The recursive DNS rant

@ UKNOF 15

Boyan Krosnov

Security

- Dan Kaminsky’s “Multiple DNS implementations vulnerable to cache poisoning” – 2008-07

www.flickr.com/photos/alexsemenzato/

- We’ve known this for a long time
- DNSSEC is the solution, but until then…

RFC5452 – 2009-01

“Measures for Making DNS More Resilient against Forged Answers “

- Query Matching rules
- Extending the Q-ID space using ports and addresses
- Spoof detection and countermeasures

Did you implement any of this?

IETF Drafts

draft-vixie-dnsext-dns0x20-00.pdf – 2008-03

- wWw.GoOgle.cOm anyone ?

draft-barwood-dnsext-fr-resolver-mitigations-08 – 2008-10

- Query repetition
- 0x20
- Random source port
- Random nonce prepending
- Maintain bad IDs count
- Use calculated entropy

Public recursive DNS

Google Public DNS – 8.8.8.8, 8.8.4.4

- Shared cache
- Prefetching
- 0x20
- Nonce prepending

OpenDNS

DynDNS / Internet Guide

Neustar / DNS Advantage

And many more…

Reponse time for valid responses

2000
1800
1600
1400
1200
1000
800
600
400
200
0
Average [ms]
95th percentile [ms]
13:39
14:09
14:39
15:09
15:39
16:09
16:39
17:09
17:39
18:09
18:39
19:09
19:39
20:09
20:39
21:09
21:39
22:09
22:39
23:09
23:39
00:09
00:39
01:09
01:39
02:09
02:39
03:09
03:39
04:09
04:39
05:09
05:39
06:09
06:39
07:09
07:39
08:09
08:39
09:09
09:39
10:09
10:39
11:09
11:39
12:09
12:39
13:09
13:39

COM+NET zones best server response time vs. average response time

250
200
150
100
50
0
com+net average [ms]
com+net best server [ms]
13:39
14:09
14:39
15:09
15:39
16:09
16:39
17:09
17:39
18:09
18:39
19:09
19:39
20:09
20:39
21:09
21:39
22:09
22:39
23:09
23:39
00:09
00:39
01:09
01:39
02:09
02:39
03:09
03:39
04:09
04:39
05:09
05:39
06:09
06:39
07:09
07:39
08:09
08:39
09:09
09:39
10:09
10:39
11:09
11:39
12:09
12:39
13:09
13:39

How can we improve this?

- Prefetching
- Shared cache

- Better choice of servers to talk to
- Local copies of Root/TLDs

Boyan Krosnov

boyan@krosnov.org

+44 7588 865 702