The Spoofer Project

Rob Beverly
<rbeverly@mit.edu>
MIT CSAIL

March 30, 2005

Spoofer Project Background

- High-profile spoofing-based DDoS attacks in 2000, 2001
- Does spoofing really matter in 2005?
  - All ISP filter, right?
  - Zombie Farms
  - NAT Rewriting
- But:
  - Reflector attacks
  - Backscatter shows continued spoofing

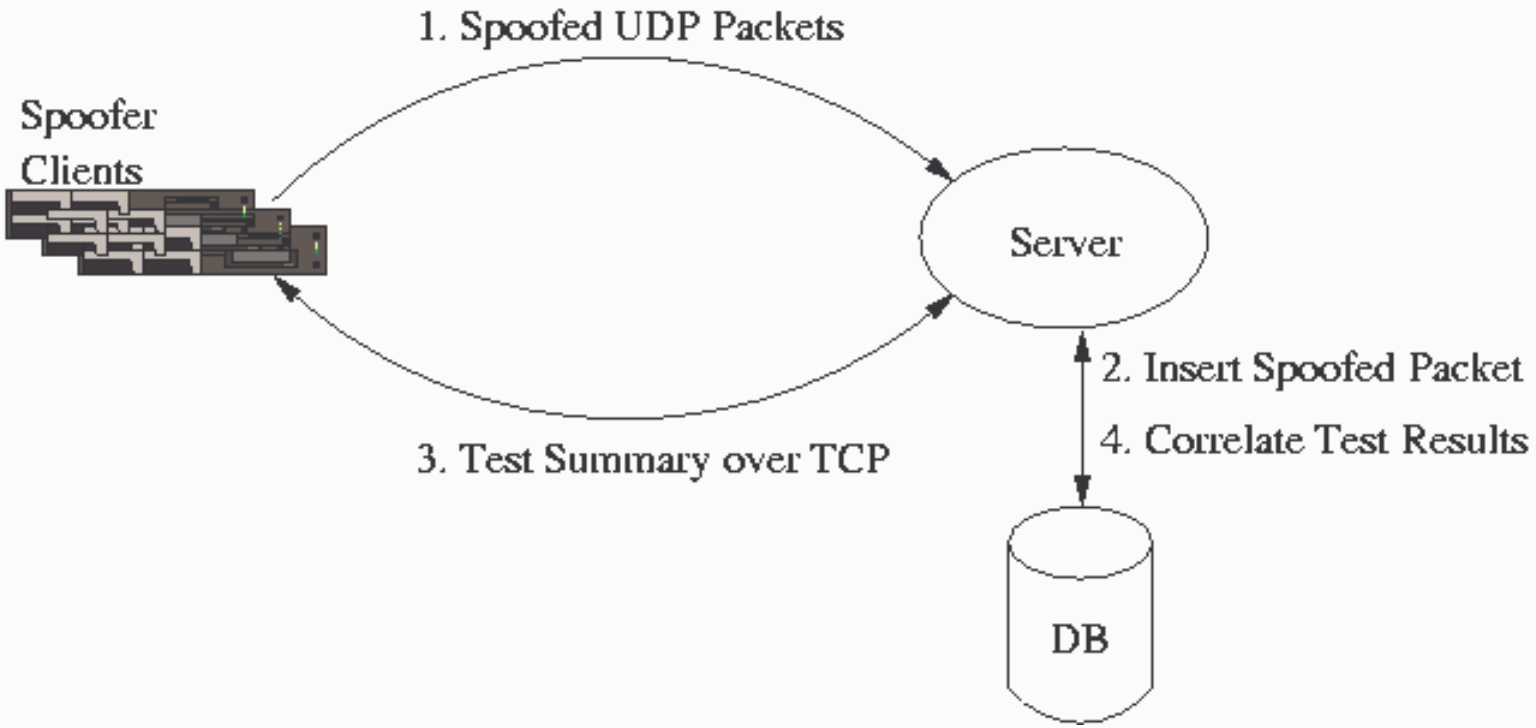
Spoofer Project

- http://momo.lcs.mit.edu/spoofer
- Active measurement project
- Clients run our program (binaries, source)
- Availability advertised to e.g. NANOG mailing list, etc

