ATHENE
National Research Center for Applied Cybersecurity

Stealth BGP Hijacks with uRPF Filtering

Authors
Haya Schulmann and Shujie Zhao

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Fraunhofer SIT

TECHNISCHE UNIVERSITÄT DARMSTADT

Agenda

1. Introduction
2. Background
3. Attack Model
4. Evaluation
5. Results
6. Limitations, Challenges, and Countermeasures
7. Conclusions

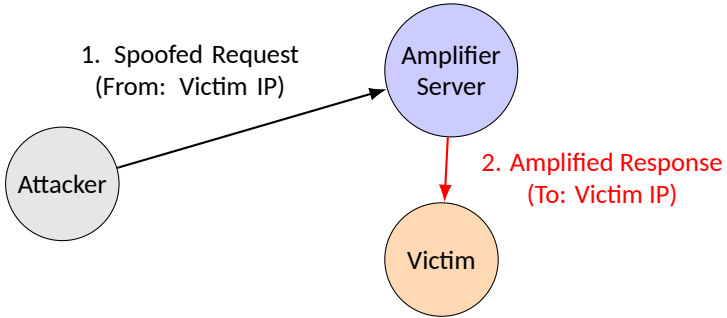
Introduction

- **IP spoofing remains a major security threat**
  - Used in Denial of Service, reflection/amplification, and bypass attacks
- **Unicast Reverse Path Forwarding (uRPF) is a primary mechanism to defend against IP spoofing**
  - Validates source IP addresses in incoming packets based on routing tables
- **But: uRPF is not robust, can be exploited by adversaries to carry out DoS attacks**
  - Exploitable via BGP prefix hijacks
- **Our contribution: SBA-uRPF attack model**
  - Adversaries utilize prefix hijacks to influence the uRPF behavior to block legitimate traffic
- **Impact:** Potential to disrupt thousands of networks

Background: IP Spoofing

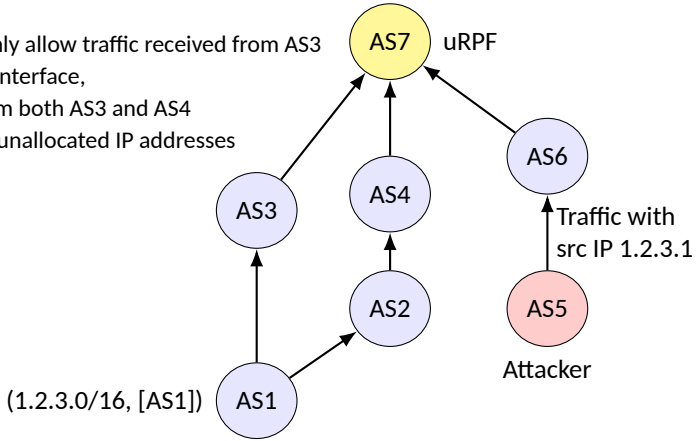
Example: DoS Amplification Attack

- The source address is specified in the IP layer header of packets to identify the origin
- But, the IP protocol lacks built-in authentication mechanisms
- Attackers can manipulate packets to appear as if they originated from another source, a technique referred to as IP spoofing



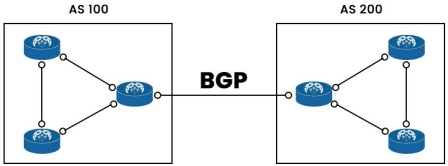
Background: Unicast Reverse Path Forwarding (uRPF)

- uRPF verifies incoming packet source via routing (forwarding) tables; checks if it can forward packets to the source through the interface
- Three common modes
  - Strict: same interface, only allow traffic received from AS3
  - Feasible-path: available interface, allow traffic received from both AS3 and AS4
  - Loose: against bogon or unallocated IP addresses



Background: Border Gateway Protocol (BGP)

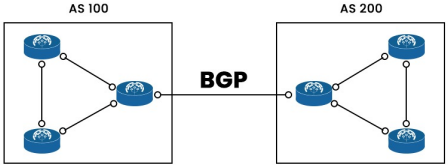
- BGP routers exchange reachability information across Autonomous Systems (ASes) using BGP;
  E.g., AS100 announces a route for its prefix 1.2.3.0/24 to AS200: (1.2.3.0/24, [AS100])
- BGP relationships: BGP customers (pay providers for traffic transfer), peers (exchange traffic for free), and providers (provide transfer service for customers)



https://www.pynetlabs.com/bgp-in-computer-networks/

Background: Border Gateway Protocol (BGP)

