Economics of security
Assignment block 2 – Group 2

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

DRAFT

Introduction

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. CAIDA's aim is to improve the security and the stability of the global cyber environment, by conducting several projects of data monitoring and connectivity mapping. The results of these projects are then shared with governments and commercial organizations in order to take countermeasures to the vulnerabilities which may have strong impact towards creating a dependable global network.

One of these projects, called Spoofer, focuses on IP Spoofing vulnerabilities. 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[1]. As a collaborative project, the tester client is available to any end user, to maximise the coverage of the results.

Because the Internet forwards packets according to the IP destination address, packet forwarding typically takes place without inspection of the source address and malicious attacks have been launched using spoofed source addresses. IP Spoofing designates the alteration of the source address in IP packets, in order to fake the sender's identity.

This kind of attack can be used in the context of Denial of Service (DoS) attacks or Distributed Dos (DDoS) by sending data packets to a machine with the address of the victim. The receiver of the packets will then answer to the victim instead of the original sender. Scientists have been continuously putting their effort to enhance the Internet with OP source address validation techniques over IPV4 and IPV6.[2]

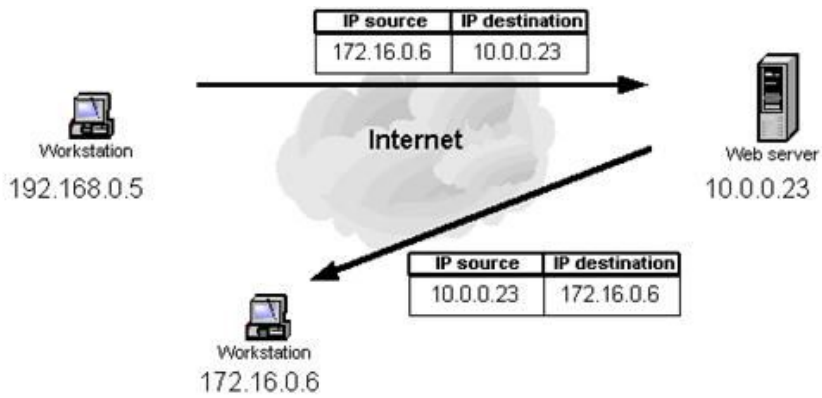

Figure 1 : Example of an IP Spoofing attack

[1] https://www.caida.org/projects/spoofer/

[2] A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience (https://tools.ietf.org/html/rfc5210)

Methodology

We are using the data provided by *Spoofer.*

The spoofer program attempts to send a series of spoofed UDP packets to servers distributed throughout the world. These packets are designed to test:

1. Different classes of spoofed IPv4 and IPv6 addresses, including private and routable
2. Ability to spoof neighboring, adjacent addresses (IPv4 only)
3. Where along the path filtering is observed (IPv4 only)
4. Presence of a NAT device along the path (IPv4 and IPv6)
5. Count of netblocks believed to prevent spoofing

We on other hand will analyse all above factors in the reports with other external reports and data found from different sources to verify the spoofer findings and in hope of finding some new relations or perspective of it.

For example, the basic idea is If country X has rated averagely safe in spoofer report but as per other reports country X sends majority of spoof attacks in the world, then there must be a factor that is hidden yer. So we tend to find such contradictions and as well as the reasons behind those, if possible. else it will be a model to verify the value of *spoofer's* findings.

Metrics

Since February 2005 until now , CAIDA collected all logs from all around the world which running the spoofer manager application. The following are some of the matrices which give a glimpse of what we can do from the given logs and results from Spoofer.

1. Spoofability

This graph plots the spoofability of prefixes, address space, and ASes over time. In order to compensate for the generally low rate of testing (and to prevent visual clutter), all tests since 6 months before the specified date are included in the spoofability calculation, and all the "inconsistent" prefixes, addresses, or ASes are considered to be "spoofable".

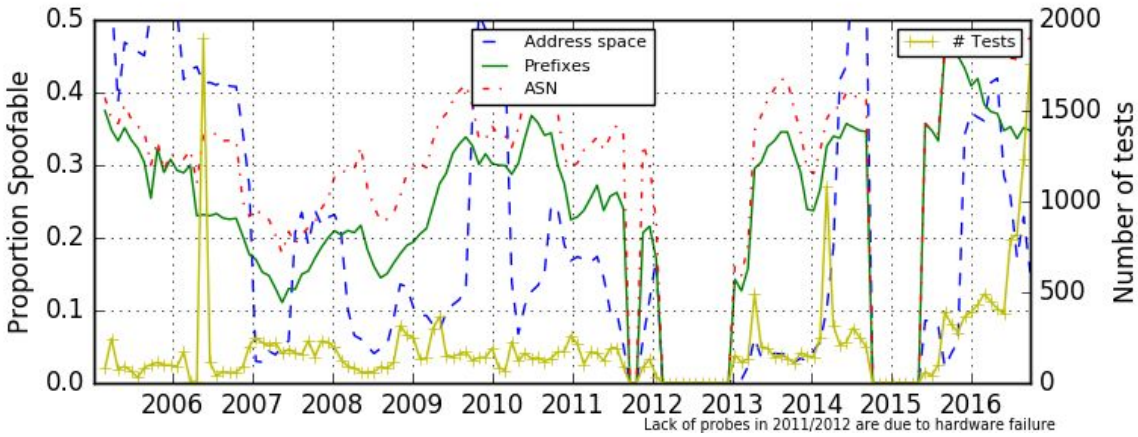

figure 2 : spoofing over time

2. Top 10 by ASN

The results are classified by Autonomous System and by country. The results for an AS can be provided to the concerned ISP so they can know if their network is secured against IP Spoofing. The results filtered by country are exploitable for the country CERT agency, which can then measure the effectiveness of the national ISP.

by ASN	Client Prefixes	Spoofing Prefixes
36352 (AS-COLOCROSSING)	74	22 (29.7%)
24560 (AIRTELBROADBAND-AS-AP)	58	18 (31.0%)
3269 (ASN-IBSNAZ)	49	16 (32.7%)
8551 (BEZEQ-INTERNATIONAL-AS)	20	14 (70.0%)
46573 (AS-GLobalf)	14	13 (92.9%)
51167 (CONTABO)	14	13 (92.9%)
17917 (QTLTELECOM-AS-AP)	14	12 (85.7%)
6830 (LGI-UPC)	66	11 (16.7%)
174 (COGENT-174)	21	11 (52.4%)
1267 (ASN-WIND)	23	11 (47.8%)

figure 3 : top ten spoofer test result by ASN

3. Top 10 by Country

Figure 4 is a list of top 10 countries on *Spoofer's* list based on the client prefixes of regions.

by Country	Client Prefixes	Spoofing Prefixes
usa (United States)	1981	476 (24.0%)
ind (India)	288	99 (34.4%)
gbr (United Kingdom)	245	59 (24.1%)
can (Canada)	225	55 (24.4%)
ita (Italy)	175	49 (28.0%)
deu (Germany)	223	45 (20.2%)
rus (Russian Federation)	119	38 (31.9%)
nld (Netherlands)	226	36 (15.9%)
aus (Australia)	107	34 (31.8%)
bra (Brazil)	112	31 (27.7%)

figure 4 : top ten spoofer test result by Country

We are in process of analyzing the data [3] from *Spoofer* and find the relationships and potential conclusions. We aim to find relative interlaces between the dataset from Spoofer and external resources.

[3] https://spoofer.caida.org/recent_tests.php