**Project Title:** The Prevalence of Source Address Validation to Protect Against IP Spoofing and DDoS Attacks

**Situation:**

How vulnerable is the Internet to different types of spoofed-source IP address attacks and what security measures can be implemented to protect against future attacks?

**Problem:**

When a host seeks to communicate with another host via the Internet, it sends data across the network in small units called packets with a source IP address and a destination IP address. The destination IP address is used to route the packet to the destination host and the source address is used so that the destination host can respond back to the source host. Unfortunately, there are two main ways in which a malicious user can exploit this system:

1. The attacker can flood a victim’s host with dubious packets so it can no longer process legitimate packets. The attacker accomplishes this by continuously sending packets with the destination addresses set to the victim’s host IP address and spoofing the source IP address with a random address so the attack cannot be traced back to its origins.
2. The attacker can employ a server called an amplifier to “amplify” the first attack by flooding the victim’s host with larger dubious packets from the amplifier. The attacker accomplishes this by continuously sending packets with the destination IP address of the amplifier and the spoofing the source IP address to the victim’s host IP address. Since the source IP address was spoofed to the victim’s host IP address, the amplifier responds by sending packets to the victim rather than the attacker.

These attacks are called a denial-of-service (DoS) attack because they result in the victim being denied the service to process legitimate packets. When an attacker employs many different sources to overwhelm the victim, it is called a distributed denial-of-service (DDoS) attack. These attacks can be mitigated through the use of source address validation (SAV). This involves setting up the edge router to drop outbound packets with a source IP address outside its network. Unfortunately, many networks do not sufficiently implement SAV due to incentive misalignment. Implementing SAV primarily benefits other networks since it blocks outbound packets with spoofed source IP addresses. However, it doesn’t protect the implementing network from receiving inbound packets with spoofed source IP addresses. Furthermore, it is difficult to measure the prevalence of SAV to identify vulnerabilities and rectify them.

**Motivation:**

The motivation behind this research is to increase our understanding of internet security by testing Internet provider’s use of robust source address validation security measures. Thus, we will identify vulnerabilities and provide solutions to address them.

**Purpose Statement (Goals):**

There are two primary goals for this research project.

1. Measure the vulnerability of the Internet to spoofed source IP address attacks such as DDoS.
2. Investigate security measures to protect against spoofed source IP address attacks.

**Methods/Approach:**

* Review relevant literature and related work. In particular, this will involve reviewing the use of loops observed in traceroute to infer the ability to spoof and using the tracefilter tool to locate SAV filters.
* Review statistics summary for the Spoofer project and identify trends and patterns in the frequency of successful source IP address spoofing compared to robust source address validation.
  + Evaluate statistics by autonomous system, country, and provider.
* Replicate previous work by using traceroute data from the Center for Applied Internet Data Analysis (CAIDA) on more recent data to infer current ability spoof.
* Document results by summarizing the current status of the Internet’s vulnerability to IP source address spoofing.
* Discuss future work that needs to be done in order to protect against IP source address spoofing.

**Resources:**

This project may use the following resources and software tools:

* **Spoofer**: Client tool that sends a spoofed UDP packets to dedicated servers to test the prevalence of effective source address validation.
* **Traceroute**: Client tool that has been used to infer ability to spoof in previous related work.
* **Wireshark**: Software tool that is used to analyze network traffic
* **Center for Applied Internet Data Analysis (CAIDA) IPv4 routed /24 topology dataset**: Dataset collected by CAIDA’s ongoing traceroute measurements for /24 prefix IP addresses
* **Scamper**: Traceroute tool used by CAIDA to collect data into wart files.
* **Pywarts**: Python library for parsing warts files output by Scamper.

**Milestones/Schedule:**

Below is the propose schedule displaying both base and active time schedule:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Milestone** | **Base Start** | **Base End** | **Actual Start** | **Actual End** |
| Review paper: “Using Loops Observed in Traceroute to Infer the Ability to Spoof” | 10/01/2019 | 10/11/2019 |  |  |
| Download CAIDA IPv4 routed data and parse it to find loops indicating ability to spoof | 10/03/2019 | 11/01/2019 |  |  |
| Document results from CAIDA data analysis | 10/11/2019 | 11/11/2019 |  |  |
| Review paper: “Tracefilter: A Tool for Locating Network Source Address Validation Filters” | 10/12/2019 | 11/23/2019 |  |  |
| Analyze data from Spoofer project and document most recent findings and trends | 10/15/2019 | 11/15/2019 |  |  |
| Write progress report | 11/01/2019 | 11/15/2019 |  |  |
| Propose solutions to identify vulnerabilities such as insufficient SAV and mitigate them | 11/16/2019 | 11/20/2019 |  |  |
| Test proposed solutions and discuss future work | 11/20/2019 | 12/01/2019 |  |  |
| Write final report | 12/01/2019 | 12/16/2019 |  |  |