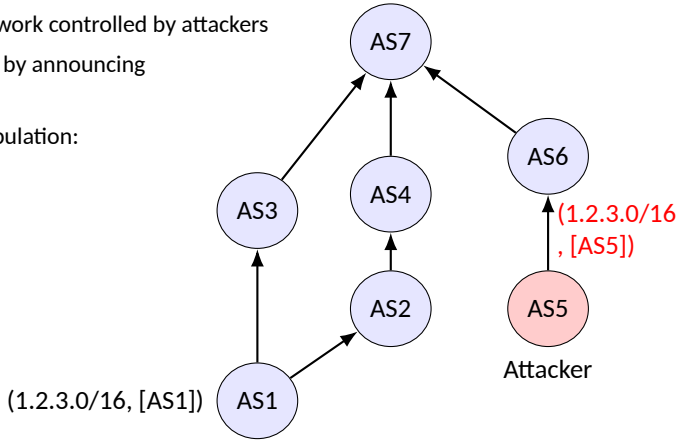
- Valley-free routing policy: An AS is not allowed to forward routes learned from its provider or peer to another provider or peer
- Route preference: Upon receiving BGP routes for the same prefix, routers select the best one for forwarding; e.g., based on Local preference: customers > peers > providers
- Routing loop prevention: ASes will discard a BGP announcement if they detect their own AS numbers in the AS path



https://www.pynetlabs.com/bgp-in-computer-networks/

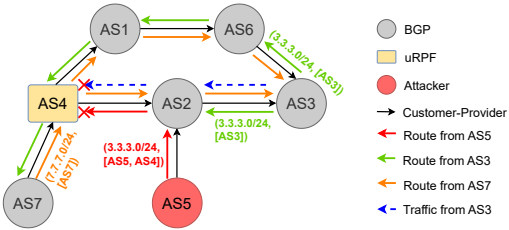
Background: Prefix Hijacks

- Prefix hijacks occur when an AS originates a BGP route for a prefix that belongs to another AS
- Redirecting the traffic to the network controlled by attackers
- E.g., AS5 launches a prefix hijack by announcing the prefix owned by AS1
- Prefix hijacks with AS path manipulation: (1.2.3.0/16, [AS5, AS1])



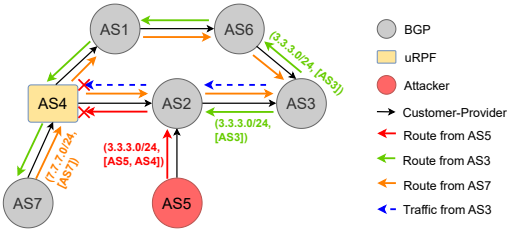
Novel Attack Model: SBA-uRPF

- **S**tealthy **B**GP **a**ttack abusing **uRPF**
- AS4 deploys uRPF; an attacker within network AS5 originates a BGP route for the prefix 3.3.3.0/24, which belongs to AS3, and appends AS4 to the end of the AS path
- AS5 is a customer of AS2, while AS3 is a provider or a peer of AS2
- Based on local preference, AS2 selects and forwards the route from AS5 to AS4
- However, AS4 drops this route to avoid routing loops
- Packets with source IP addresses within the prefix 3.3.3.0/24 can not be accepted on the interface connected to AS2
- We refer to AS2 as the “bridging network”



Novel Attack Model: SBA-uRPF

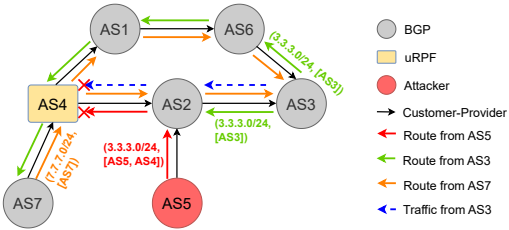
- **S**tealthy **B**GP **a**ttack abuses **uRPF**
- AS7 is a customer of AS4 and orignates a route for its prefix 7.7.7.0/24
- Two potential paths to AS3: [AS4, AS2, AS3] and [AS4, AS1, AS6, AS3]
- Since AS3 is AS2's provider or peer, to enable the route forwarding to AS3, AS4 must be a customer of AS2 (valley-free policy)
- AS3 selects the best route [AS2, AS4, AS7] to forward the traffic with a source IP from 3.3.3.0/24 to AS7
- As a result, the traffic is discarded by uRPF within AS4



Novel Attack Model: SBA-uRPF

The attack possesses the following major properties:

