PowerDNS Recursor: The Most Advanced Way To Resolve Domain Names

Scope

- Very short introduction of PowerDNS & Recursor
- Short update on progress over past year
  - Use figures
  - Performance improvements
- DNS Security
- Counter-measures
- Future developments

Very short introduction

- PowerDNS launched in 2000, closed source (lots of .COM fun)
- Open Source (GPL) since 2002 or so
- Database & Zone powered Authoritative Server
- Since 2003, Innovative Recursor, as a separate product
- Recursor has Auth features, Auth server can proxy to Recursor

Update on Recursor

- Was “promising” 12 months ago
- XS4ALL sponsored transition from “Promising” to “Useful”
  - Thanks!
- Wrote “dnsreplay” and “dnsstat” to replay PCAP dumps and analyse them for performance
- Recursor is now exclusive nameserver for at least 40 million internet connections
  - That we know of!

Big Recursor users we can mention

- XS4ALL (mix)
  - influential in getting product ready
- Shaw Cable
- Neuf Cegetel
  - Acquired AOL France recently
- Freenet.de (“mcbone”)

These ISPs all provided very valuable feedback and debugging!

New since last time

- Source port randomisation
  - draft-hubert-dns-anti-spoofing-00.txt
- Query chaining
  - “anti-birthday effect”
- Permanent LRU cache cleaning
- SMP support
- “Rec_control” runtime support
  - cache purging
- Supports almost the same broken domains as BIND

Validation tools

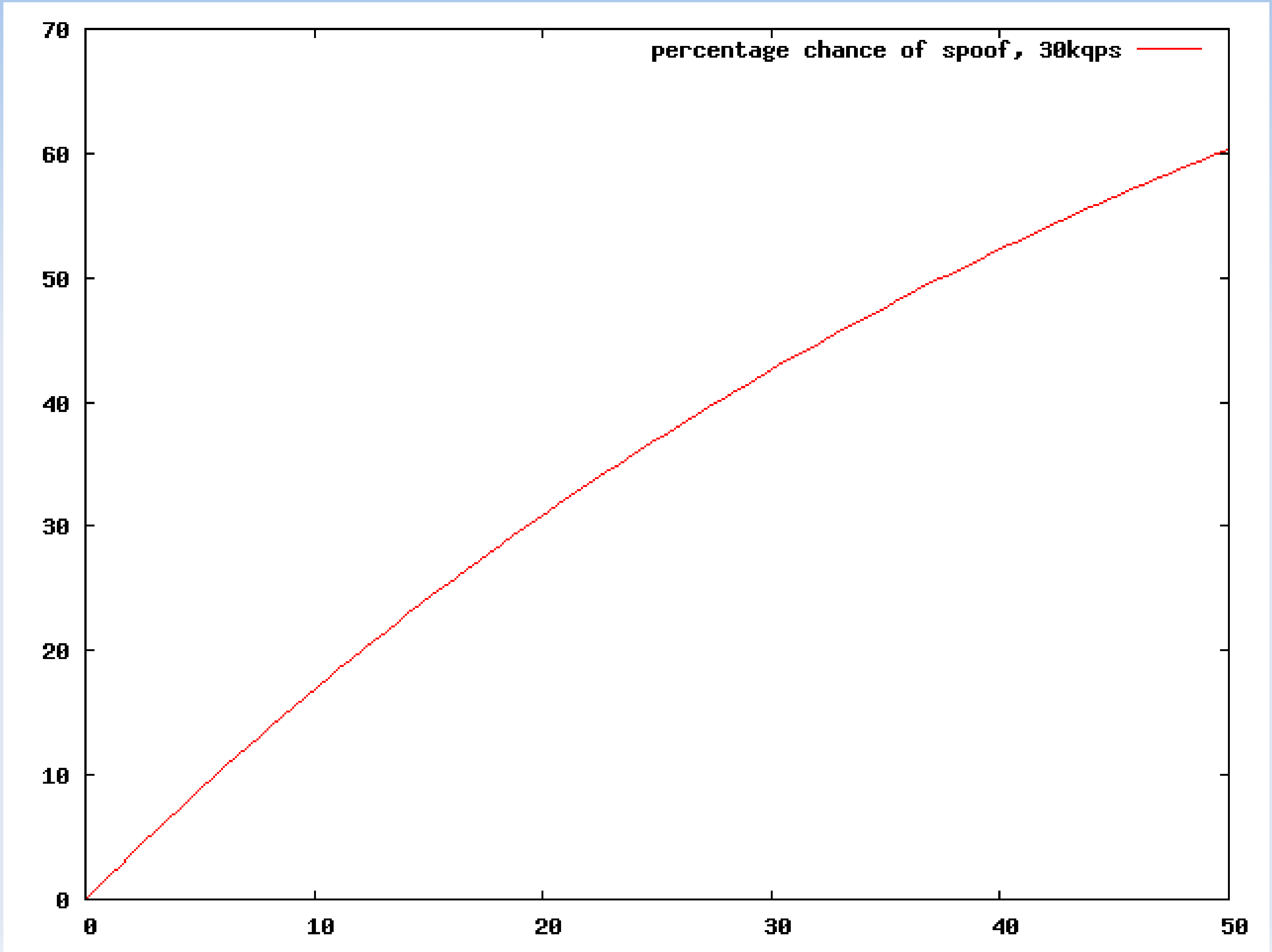
- Migrations make people nervous
- DNS at the core of, well, everything
  - except BGP
- So: tcpdump your current resolver
- examine using “dnsscope”
  - teh horror!
  - response times, drops, servfails
- replay to PowerDNS using dnsreplay

