



SOURCE ADDRESS VALIDATION

EOS

Akbar Aryanto(s1770705)

**Faculty of Electrical Engineering,
Mathematics and Computer Science (EEMCS)**

Documentnumber

4TU : Cyber Security Specialization — 201500028

Contents

1	Introduction	3
2	Literature Review	4
3	Research Question, Objective and Hypothesis	4
4	Methodology	5
4.1	CAIDA	5
4.2	AKAMAI	6
5	Results	7
6	Limitations	9
7	Conclusions	9
	References	9

Abstract

The growth of internet brings positive and negative impact to different actors. One security issue is IP spoofing. Implementing Source Address Validation (SAV) is necessary in order to detect and reject spoofed IP packets in the network, and contributes to the overall security of IP networks. The country as other big actor got indirect incentive from implementing the countermeasure. In this paper will describe whether the country with low cyber attacks originate is the safest from IP spoofing. we analyze two variable data from CAIDA and AKAMAI using t-test statistic technique. The result proved that there is a correlation between that two variable. *Keywords* - **networks operator, ingress filtering, SAV**.

1 Introduction

Internet change all the time, the growing of the social web and mobile technology changed the way of people using the internet. Access to the social media become easy by mobile technology. The number of internet user become growing fast annually(Stats, 2016 (accessed November, 2016)). Moreover, with very low investment people can easily build and hosting their own web page on the internet, one aspect such as business give an impact to the growing of the internet.

Due to the growth in Internet use, the number of computer security breaches has increased rapidly in recent years. No one can guarantee a hundred percent safe while dealing with the internet. In this paper, we will focus on Distributed Denial of Services (DDoS) as a security issue. The increasing number of DDoS attacks growths rapidly in this two year(Akamai, 2016). Several attackers massively exploited recursive name servers to amplify DDoS attacks against several networks utilizing IP spoofing.

The Center for Applied Internet Data Analysis (CAIDA), is an organization funded by the U.S. Department of Homeland Security Science and Technology Directorate. Its mission is to conduct research in macroscopic usage and behavior of the Internet. One of CAIDA projects called Spoofer, focuses on IP Spoofing vulnerabilities¹. Seeking to minimize Internet's susceptibility to spoofed DDoS attacks, the organization is developing and supporting open-source software tools to assess and report on the deployment of Source Address Validation (SAV) best anti-spoofing practices.

However, in the context of this project the idea of finding a solutions for mitigate or reduce the main issue. SAV is a technique to verify that source IP addresses of packets submitted to the internet are valid, not assigned from private address space and from a range within of legitimately advertised prefixes for a liable origin, on the other words SAV can mitigate IP spoofing and DDoS attacks as well. To analyze such activities we have defined a goal and illustrated an approach to reach to a desired conclusion.

¹<https://www.caida.org/projects/spoofer/>

2 Literature Review

In this paper, we choose actors impacted by this security issue, and especially on the problem owner. We identified network operators as the problem owner because they have the ability to implement SAV solution to prevent IP spoofing and DDoS attacks. Many operational networks implement SAV best common practices (Beverly & Bauer, 2007). Ingress address filtering (Ferguson, 2000) and unicast reverse path forwarding (uRPF) (Baker, 2004) are effective countermeasures against source spoofing. Ingress traffic filtering at the periphery of Internet connected networks will reduce the effectiveness of source address spoofing denial of service attacks. Network service providers and administrators have already begun implementing this type of filtering on periphery routers, and it is recommended that all service providers do so as soon as possible (Ferguson, 2000). The Governments might endorse regulations that require networks operator to implement filtering, overcoming the aforementioned security issues (Beverly, Berger, Hyun, & k claffy, 2009).

Another actor, that can be influenced by the security issue 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. 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.

3 Research Question, Objective and Hypothesis

This paper was mainly initiated to find the countermeasures of IP spoofing that impact to DDoS attack on the problem owners. While network operators in the particular country try to mitigate the IP spoofing, theoretical the number of attackers from that country will decrease. The country's reputation is a very sensitive issue. The government of each country should take some measures in order to avoid and mitigate in the first place the risk caused by spoofing based on denial of service (DoS) attacks. The question that we are trying to answer here is whether the country with low cyber attacks originate is the safest from IP spoofing. To answer this question we make hypotheses.

H0: Security performance is correlated to the number of attackers

H1: Security performance is independent to the number of attackers


The main aim of this paper is to find the relationship between the country with high cyber attacks originate with the level of safety from IP spoofing.

4 Methodology

Our methodology is based on CAIDA spoofer project data². CAIDA collected all logs from all around the world which running the spoofer manager application. Data that we use are result categorized by country. Another data that we will compare is Top 10 Source Countries for DDoS Attacks, Q2 2016 from Akamai(Akamai, 2016). Both data are quantitative data, to comparing the mean of two unmatched groups we use unpaired t-test statistical technique.

