his problem since they do not harm his network, and chose to save money by not implementing filtering. However, the author underlines that these costs are overestimated, as for instance a large part of current equipment from ISPs can already be used to process filtering. The only cost would be the additional load of work of training staff and maintaining large lists of filters. For this problem, McConachie argues that information is provided to network operators in order to facilitate this work, by the means of public work groups.

In the paper from Beverly et al. [5], the issue of spoofing is well described, especially by showing three types of attack that exploit it. Moreover, CAIDA Spoofer project is promoted, by detailing the methodology, the results, and finally the conclusions that can be drawn from these measurements. A noticeable number is the percentage of clients that can send spoofed traffic, which is 0.33. This shows that spoofing is still an issue, even if solutions like BCP 38 exist since more than a decade. The limitations of these solutions are also discussed. For instance, ingress filtering is the more effective when applied at the edge of the network, where most users are. Otherwise, an AS in the core of the network would have to handle very large filtering lists to validate the non-malicious traffic.

Research Question, Objective and Hypothesis

As we have seen in the previous section, a lot of efforts have been done to encourage the Internet Service Providers (ISPs) and other network operators to mitigate IP spoofing. Some technical solutions like ingress filtering have been proven efficient, but only if implemented at a global scale. The main negative incentive for network operators is that filtering will only benefit the others without generating profit for themselves.

Some initiatives to promote the good behaviors exist, like the MANRS program from the Internet Society, which gathers AS operators cooperating to fight spoofing. The Spoofer project from CAIDA allows everyone to test its provider network and determine if it is spoofable or not. This way, the security performances of every tested operator is publicly available, and this can produce a “shaming” effect.

The aim of this paper is to understand better why there are still some differences in security performances regarding spoofing. In others words, what are the factors that explain these differences? This will result in subquestions, such as: “Are ASs on the edge of the network more secured than in the core?”, and “Is security performance better within the more developed countries?”.

Methodology

The method that will be used for this study is quantitative measurement, relying on the data provided by the Spoofer project. For the analysis of the influence of the position of an AS on its security performance, each AS transit degree will be sampled. The degree of an AS represents the number of relationships it has with its neighbors. The higher the degree, the deeper in the network is the AS is located. The dataset will include all ASs from Netherlands that have been tested within the Spoofer project. Regarding the relationship between security performance and ASs' country of affiliation, a quantitative method will also be used. The scope will be limited to a few countries.

Results

The dataset includes records for 29 different ASs from the Netherlands. For each of them, their transit degree has been collected, using the data from another CAIDA project[2]. The Spoofer project provides different tests, using private or routable IPv4 addresses, or even IPv6 if it is available to the user. For the analysis, the test with a routable IPv4 address has been selected, as it represents the main part of the issue. Moreover, the records which detected the presence of a NAT have been put aside, since they do not permit to test the vulnerability of the network.
Several test records exist for some ASs, and when this is the case, it is considered as spoofable if 50% or more of the tests are positive. On the table 1 below, we can find the list of these ASs, their transit degree and their vulnerability to spoofing.

For a certain number of ASs, the transit degree is null, meaning that they have very few neighbors, usually one or more provider(s). These ASs are on the edge of the network topology. As we can see, a large majority of those are not allowing spoofed traffic, which is a positive point, because they are the interfaces for end users. On the other hand, we notice that all ASs with a degree between 50 and 100 are spoofable. One could argue that this networks are in the core, and therefore it is not their responsibility to validate the source of the traffic, but rather that of their customers. However, if their customers do not implement SAV, any end user of these networks can send spoofed traffic successfully. In fact, ASs with more relations need more work to build and maintain the filters on their edge routers, because the number of prefixes to check is much larger. Nonetheless, the ASs with a large number of customers should have the financial and human resources to handle this problem.

[2] http://as-rank.caida.org/

ASN	Spoofable	AS transit degree
1128 (TUDELFT-NL)	No	0
20857 (TRANSIP-AS)	No	0
196752 (TILAA)	No	0
198203 (ASN-ROUTELABEL)	No	0
199664 (NLNETLABS)	No	0
200130 (DIGITALOCEAN-ASN-1)	No	0
200837 (PCEXTREME-UK)	Yes	0
202018 (DIGITALOCEAN-ASN-3)	No	0
202109 (DIGITALOCEAN-ASN-2)	No	0
1133 (UTWENTE-AS)	No	0
57043 (HOSTKEY-AS)	No	0
57062 (SERVERCLUB-AS)	No	0
59743 (EliteHosting)	No	0
60117 (HS)	No	0
63473 (HostHatch-NA-AS)	No	0
57771 (STEFFANN-AS)	No	2
35017 (SWIFTWAY-AS)	No	4
56611 (REBACOM-AS)	No	4
49349 (DOTSI)	No	5
60144 (THREE-W-INFRA-AS)	Yes	6
4608 (APNIC-SERVICES)	No	9
48635 (PCEXTREME)	No	21
49981 (WorldStream)	Yes	60
29073 (QUASINETWORKS)	Yes	66
47869 (NETROUTING-AS)	Yes	89
31216 (BSOCOM)	Yes	98
43350 (NFORCE)	Yes	98
49544 (INTERACTIVE3D)	No	106
50673 (Serverius-as)	No	110

Table 1: Vulnerability to spoofing and degree of ASs in the Netherlands

To compare security performance within different part of the world, 8 countries have been selected in the dataset from CAIDA, for which significant data is available. For each country, all records which do not include NAT are considered, and with the same method as before, each AS is determined as spoofable or not. The results of these measurements are visible on figure 2.