Spoofer Project

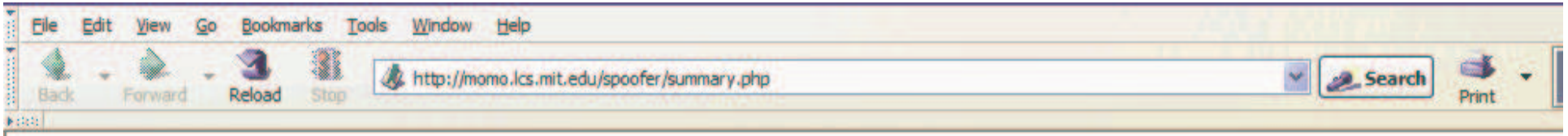
- Send series of spoofed UDP packets to server on campus
  - Five of each with random inter-packet delay
  - Payload includes unique 14 byte identifier
  - If received, packets stored in DB
- Send TCP report of spoofed packets to server
- Send traceroute to server
- Use UDP port 53, TCP port 80 to avoid secondary filtering effects

Spoofer Operation



Spoofed Packets

Spoofed Source	**Description**
1.2.3.4	Bogon (Not in BGP table)
6.1.2.3	Valid (In BGP table)
172.16.1.100	Martian (RFC1918 private address)
IP $\oplus$ (2^N) for 31>N>8	Neighbor Spoof



The Spoofer Project: State of IP Spoofing

This report, provided by MIT ANA, intends to provide a current aggregate view of ingress and egress filtering and "Spoofing" on the Internet. While the data in this report is the most comprehensive of its type we are aware of, it is still an ongoing, incomplete project. The data here is representative *only* of the netblocks, addresses and autonomous systems (ASes) of clients from which we have received reports. For this reason, we present data both in terms of what we've observed as well as globally routeable space. The more client reports we receive the better - they increase our accuracy and coverage. Test your own system and network connection and read more about the project on the Spoofer Project Page. This page is regenerated hourly.

Summary:

Current as of: Wed Mar 30 12:21:02 EST 2005

Reports: 346

Spoofing Coverage			
Metric	Spoofable	Believed Unspoofable	Estimated Global Spoofability
Netblocks	55	184	38,861
IP Addresses	3,611,904	49,338,880	108,749,639
ASes	36	113	4,351

Relative Spoofing Coverage		
Metric	Spoofable (% Observed)	Spoofable (% Globally Routable)
Netblocks	23.0%	0.0%
IP Addresses	6.8%	0.2%
ASes	24.2%	0.2%

Details:

Failed Spoofs:

Failed Spoofs: 228
Blocked by Operating System: 16
Blocked by Windows XP SP2: 82
Hosts unable to Spoof Neighbor's Address (IP + 1): 2
Hosts Behind NATs: 92

Successful Spoofs:

