The Prevalence of Source Address Validation to Protect Against IP Spoofing and DoS Attacks

Jeffrey McCullen   
 Computer Science  
 Virginia Tech  
mccullen@vt.edu

ABSTRACT

…

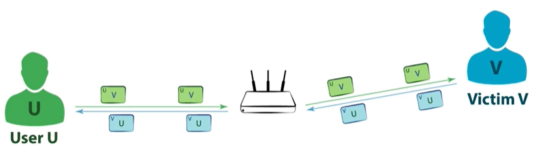
KEYWORDS

Data mining, data analytics, source address validation, ip spoofing, DoS attack, computer networks, traceroute, spoofer

**1. Problem Motivation and Design Goals**

The specific problem we are addressing through this research is the lack of understanding on the vulnerability of the Internet to different types of spoofed-source IP address attacks. Our goal is increase this understanding in order to investigate the deployment security measures such as source address validation to protect against future attacks.

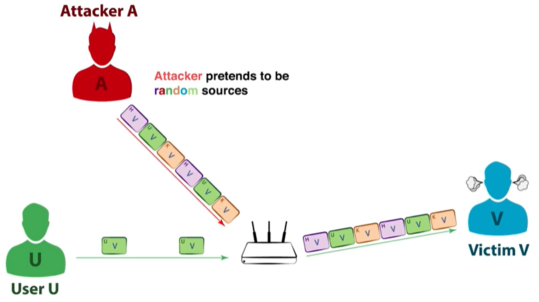
These attacks occur when a malicious user exploits the communication protocol between host machines. When a host seeks to communicate with another host via the Internet, it sends data across the network in small units called packets. Each packet contains headers with the source IP address and destination IP address. Routers use the destination IP address to route the packet to the destination host. After the packet arrives at the destination host, the destination host uses the source IP address to respond to the source host. See figure 1.1 for an illustration of this process.



**Figure 1.1: Figure from [] showing the normal process of communication between hosts. The user’s host sends data across the network to the victim in packets with the source address set to U and the destination address set to V. The router uses the destination address to route the packet to the victim. The victim’s host uses the source IP address of these packets (U) to respond by sending packets across the network in a similar manner.**

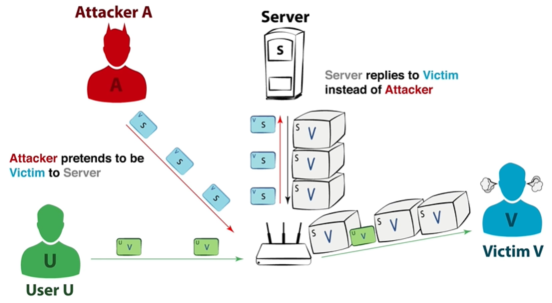
Unfortunately, a malicious user can exploit this system in two main ways:

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 IP addresses set to the victim’s host IP address and the source IP address set to a random address. Setting the source IP address to a random address makes it difficult for the victim to trace the attack back to its origins. IP address spoofing refers to this process of using a fake source IP address, usually with malicious intent. See figure 1.2 for an illustration of this process.



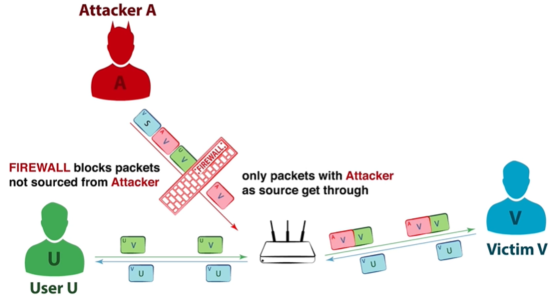
**Figure 1.2: Figure from [] showing how an attacker can overwhelm a victim’s host with dubious packets and use source IP address spoofing to make it difficult to trace the attack back to the attacker.**

1. 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 attacker spoofed the source IP address to the victim’s host IP address, the amplifier responds by sending packets to the victim rather than the attacker. See figure 1.3 for an illustration of this process.



**Figure 1.3: Figure from [] showing how a use an amplifier to “amplify” the attack. Instead of sending packets directly to the victim, the attacker sends packets to an amplifier server (S). The attacker spoofs the source IP address to the victim’s IP address so the amplifier will respond to the victim instead of the attacker.**

We refer to these attacks as a denial-of-service (DoS) attack because they result in the attacker denying the victim the service to process legitimate packets. When an attacker employs many different sources to overwhelm the victim, we call it a distributed denial-of-service (DDoS) attack. We can mitigate these attacks using source address validation (SAV). This involves setting up the edge router to drop outbound packets with a source IP address outside its network. See figure 1.4 for an illustration of SAV.



**Figure 1.4: Figure from [] showing how a router can use a firewall to implement SAV. The edge router uses a firewall to drop outbound packets with a source IP address outside its network. Thus, the edge router prevents the attacker from spoofing IP addresses and carrying out a DoS attack.**

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 does not 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.

Thus, the motivation behind this research is to increase our understanding of internet security by testing the extent to which autonomous systems use robust SAV security measures. We will identify the prevalence of vulnerabilities and provide solutions to address them. Specifically, there are two primary design 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

**2. Approach**

To achieve these goals, we used a multistep research pipeline involving numerous resources and software tools. This pipeline included steps for reviewing relevant literature, replicating previous work, documenting results, and discussing future work.

Our research pipeline began with reviewing the relevant literature and related work to inform the subsequent steps. . In particular, this involved reviewing the use of loops observed in traceroute to infer the ability to spoof and using the tracefilter tool to locate SAV filters. Additionally, we reviewed the statistics summary for the Spoofer project and identified trends and patterns in the frequency of successful source IP address spoofing and compared it to robust source address validation. We evaluated these statistics by autonomous system, country, and Internet provider. We replicate previous work by using traceroute data from the Center for Applied Internet Data Analysis (CAIDA) on recent data to infer current ability spoof. Subsequentally, we document the results of our analysis and replication by summarizing the current status of the Internet’s vulnerability to IP source address spoofing. Finally, we discuss future work that is necessary to protect against IP source address spoofing. See the subsequent sections for a more detailed description of each step.

Resourrces :

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.

**3. Relevant Literature**

…

**3. Evaluation Results**

…

**4. Conclusion and Future Work**

…

**ACKNOWLEDGEMENTS**

…

REFERENCES

[1] Rajkomar, A. et al. 2018. Scalable and accurate deep learning with electronic health records. *Nature Partner Journals*