An analysis on London Action Plan's efforts in anti- IP Spoofing measures on ISPs based on CAIDA's Spoofer Project

Amit Gupta
Masters Student, Security and Privacy, University of Twente, Netherlands
a.k.gupta@student.utwente.nl

ABSTRACT
Analyzing the Spoofer data for 37 countries across the globe, it appears that majority of the global ASes are still vulnerable to IP spoofing and need to be protected. This research paper brings forward the importance of protection of IP addresses from being spoofed. Based on the vast utilization of internet and the inter connected devices over the networks, the impact of cybersecurity is strongly reflected on the economies of the world, specially how of the DDoS attacks lead to massive losses to e- businesses. The information from CAIDA's Spoofer application has been used as a basis to study the impact of Source Address validation techniques on control over the uncontrolled DDoS attacks in present day Internet infrastructures. Realizing the importance of reputed London Action Plan (LAP) [12], in the later section of the document, the existent problem has been devised to a research question in relation to LAP. The hypothesized solutions have been solved using statistical measures and the conclusion has been deduced. To solve the issues, we conclude that the network nodes should implement ingress filtering in order to contribute for a better Worldwide network system.

Keywords
Source address validation, IP spoofing, filtering, Autonomous Systems

1. INTRODUCTION
Today, we call the world as a global village. We, the humans have been really innovative and tremendously successful in connecting the people and machines and facilitate their communications. From developing ARPANET in 1960's [1] to today's light fast fiber optics internet connections, we have progressed a long way in the right direction. But it goes unsaid that with great power, comes great responsibilities to make systems safe and secure. No doubt that the billions of connected devices over IoT [2] give us immense empowerment, but the question is how sure are we that the generation old Internet protocols are robust to handle the abuses.

One such gigantic problem today is the Distributed Denial of Service Attack (DDoS) or Denial of Service, as you may call it. We understand one of the core issues how attackers are able to exploit the current Internet infrastructure is by spoofing data request packets from innocent IP Addresses, just with the intention to overload the target servers bandwidth capacity and lead to its downtime. Forcing all IP packets to carry correct source addresses can greatly help network security, attack tracing, and network problem debugging. [3]

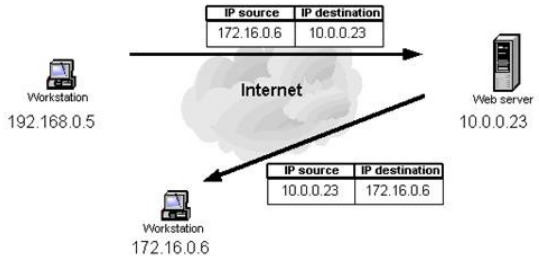

Fig 1: IP Spoofing: A simplified example.

In this paper, we will analyze the study of Center for Applied Internet Data Analysis, CAIDA's "Spoofer" [4] project. As explained in figure 1, IP spoofing is a very simple yet strong way of exploiting present day Internet to as bad as bringing down any online service over IT.

2. LITERATURE REVIEW
Securing the network of networks its susceptibility to malicious attacks has been quite a concern of the Internet Service Providers and the Infrastructure architects. Research and development in this domain has been a hot plate since its existence. There have been many research papers, which reflect intensity on the same domain of problem. In one of the papers [5] presented at the ACM [6], the authors say how IP source address forgery, or "spoofing," is a long-recognized consequence of the

Internet's lack of packet-level authenticity. Despite historical precedent and filtering and tracing efforts, attackers continue to utilize spoofing for anonymity, indirection, and amplification. Using a distributed infrastructure and approximately 12,000 active measurement clients, they collected data on the prevalence and efficacy of current best practices source address validation (SAV) techniques. They quote that, of clients able to test their provider's source-address filtering rules, they find 31% were able to successfully spoof an arbitrary, routable source address, while 77% of clients otherwise were unable to spoof can forge an address within their own /24 sub-network.