Legitimate Spoofs: 61

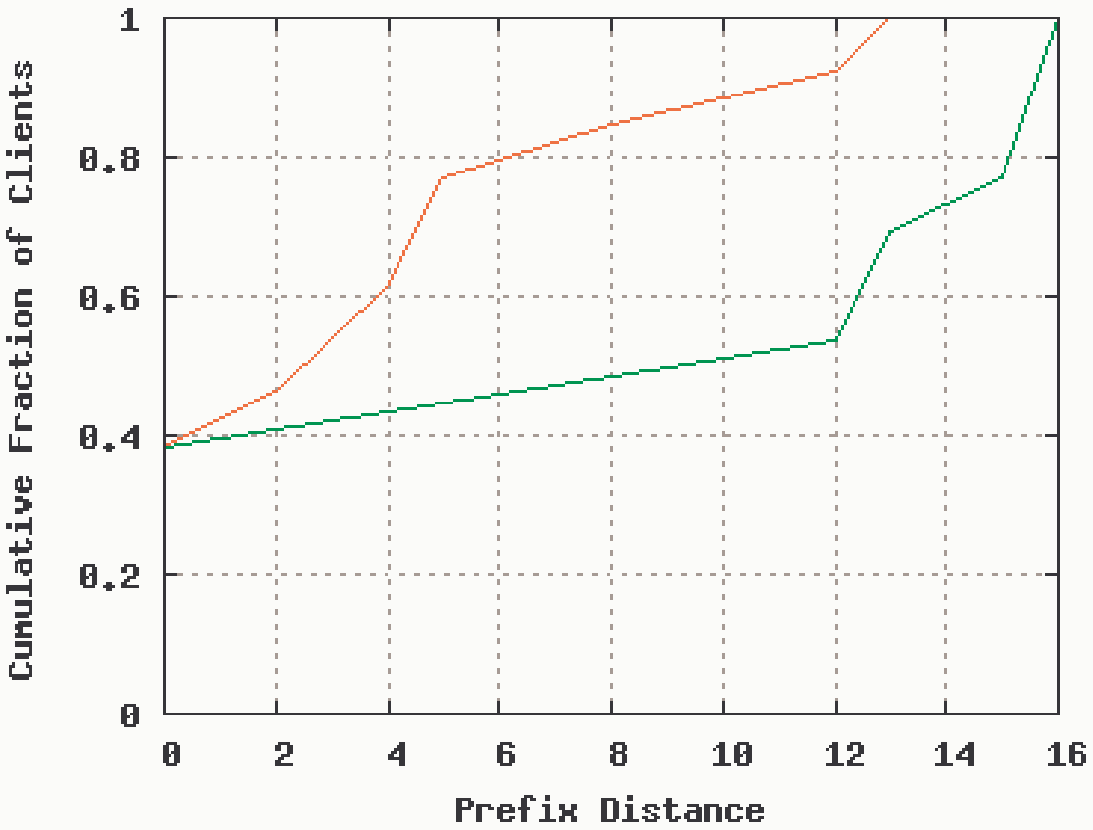
IP Space Coverage (based on routeviews BGP view):

