Abstract

Introduction

* Background of problem
  + DNS hijacking
    - With unencrypted DNS, information is leaked to resolvers – untrustworthy resolvers can exploit this)
  + Encrypting DNS makes it more difficult for these untrustworthy resolvers to corrupt and tamper with messages
    - DoH v DoT
* Our question
  + A couple mainstream resolvers exist (i.e., Google, Cloudflare, Quad9)
    - We found 75 DoH servers (majority are lesser known)
  + How extensive is the deployment of encrypted DNS outside of the mainstream resolvers?
  + How does the performance of these services depend on where you are on the network
    - Relates to the resolvers being grouped by continent
    - Different vantage points necessary to answer this

Background

* Overview of the Domain Name System (DNS) and resolvers
* How do we classify resolvers as reliable?

Method

* Overview of goal:
  + Understand how usable the DNS encrypted ecosystem is as a whole rather than just major operators
* Metrics
  + DNS response times
  + Ping times
  + Response size?
  + Geolocation of each resolver
    - MaxMind
    - Explain why we grouped the resolvers by location (continent)
* Vantage points
* List which resolvers we measure
* Describe the domains that we use and how we arrived at this list
  + We want to measure a wide array of websites
    - Smaller: Google
    - Larger: New York Times
      * Takes longer to load
  + Same domains for each vantage point
* Limitations?

Results

* Boxplots
* Many lesser known resolvers had higher response times than well-known resolvers
  + Ex: Tiar had a significantly higher response time than quad9’s resolver (by over 700 ms)
* A couple lesser-known resolvers had close speeds to mainstream resolvers
  + Ex: Ordns and Google (Ordns is slightly faster than Google)
  + Ex: Mullvad and Google
* Results from different vantage points

Conclusion