Garrett Kalter, Cade Smith, Lucca Figlioli, and James Burke

Aaron Gember-Jacobson

COCS465A Computer Networks

March 27, 2024

Address Validation Study Reproduction

1. Objective and Motivation

This project aims to reproduce the results found in the paper "Don't Forget to Lock the Front Door! Inferring the Deployment of Source Address Validation of Inbound Traffic". Specifically, Table 3 in the article which shows geo-location results and their vulnerability to spoofing.

The purpose of this paper was to address the issue of IP spoofing and the lack of inbound packet

Table 3. Geolocation results

Rank	Country	Resolvers (#)	Country	Vulnerable to spoofing /24 networks (#)	Country	Vulnerable to spoofing /24 networks (%)
1	China	2 304 601	China	271 160	Cocos Islands	100.0
2	Brazil	687 564	USA	157 978	Kosovo	81.82
3	USA	678 837	Russia	55 107	Comoros	57.89
4	Iran	373 548	Italy	32 970	Armenia	52.16
5	India	348 076	Brazil	29 603	Western Sahara	50.00
6	Algeria	252 794	Japan	28 660	Christmas Island	50.00
7	Indonesia	249 968	India	27 705	Maldives	39.13
8	Russia	229 475	Mexico	24 195	Moldova	38.66
9	Italy	108 806	UK	18 576	Morocco	37.85
10	Argentina	103 449	Morocco	18 135	Uzbekistan	36.17

filtering in network infrastructures. IP spoofing is where the source IP address in packet headers is falsified, and in turn poses a significant security threat as it enables attackers to hide their identity and launch cyberattacks, such as Distributed Denial-of-Service (DDoS) attacks and cache poisoning attacks (Korczynski et al., 2020).

2. Prior Artifacts

The main article we are using as a baseline for this project is the paper by Korczynski et al. (2020) which tests spoofability of all available /24 BGP prefixes available. This is done using a scanner and recursive resolver as shown in Figure 1. The data Korczynski used for the project was from BGP

prefixes maintained by RouteViews. The results the authors obtained were then compared to similar studies and results from other spoofers, such as the Spoofer project (CAIDA, 2020). The methodology we intend to reproduce, which was used by the authors of the paper is described by Mauch (2013) and shown in Figure 1.

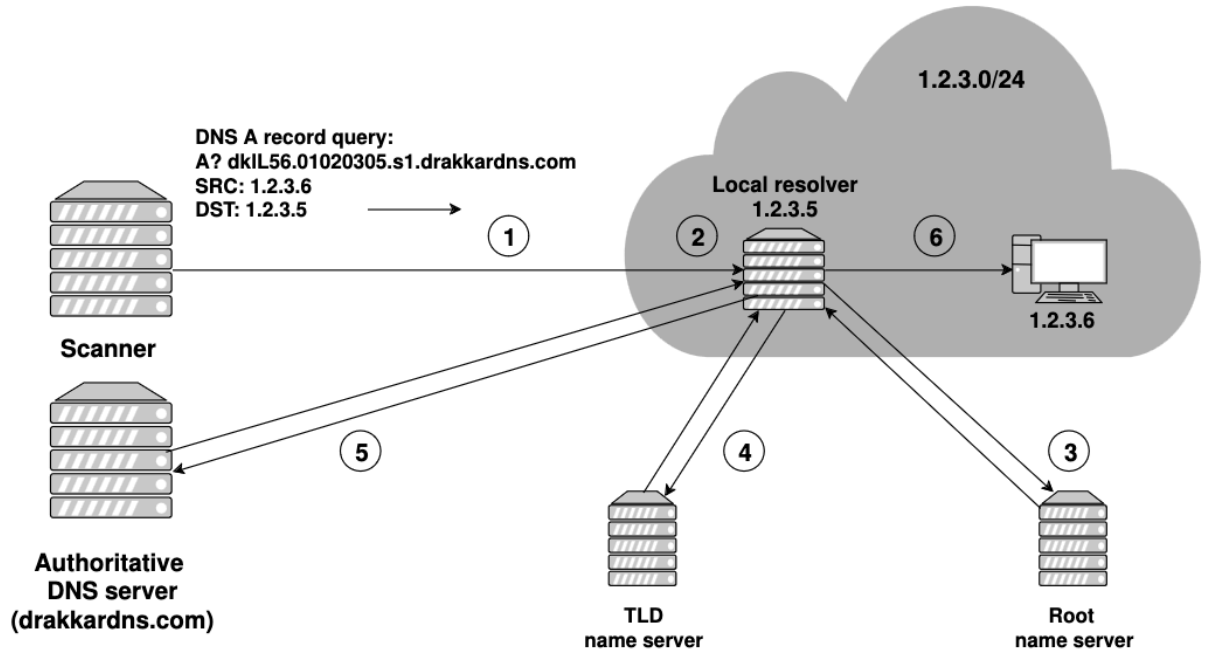

Fig. 1. Inbound spoofing scan setup.

3. Project Plan

To reproduce the Korczynski study we will start by setting up an authoritative DNS server to capture traffic and data. Then, we will confirm that our upstream providers do not implement Source Address Validation (SAV). Next, we will deploy a VM without outbound SAV. After that, we'll obtain or create a spoofer tool capable of generating packets with spoofed source addresses. Finally, this tool will be used to send spoofed packets to hosts within a network, each requesting A records for random subdomains of our authoritative DNS server. This process will help assess network behavior for potential vulnerabilities or misconfigurations

4. Artifacts to Deliver

Drawing from the paper, there are two artifacts that we would be able to deliver. These two artifacts are Table 3, as shown above, which shows geographic locational results of spoofability. The second artifact is Table 2 which shows the overall results of the Spoofing scan. These are the current artifacts we intend to reproduce and deliver - however, more may arise as we get further into the project.

Table 2. Spoofing scan results

Metric	Number	Proportion (%)
DNS forwarders	6 530 799	94.01
Open resolvers	2 317 607	35.49
Closed resolvers	4 213 192	64.51
DNS non-forwarders	415 983	5.99
Open resolvers	39 924	9.6
Closed resolvers	376 059	90.4
Vulnerable to spoofing /24 IPv4 networks	959 666	8.62
Vulnerable to spoofing longest matching prefixes	197 641	23.61
Vulnerable to spoofing autonomous systems	32 673	49.34

Bibliography

Korczyński, M., Nosyk, Y., Lone, Q., Skwarek, M., Jonglez, B., & Duda, A. (2020). Don't forget to lock the front door! Inferring the deployment of source address validation of inbound traffic. In A. Sperotto, A. Dainotti, & B. Stiller (Eds.), *Passive and Active Measurement* (pp. 107–121). Springer International Publishing. https://doi.org/10.1007/978-3-030-44081-7_7

Nanog: Re: spoofing asns(Re: SNMP DDoS: the vulnerability you might not know you have). (n.d.). Retrieved March 27, 2024, from https://seclists.org/nanog/2013/Aug/132

Routeviews – university of oregon routeviews project. (2024, January 19). https://www.routeviews.org/routeviews/

Spoofer. (2020, October 15). CAIDA. https://www.caida.org/projects/spoofer/