Seeking to minimize Internet's susceptibility to spoofed DDoS attacks, CAIDA has been developing and supporting open-source software tools to assess and report on the deployment of source address validation (SAV) best anti-spoofing practices. CAIDA has developed and support a new client-server system that periodically test a network's ability to both send and receive packets with forged source IP addresses (spoofed packets).

One logical solution that came out from the observed gravity of the problem was to use ingress filters on the end of Internet nodes and serving houses. In ingress filtering, packets coming into the network are filtered if the network sending it should not send packets from the originating IP address (es). If the end host is a stub network or host, the router needs to filter all IP packets that have, as the source IP, private addresses (RFC 1918), bogon addresses or addresses that do not have the same network address as the interface. [7]

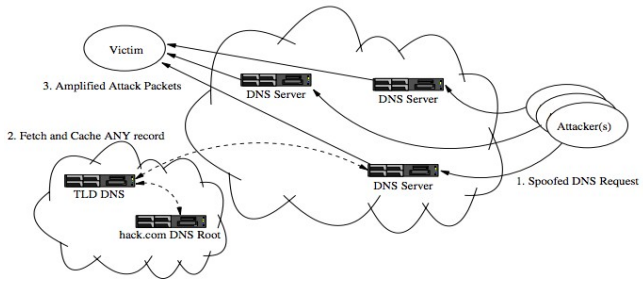

Fig 2: DNS Amplifier: 1) Attacker spoofs DNS request with victim's source for large TXT record. 2) Third-party DNS servers fetch and cache record. 3) Server responds to victim. Attacker's small query packets are amplified and victim cannot identify attack source. [5]

In one of the informational publications [8], Dr. Ferguson and Dr. Senie say, that Ingress traffic filtering at the periphery of Internet connected networks will reduce the effectiveness of source address spoofing denial of service attacks. They believe that though many Network service providers and administrators have already begun implementing this type of filtering on periphery routers, it is highly recommended that all service providers do so as soon as possible. In the also report that, in addition to aiding the Internet community as a whole to defeat this attack method, it can also assist service providers in locating the source of the attack if service providers can categorically demonstrate that their network already has ingress filtering in place on customer links. In one of the research studies [9] where authors Beverly and Bauer study the origin and nature of source address filtering claim an interesting conclusion that a significant fraction, approximately one-quarter, of the net blocks, IP addresses and ASes observed permit spoofing. This suggests that a large portion of the Internet is still vulnerable to spoofing and concerted spoofing attacks remain a serious concern. Projecting our results to the entire Internet yields over 360M spoofable addresses and 4,600 ASes from which spoofing is possible. This is particularly significant if next generation attack farms intelligently probe the network and adaptively change behavior based on the ability to spoof.

3. OBJECTIVE/HYPOTHESIS

Given our understandings about the harsh effects because of DDoS attacks on standing economies, this paper brings forward a perspective about the gravity of the issues pertaining around IP Spoofing in the present day internet protocol system and how source address validation can mean some help. Keeping in mind the results from CAIDS's Spoofer tools, this brings in to the postulation of a strong question in the domain of economics of cyber security - *given the negative impacts of DDoS attacks, it is suggested that all the ASes implement SAV on their network nodes, then what is that one corrective action that decision makers can take?*

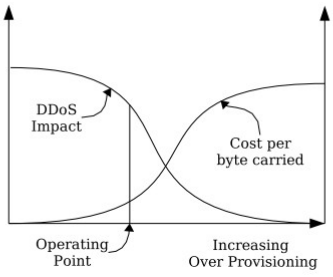

Fig 3: Cost per-byte-carried and DDoS Impact as a function of network over-provisioning [10]

The cost of a Distributed Denial of Service (DDoS) attack can continue to impact on the targeted organization long after the event has been dealt with. It is not just the disruption to the public interface, which is damaging enough to any organization that conducts a substantial volume of its business online. Loss of revenues while services and systems are unavailable to customers