- **Targeted:** specifically tailored to each uRPF-enabled network (by triggering routing loop prevention)
- **Stealthy:** hidden from the uRPF-enabled network as well as its downstream customer networks (such as AS4 and AS7)
- **DoS:** leads to Denial-of-Service (DoS) by causing legitimate traffic drops



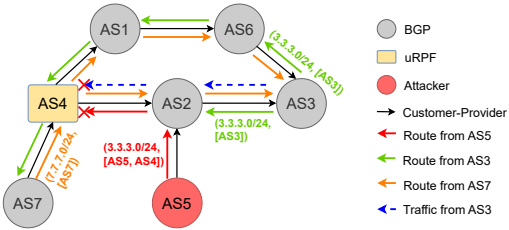
Evaluation Methodology

- We identify uRPF-enabled networks that are vulnerable to SBA-uRPF attacks.
- We assess the vulnerability using a simulator built upon CAIDA AS topology data, including 77K ASes (65K stub or multihomed, 12K transit, and 19 tier-1 networks)
- We assume that all of ASes deploy uRPF on the simulator to conduct a theoretical evaluation

Evaluation

Steps to Identify a Vulnerable uRPF-Enabled Network:

- Select a uRPF-enabled network to evaluate (e.g., AS4)
- For each of its providers, check if it can act as a bridging network (e.g., AS2):
  - Has a customer exploitable by attackers
  - Has a provider or peer that could be a victim
- Simulate a route announcement from the uRPF network (e.g., 4.4.4.0/24)
- Check if any potential victim sees the best route via the bridging network
- If such a bridging network exists, the uRPF network is vulnerable to SBA-uRPF



Results

Our analysis is based on a simulation with universal uRPF deployment assumption. The main results are:

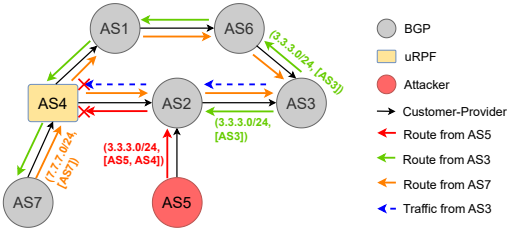
- 99.3% (76,953) of networks across the Internet could be vulnerable to SBA-uRPF attacks
- Vulnerable transit networks exhibit larger numbers of attack scenarios (different pairs of attacker and victim networks), resulting in a total of 1.7M potential attacks
- In the worst-case scenario, up to 59K networks (76.3%) could be affected
- No Tier-1 networks are vulnerable (no providers act as bridging networks)

	Tier-1	Transit	Edge
Vulnerable	0	12,045	64,908
Attacks	0	1,781,854	818,355
Impact (mean)	0	1,141	1
Impact (maximum)	0	59,115	1

Table: Simulation statistics across different types of networks.

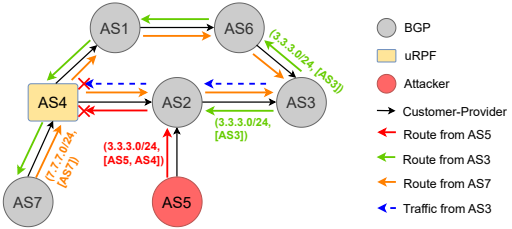
Limitations and Challenges

- **Theoretical analysis:** Assumes universal uRPF deployment
- **Upper bound:** Real networks use complex policies; they may use BGP communities to adjust local preferences and control route export behavior; SBA-uRPF may not apply to these cases
- **Traffic load:** Attackers receive unwanted redirected traffic
- **Reduced stealth:** Hijacks may be detected by global BGP monitoring systems



Countermeasures

- ASes such as AS2 deploy mechanisms that defend against AS path manipulation, e.g., BGPsec: path validation prevents AS path manipulation), ASPA (AS Provider Authorization): validates provider-customer relationships
- AS2 deploys Route Origin Validation (ROV) to filter out bogus routes



Conclusions

- We introduce a new attack model that exploits prefix hijacks to manipulate uRPF behavior to cause the dropping of legitimate traffic
- SBA-uRPF attacks remain undetectable to affected networks; can cause long-term service disruption; can target critical Internet infrastructure such as DNS, NTP, web servers
- Our theoretical evaluation shows that 99.3% of networks are vulnerable to SBA-uRPF, with a potential maximum impact affecting over 76.3% of networks
- Finally, our findings reveal a troubling paradox: in the case of uRPF, protection can be turned into a weapon by attackers.

Questions?

Thank you for your attention!