4.1 CAIDA

We analyze the data from CAIDA's website³, those data categorized based on country from year 2016.



Center for Applied Internet Data Analysis

HOME	RESEARCH	DATA	TOOLS	INTERACTIVE	PUBLICATIONS	WORKSHOPS	PR
------	----------	------	-------	-------------	--------------	-----------	----

Country stats for last year of data

I Spoofer Project Page
I Data: Stats Summary Recent Tests

Country	Client Prefixes	Spoofing Prefixes	Blocking Prefixes	Inconsistent Prefixes
usa (United States)	286	118 (41.3%)	162 (56.6%)	6 (2.1%)
can (Canada)	35	19 (54.3%)	15 (42.9%)	1 (2.9%)
deu (Germany)	54	14 (25.9%)	36 (66.7%)	4 (7.4%)
zaf (South Africa)	16	14 (87.5%)	2 (12.5%)	0 (0.0%)
ind (India)	14	11 (78.6%)	3 (21.4%)	0 (0.0%)
gbr (United Kingdom)	39	10 (25.6%)	27 (69.2%)	2 (5.1%)
nzl (New Zealand)	11	9 (81.8%)	2 (18.2%)	0 (0.0%)
bra (Brazil)	13	7 (53.8%)	6 (46.2%)	0 (0.0%)
fra (France)	20	7 (35.0%)	13 (65.0%)	0 (0.0%)
nld (Netherlands)	53	7 (13.2%)	42 (79.2%)	4 (7.5%)
aus (Australia)	18	6 (33.3%)	11 (61.1%)	1 (5.6%)
ita (Italy)	11	6 (54.5%)	5 (45.5%)	0 (0.0%)
rus (Russian Federation)	12	6 (50.0%)	6 (50.0%)	0 (0.0%)
aut (Austria)	8	5 (62.5%)	3 (37.5%)	0 (0.0%)
che (Switzerland)	13	4 (30.8%)	8 (61.5%)	1 (7.7%)
idn (Indonesia)	4	4 (100.0%)	0 (0.0%)	0 (0.0%)
isr (Israel)	4	4 (100.0%)	0 (0.0%)	0 (0.0%)
kor (South Korea)	98	4 (4.1%)	93 (94.9%)	1 (1.0%)
lva (Latvia)	5	4 (80.0%)	1 (20.0%)	0 (0.0%)
vnm (Vietnam)	5	4 (80.0%)	1 (20.0%)	0 (0.0%)
arg (Argentina)	4	3 (75.0%)	1 (25.0%)	0 (0.0%)

Figure 1: Spoofer result classified by country

From the data we grab information about:

²<https://www.caida.org/projects/spoofers/>

³https://spoofers.caida.org/country_stats.php

1. Name of country
2. Client prefixes, number of clients prefixes that running the application
3. Spoofing prefixes, number of client source prefixes that vulnerable or spoofable
4. Blocking prefixes, number of client source prefixes that secure or unspoofable
5. Inconsistent prefix, number of client source prefixes with conflicting results from different IP addresses

We will focus on unspoofable data that will show security performance of a particular country.

4.2 AKAMAI

The State of the Internet / Security Report from Akamai shows Top 10 Countries Where Cyber Attacks Originate at quarter 2 year 2016(Akamai, 2016),


















 China	56.09%	
 US	17.38%	
 Taiwan	5.22%	
 Canada	3.77%	
 Vietnam	3.70%	
 Brazil	2.96%	
 Spain	2.94%	
 Singapore	2.90%	
 Italy	2.65%	
 UK	2.38%	

Figure 2: Top 10 Source Countries for DDoS Attacks

From the data shows the percentage number of Source Countries for DDoS Attacks at quarter 2, 2016.

We will use SPSS statistics software to analyze those two data provided by CAIDA⁴ and AKAMAI⁵. The data very limited because of we only data for less than one year. The result at part 5 will describe a correlation between the two variables and consequently to answer the research question using the hypothesis.

5 Results

Because we cannot find Taiwan on the data prefix client which running the application in CAIDA result, so we decided to omit Taiwan from list attacker table.

Country	world's attack traffic (%)	Blocking Prefix (%)
China	56.09	100
U.S.	17.38	59.7
Canada	3.77	44.4
Vietnam	3.7	20
Brazil	2.96	46.2
Spain	2.94	50
Singapore	2.9	100
Italy	2.65	45.5
UK	2.38	73

Figure 3: Table security performance vs number attackers

to comparing the means of two unmatched groups we use unpaired t-test.