Some bold statements

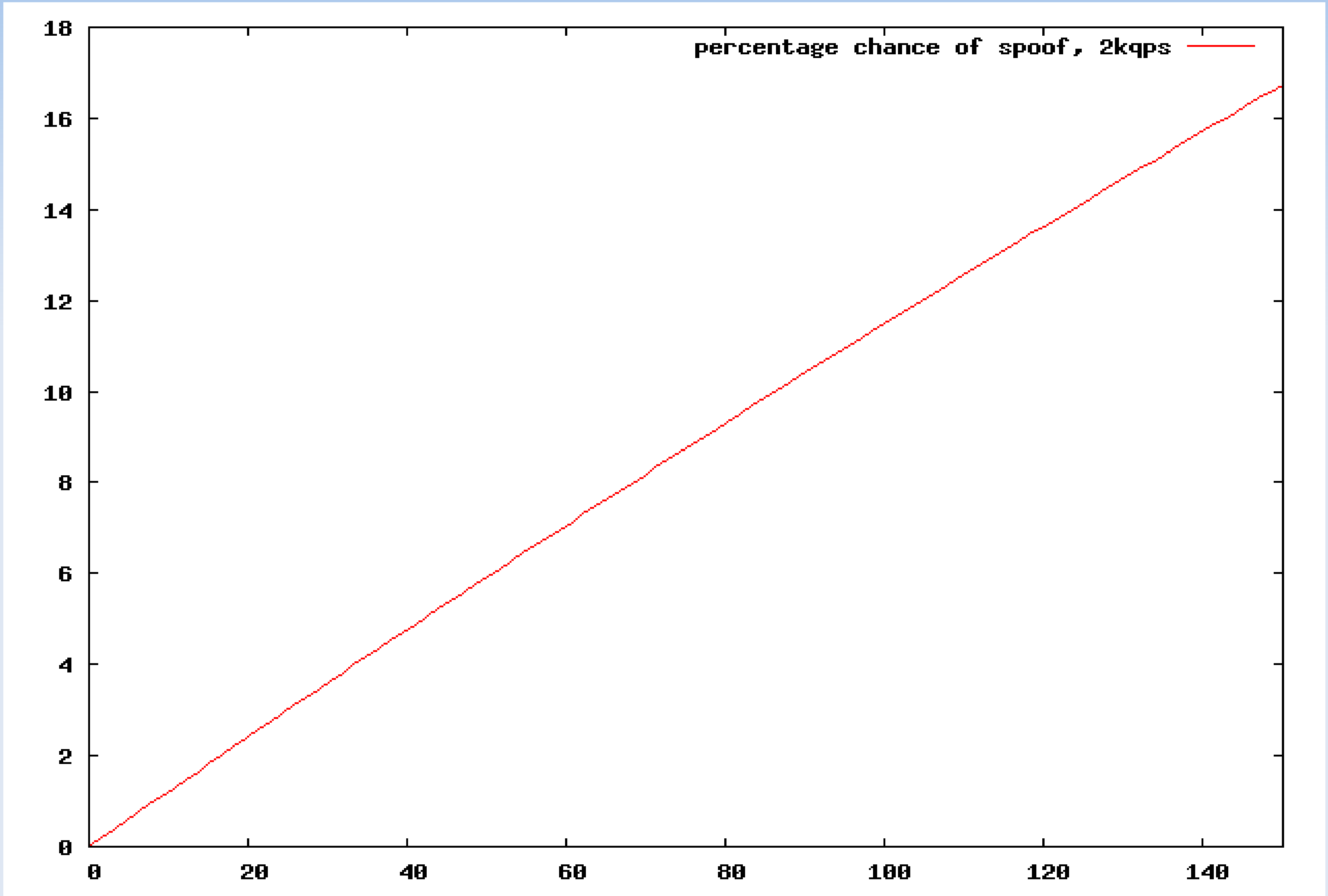
- This is about a well known nameserver
- You probably use it

> an attacker sending 7000 fake answer packets/s (a rate of 4.5Mb/s), stands a 10% chance of spoofing a record in the first 24 hours, which rises to 50% after a week.
>
> For a domain with a TTL of 60 seconds, the 10% level is hit after 24 minutes, **50% after less than 3 hours**, 90% after around 9 hours.

A graph


percentage chance of spoof, 30kqps
70
60
50
40
30
20
10
0
0
10
20
30
40
50

Another graph



Not good!

- Some nameservers do even worse!
  - Microsoft resolver
    - nobody uses it though
- Safe choices: dnscache, PowerDNS
- Unsafe: all versions of BIND
- And, it appears, the Nominum CNS
  - hard to know, everything under NDA
-