Frequency of Inconsistent Filtering

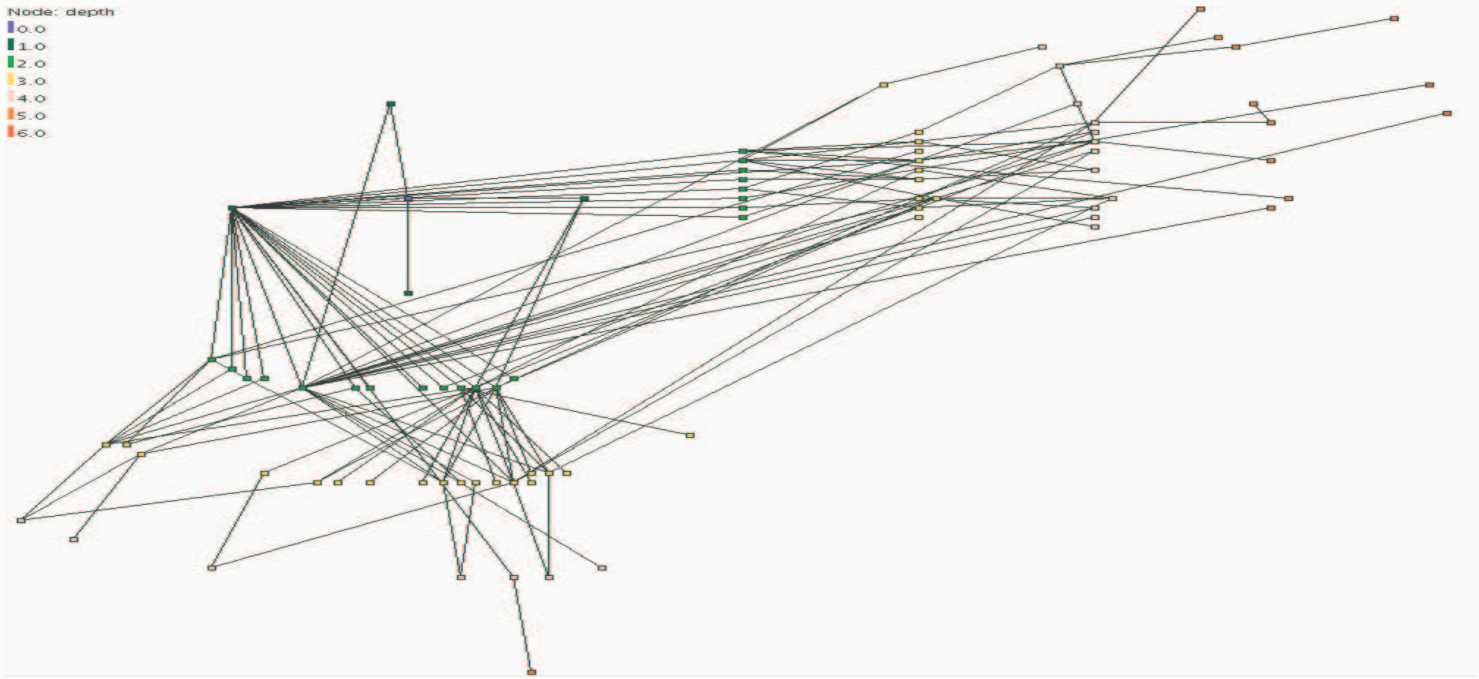
RFC1918	Bogon	Valid	Count
-	-	X	17
-	X	-	0
-	X	X	39
X	-	-	0
X	-	X	0
X	X	-	0

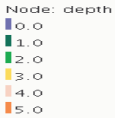
Example: providers that automate filtering by only forwarding packets sourced with valid address (in BGP table)

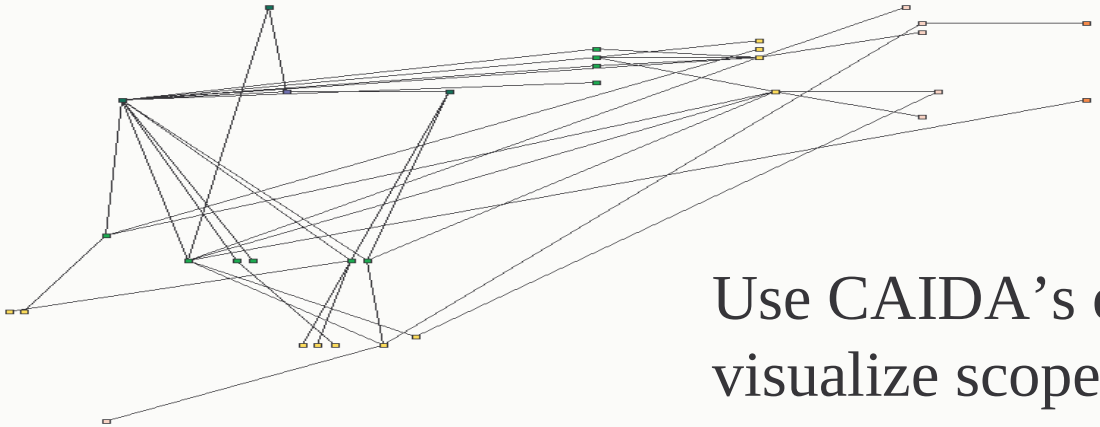
Filtering Granularity



How consistent are inferred filtering boundaries with advertised BGP prefixes?







Use CAIDA’s otter to visualize scope of spoofing