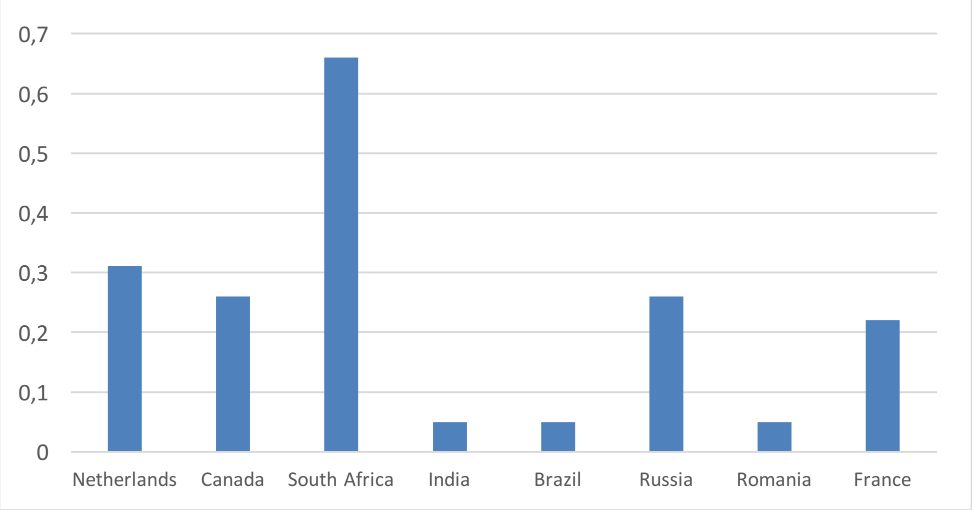

Figure 2: Percentage of spoofable ASs by country

Contrary to what we could infer, the more developed countries do not present better security performance than others. Indeed, apart from South Africa, it seems that countries of the “South” have lower rates than their pairs from the “North”. However, this hypothesis is not fully verified, as only eight countries do not represent the whole picture. Moreover, some countries do not have sufficient data to draw raw conclusions, like only 3 different ASs for South Africa. Plus, because the tests from Spoofer depend on the users willing to run the client, the trends shown by the measurements can differ from the real situation. For instance, because the usage of a NAT does not allow the tests to be concluding, a large part of the population is not represented in these results. All these factors could explain the surprising trend pictured by the graph.

In fact, Beverly et al. described the inverse situation, with for example 32% of positive spoofable results, and less than 20% for Europe and North America. However, the dataset they used is slightly different, as the time period is not the same, and the metric may also be different.

Limitations

A valuable metric for this analysis would have been the evolution over the years from the behavior of network operators. For instance, verifying if networks gained in customers or peering relations after having implemented filtering. Unfortunately, the dataset from CAIDA contains only records for the last 6 months, which does not permit to conduct this analysis with enough samples. Another interesting information would be the evolution of spoofable networks by country, in order to show if a policy adopted by a country was efficient to mitigate spoofing.

In addition, it has not been possible to compare security performance between different types of network, due to the unavailability of a reliable source of data. Plus, by looking manually for the ASs from the dataset, it is noticeable that most of them are from hosting companies or educational networks.

Conclusions

The literature review showed that IP spoofing is still a major issue, even if some technical solutions exist since more than ten years. Many initiatives exist to encourage network providers to implement filtering, in order to reduce the number of anonymized DDoS attacks. However, within this study we have seen that there is still a substantial part of networks that allow spoofing. And this situation is not necessarily better in developed countries than in others.

The Spoofer project allowed us to have a picture of the current situation, by gathering data over a large population of networks. Nonetheless, the dataset was limited by the number of clients that ran the tool from CAIDA. To have complete and reliable data over all networks, the solution may be what Krebs described as a “coalition” of hardware and software manufacturers. They could decide to include measurement tools like the one from CAIDA. This would allow to break the asymmetry information that exists nowadays, and shame the bad behaviors.

Bibliography

1. P. Ferguson (2000), *RFC 2827 (BCP 38)*, https://tools.ietf.org/html/rfc2827#page-3

2. F. Y. Rashid (2016), *ISPs mind their MANRS to block DDoS attacks*, http://www.infoworld.com/article/3131016/security/isps-mind-their-manrs-to-block-ddos-attacks.html

3. B. Krebs (2016), *The Democratization of Censorship*, https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/

4. A. McConachie (2014), *Anti-Spoofing, BCP 38, and the Tragedy of the Commons*, http://www.internetsociety.org/deploy360/blog/2014/07/anti-spoofing-bcp-38-and-the-tragedy-of-the-commons/

5. R. Beverly, A. Berger, Y. Hyun, K. Claffy, *Understanding the Efficacy of Deployed Internet Source Address Validation Filtering*, https://www.akamai.com/cn/zh/multimedia/documents/technical-publication/understanding-the-efficacy-of-deployed-internet-source-address-validation-filtering-technical-publication.pdf