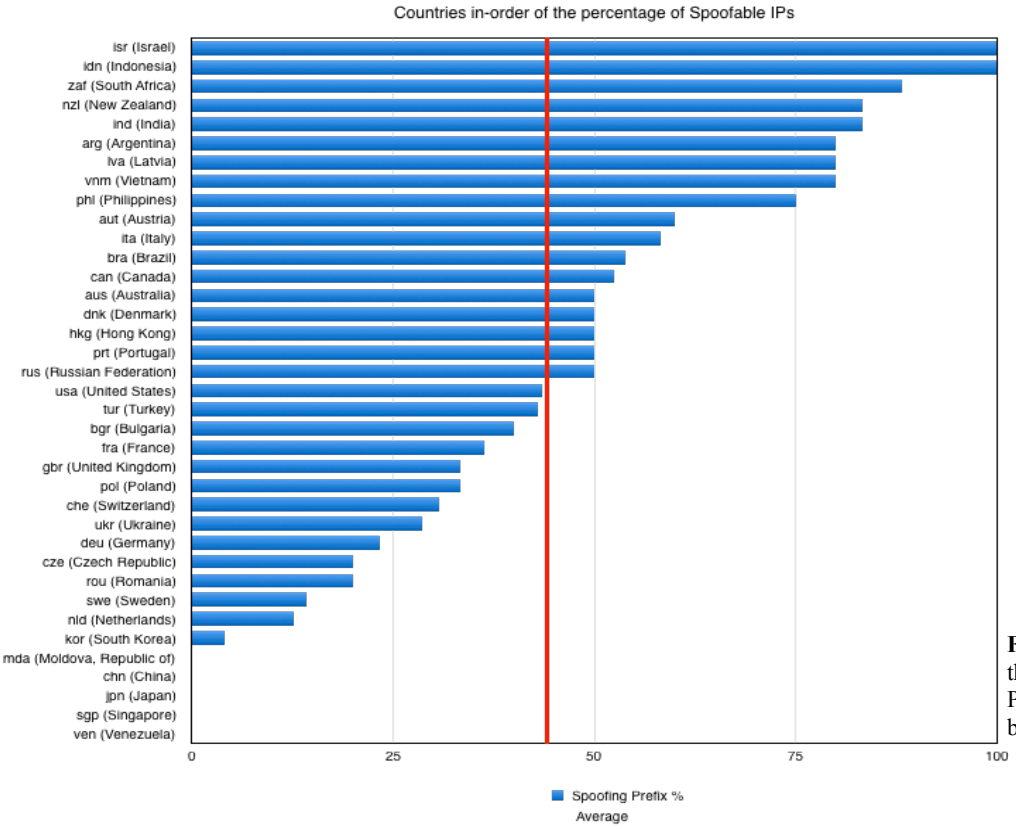

Figure 5: Countries with less than average Spoofable Prefixes and the percentage of blocked Spoofing attacks by

are compounded by the cost of rectifying the crisis and long- term damage to the business's reputation In some cases an organization might even submit to extortion from the hackers, effectively paying a ransom to rid itself of the problem – until the next strike from another hacker source. [11]. Then what is it that's stopping the empowered people to take charge on the situation and take decisions to mitigate the arising problems.

3.1 RESEARCH QUESTION AND HYPOTHESIS

In one of his paper on Economics of Fighting Botnets, Hadi et.al proposes how ISPs have become increasingly central to the effort, as they can undertake mitigation more economically than end users. [12] In this research we take the research to a more action-oriented cone. I analyzed the Spoofer data for 37 countries across the globe to understand the differences and draw relations. *Given the dataset, the purpose of this research is to find the top countries that need to take actions to minimize Internet's susceptibility to IP Spoofing.*

London Action Plan (LAP) is an international cybersecurity enforcement network. 80 organizations from 35 nations are member of this association where they share information and intelligence to identify risks and opportunities for enforcement action and/or prevention. [13] The members of the LAP follow the shared cybersecurity enforcements to make sure the world has an ethical and balanced IT network system.

