Bailiwickness of DNS glue records

Networks project, 2019

Steven Karas, Phillip Kaplan, Ron Aharoni

Introduction

- DNS is one of the critical protocols underpinning the internet
- Glue is a necessary component - a sort of bootstrapping to be able to locate name servers before knowing where to find the domain they’re hosted on
    - Critical when they’re the authoritative server for the domain they’re hosted on
- Certain classes of DNS spoofing attacks can be mitigated by not caching out of bailiwick glue
- We set out to find out how prevalent out of bailiwick glue is on the internet

Related Work

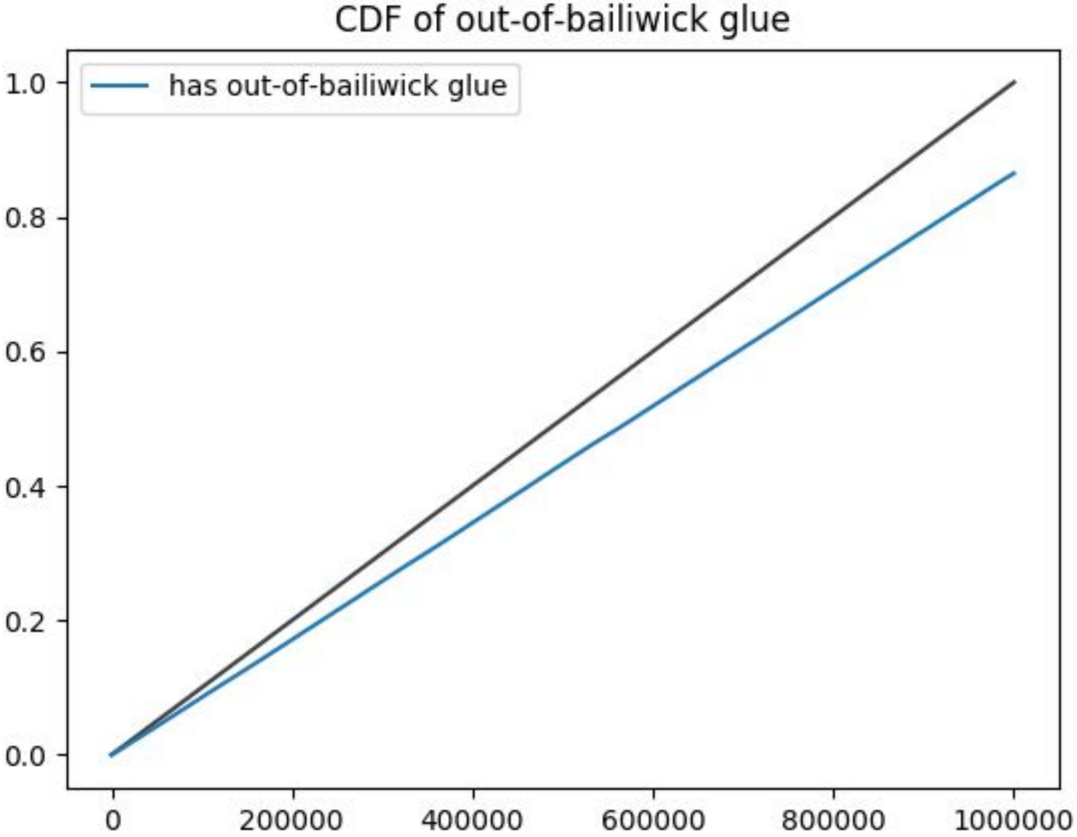
- “The Availability and Security Implications of Glue in the Domain Name System” Zheng Wang, 2016
    - A summary of the uses of glue and the implications in terms of availability and security
    - An examination of various attacks and mitigations, including DNSSEC

- “Black Ops 2008: It’s The End Of The Cache As We Know It” Dan Kaminsky, 2008
    - Presentation of various attacks on DNS and mitigations

Technical Details

- Tools:
  - Majestic Million - domains list
  - BIND recursive resolver
  - dig - for lookups
  - Parallel - useful utility, because 1,000,000*(round trip time) is a lot
  - The usual suspects: Python 3, pandas, matplotlib, bash