Parameter	
Table Analyzed	Paired t test data
Column A	World attack
vs	vs
Column B	Blocking
Unpaired t test	
P value	0,0003
P value summary	***
Are means signif. different? (P < 0.05)	Yes
One- or two-tailed P value?	Two-tailed
t, df	t=4.615 df=16

Figure 4: Table unpaired t test

⁴https://spoofer.caida.org/country_stats.php

⁵<https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-state-of-the-internet-security-report.pdf>

The unpaired t test assumes that the worlds attack traffic and blocking prefix data have the same variances. The two tailed P value less then 0.05, that mean number of attackers from particular country differed significantly among the security performance on the same country. This means we have chance higher than 1 percent to finding the differences in our data. with P value 0.0003 we conclude those two groups are not equal.

Correlations			
		percentage of the world's attack traffic	percentage of Blocking Prefix
percentage of the world's attack traffic	Pearson Correlation	1	.549
	Sig. (2-tailed)		.126
	N	9	9
percentage of Blocking Prefix	Pearson Correlation	.549	1
	Sig. (2-tailed)	.126	
	N	9	9

Figure 5: Table correlation

From the Pearson's r we can find there is a relative strong relationship between these two variables, but no significant correlation (P higher than 0.05).

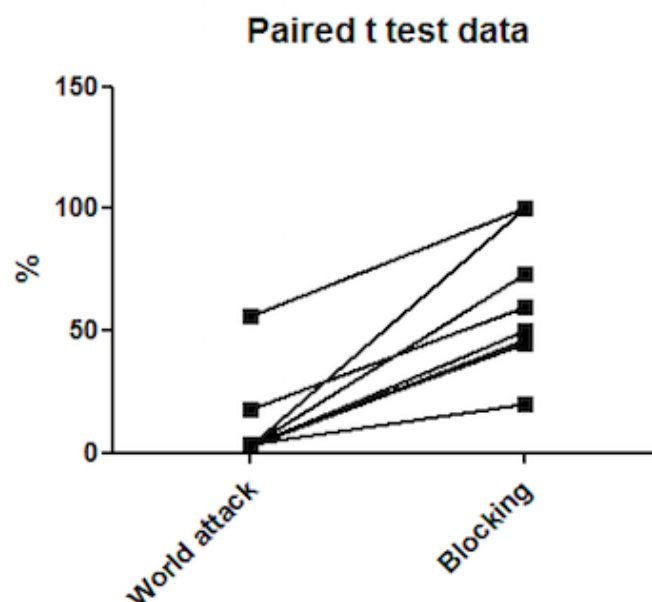


Figure 6: security performance vs number of attackers

the conclusion of the data analysis using unpaired t-test statistical technique shows on figure 6, security performance or a number of blocked spoofing IP is correlated with a number of attackers comes from the same country.

6 Limitations

This paper describes concrete countermeasure for the actors, implementing ingress filtering at network operators will bring direct incentive to them, such as customer protection and customer satisfaction. Moreover, others actor like country got positive incentive as well. The most valuable impact is reputation. Parallel with it, a theoretical number of the attacker from origin country will decrease, but this report rejected these hypotheses. Due to a limitation of data that we have, this proven can be improved in the future.

7 Conclusions

In this paper, we show important actor that can bring the solution to mitigate DDoS attack, networks operator, parallel with that Country another big actor also get the positive impact of implementing the countermeasures. One of the countermeasures is ingress filtering(Ferguson, 2000). on the analysis at section 5 shows security performance or number of blocked spoofing IP is correlated with number of attackers comes from the same country, and out question answer that the country with low cyber attacks originate is not the safest from IP spoofing (figure 6). And proven hypotheses 0 : there is correlation between Security performance and the number of attackers from the same country, even tough only small correlation due to small data we have.

References

- Akamai. (2016). *Akamais [state of the internet] / security q2 2016 report*. Retrieved from <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-state-of-the-internet-security-report.pdf>
- Baker, F. (2004). *Bcp 84 : Ingress filtering for multihomed networks*. Retrieved from <https://www.ietf.org/rfc/rfc3704.txt>
- Beverly, R., & Bauer, S. (2007, August). *Tracefilter: A tool for locating network source address validation filters*.
- Beverly, R., Berger, A., Hyun, Y., & k claffy. (2009, November). Understanding the efficacy of deployed internet source address validation filtering. In *Proceedings of the ninth acm sigcomm/usenix internet measurement conference (IMC)*.
- Ferguson, P. (2000). *Bcp 38 : Network ingress filtering : Defeating denial of service attacks which employ ip source address spoofing*. Retrieved from <https://www.ietf.org/rfc/rfc2827.txt>
- Stats, I. W. (2016 (accessed November, 2016)). Internet usage statistics [Computer software manual]. Retrieved from <http://www.internetworldstats.com/stats.htm>