Hypothesis 0: Being a member of the LAP would help the underperforming countries standardize their network against IP Spoofing.

Hypothesis 1: Being a member of LAP does not guarantee security against IP Spoofing.

4. METHODOLOGIES

4.1 We analyzed the data from the Spoofer application to sort the countries in order of their vulnerability to IP spoofing and draw an average performance score for the given dataset.

4.2 It was interesting to find that the at an average 43.98 % of the IPs in the network of the given countries were spoofable. Now the question was to understand which countries appear to be most spoofable and what can they do to be better. Also, to mention, which countries have score less than average and what did they do to mitigate the risks.

4.3 To understand what is special about the countries scoring best on the list of most spoofable nations, I casted a relationship between the countries blocked prefixes and its spoofable prefixes.

4.4 It is quite evident that the best performing countries are blocking the spoofing attacks. That bolsters the point for the underperforming countries, that blocking the malicious packets can be one good way to protect their networks from being used for complex cyber attacks.

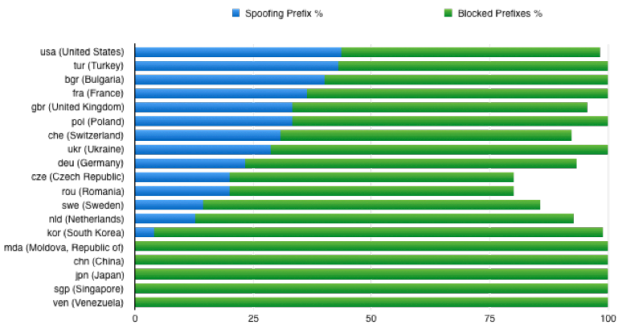

Figure 4: Spoofability of countries and average spoofability percentage score.

Country	% Spoofable Prefixes
usa (United States)	43.6
tur (Turkey)	42.9
bgr (Bulgaria)	40
fra (France)	36.4
gbr (United Kingdom)	33.3
pol (Poland)	33.3
che (Switzerland)	30.8
ukr (Ukraine)	28.6
deu (Germany)	23.3
cze (Czech Republic)	20
rou (Romania)	20
swe (Sweden)	14.3
nld (Netherlands)	12.7
kor (South Korea)	4

Figure 6: Best-Performing countries against IP spoofing attacks.

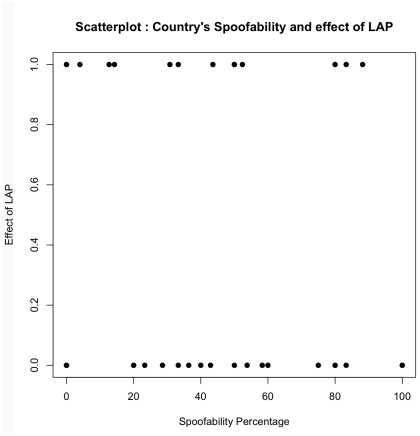

Figure 5: Scatterplot denoting relationship between country's spoofability percentages and being member of LAP. No clear correlation found.

4.5 To test the hypothesis, a scatterplot was casted to see if the country clearly, according to the scatterplot in figure 5, no clear relationship was seen in the spoofable percentages of the countries and the country being a member of the LAP organization. This proves that being a member of LAP and sharing the cybersecurity enforcements through LAP is definitely not making the impact of protection against Anti-Spoofing.

4.6 To prove the hypothesis and substantiate the correlations, we also ran the tests to find the oddsratio of countries having more than average spoofable prefixes and being a member of the LAP.

If,

A = Number of countries having more than Avg. Spoofable Prefixes and is a member of the LAP.

B = Number of countries not having more than Avg. Spoofable Prefixes and is a member of the LAP.

C = Number of countries having more than Avg. Spoofable Prefixes and not a member of the LAP.

D = Number of countries not having more than Avg. Spoofable Prefixes and not a member of LAP.