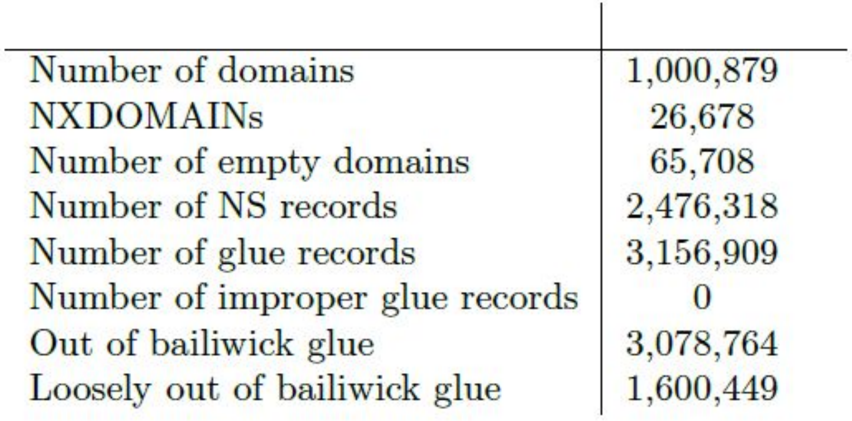
- Zones, not domains
  - We’re only interested in domains that speak for themselves
  - plus.google.com is equivalent to google.com as far as name servers are concerned


CDF of out-of-bailiwick glue
has out-of-bailiwick glue
1.0
0.8
0.6
0.4
0.2
0.0
0
200000
400000
600000
800000
1000000

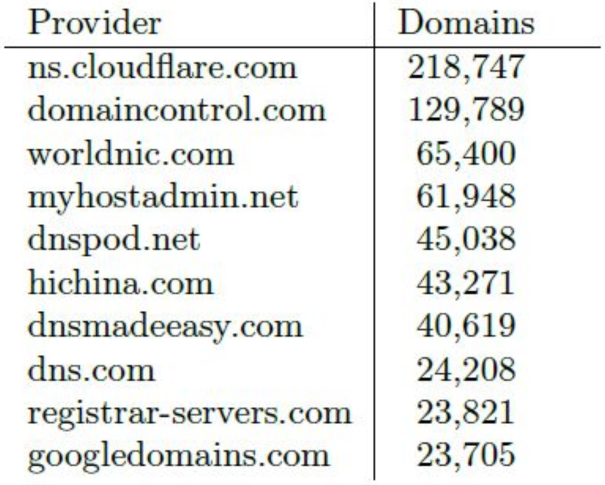
Domain Rank

Other Statistics

the real magic is the friends we made along the way



Number of domains	1,000,879
NXDOMAINs	26,678
Number of empty domains	65,708
Number of NS records	2,476,318
Number of glue records	3,156,909
Number of improper glue records	0
Out of bailiwick glue	3,078,764
Loosely out of bailiwick glue	1,600,449



Provider	Domains
ns.cloudflare.com	218,747
domaincontrol.com	129,789
worldnic.com	65,400
myhostadmin.net	61,948
dnspod.net	45,038
hichina.com	43,271
dnsmadeeasy.com	40,619
dns.com	24,208
registrar-servers.com	23,821
googledomains.com	23,705

Evaluation and Discussion

- Out of bailiwick glue is everywhere
  - Mitigation - don’t cache (used by many servers, different definitions of bailiwick than we used)
- Third party name server hosting is far more common than self hosting
- This is probably desirable
  - DNSSEC adoption fixes most problems
    - DNSSEC is hard (or costs money), but third party name server hosts could make it easy
  - Bailiwick checking is a very limited mitigation in any case, and it doesn’t protect against all kinds of attacks
- Glue records sometimes cost money (e.g. Cloudflare charges $200/m)
- DNSSEC sometimes costs money (e.g. GoDaddy charges $5/m)

Conclusion

- DNS is one of the main protocols underpinning the internet, and glue is a critical component in its function
- Certain classes of attacks on on DNS infrastructure make use of out-of-bailiwick glue
- Use of out-of-bailiwick glue is widespread across the internet
- This is probably a reasonable tradeoff
- DNSSEC is an effective mitigation