Then,

oddsratio can be calculated using R's function [14]

oddsratio(A,B,C,D,ConfidenceScore)

This gives us the p-value to reflect on the relationship between countries which are more prone to IP spoofing and them being members of LAP. Clearly, even the underperforming countries don't show a correlation with following the LAP enforcements.

p-value = 0.8874

```
> oddsratio(8,8,10,11,0.95)
           Disease Nondisease Total
Exposed          8         10    18
Nonexposed       8         11    19
Total           16         21    37

    Odds ratio estimate and its significance probability

data:  8 8 10 11
p-value = 0.8874
95 percent confidence interval:
 0.299355 4.042024
sample estimates:
[1] 1.1

>
```

5. RESULT OF ANALYSIS AND SOLUTION TO PROBLEM

Based on the above results it is clear that *Hypothesis H0 has proved to be false* and ***Hypothesis H1 is true***.

Having multiple actors involved in a security issue like network operators, country IT security board and ASes, 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.

The one we will focus in this paper 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, literature [8] shows that this method has been found to be highly effective in diminishing DDoS. New techniques like Unicast Reverse Path Forwarding, or uRPF which are preferred to use today or also the automation of Ingress Filtering implementation. Which are further explained below.

The prime decision makers, Network Providers 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:

5.1 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.

5.2 Strict Reverse Path Forwarding

It is conceptually identical to using access lists for ingress filtering, with the exception that the access list is dynamic.

5.3 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.

5.4 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).

5.5 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.

6. LIMITATIONS

The research produced in this paper has primarily focused on the trends in the data from the Spoofer application. Since the data is not very consistent, hence data cleaning has been done as in where required.

7. CONCLUSIONS

Based on the statistical analysis in section 4, it is clear that hypothesis H1 is true. Even though London Action Plan is highly reputed and is of a high potential organization to enforce cybersecurity standardization across the global IT networks. But, so far, being a member of the LAP and following its cybersecurity enforcements does not guarantee a country's network to perform any better against IP Spoofing.

Based on the literature study and experimental data from artifact sources, it is understood that the action items mentioned in section 5 would be the be best way to resolve the IP Spoofing problem.

8. REFERENCES

[1] History of Internet, https://en.wikipedia.org/wiki/History_of_the_Internet.

[2] "6.4 Billion Connected "Things" Will Be in Use in 2016" http://www.gartner.com/newsroom/id/3165317

[3] "SAVE: source address validity enforcement protocol" 07 November 2002: http://ieeexplore.ieee.org/document/1019407/?arnumber=1019407

[4] CAIDA's Spoofer Project: https://www.caida.org/projects/spoofer/

[5] "Understanding the Efficacy of Deployed Internet Source Address Validation Filtering" : ACM, Chicago, Illinois, USA — November 04 - 06, 2009

[6] ACM Conference: http://dl.acm.org/

[7] Robert Gezelter (1995) Security on the Internet Chapter 23 in Hutt, Bosworth, and Hoytt (1995) "Computer Security Handbook, Third Edition", Wiley, section 23.6(b), pp 23-12, et seq.

[8] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2267,DOI 10.17487/RFC2267, January 1998, http://www.rfc-editor.org/info/rfc2267

[9] The Spoofer Project: Inferring the Extent of Source Address Filtering on the Internet (SRUTI '05): http://static.usenix.org/legacy/events/sruti05/tech/full_papers/beverly/beverly_html/

[10] "MIDAS: An Impact Scale for DDoS attacks" - Rangarajan Vasudevan Z. Morley Mao Oliver Spatscheck Jacobus Van der Merwe: web.eecs.umich.edu/~zmao/Papers/midas.pdf : EECS

[11] "DDoS attacks: The impact": http://www.itp.net/591175-ddos-attacks-the-impact.

[12] IEEE-Explore : http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7310846&tag=1

[13] London action Plan: https://www.ucenet.org/who-we-are/

[14] Calculate odds ratio and its confidence intervals : http://minato.sip21c.org/msb/man/oddsratio.html