TRADEOFFS IN DNS PROTOCOL EVOLUTION, SECURITY, AND CENTRALIZED VS. DISTRIBUTED ARCHITECTURES

Jari Arkko
Ericsson Research, Finland

BACKGROUND

- Technology evolution in the Internet stack
    - New tech provides significant improvements & has considerable take-up
- Defending against large-scale unwarranted surveillance
    - Concerns about commercial data gathering and use
    - Perspectives beyond (“my layer”) or (“tech only”)

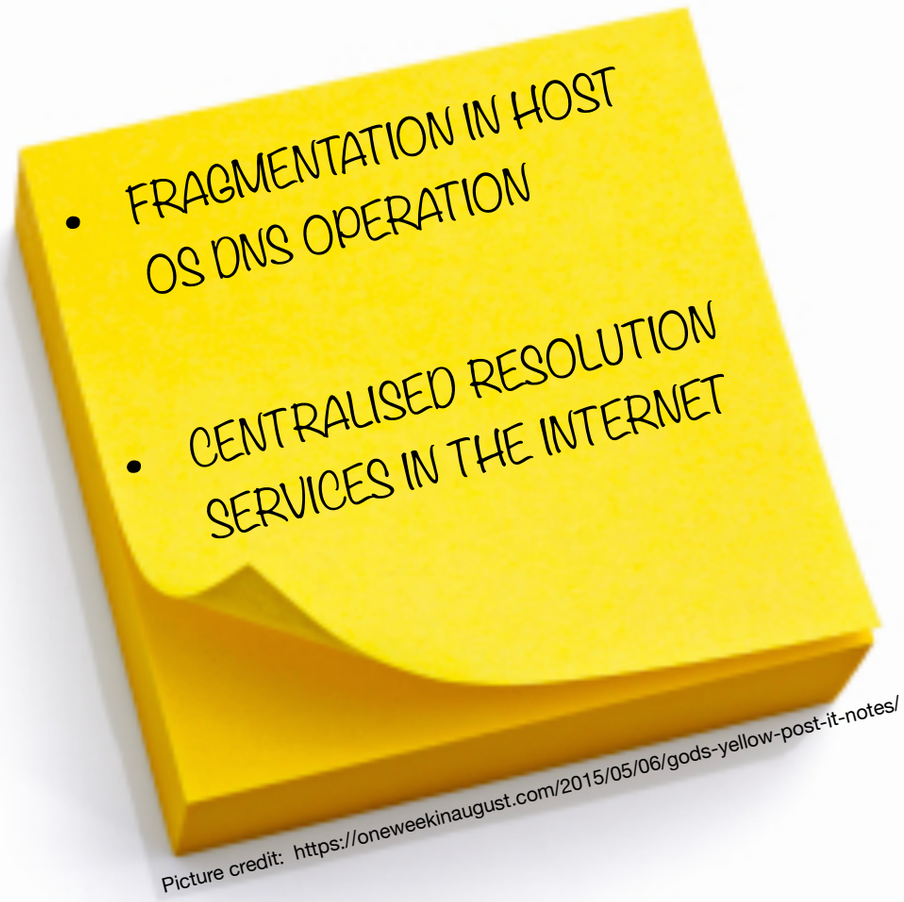
DNS EVOLUTION

- Tech largely stable (or stagnant, but stability can be good)
    - With some technical difficulties, and difficulty in deploying new things universally across the world
- Recent interest in employing web tech developments in DNS
    - Much better (query) security & efficiency & programmability
    - Similar market factors as in the web evolution case; deployment easy
- Growth in “quad n.n.n.n” solutions
    - Much better adoption of new tech
    - Security improvements, less local control

Image source: Tom’s Hardware

ANALYSIS

- It seems like we have found an opportunity for evolution
- With significant end-user improvements in sight
- Some concerns, exist, however:
  - Potential fragmentation of host OS resolution services (browser vs. other apps, debugging, etc.)
  - New tech coincides with a centralisation trend
  - Resolution services in the hands of few players vs. 1000s of ISPs creates a large, attractive target
    - Effects of users being behind carrier-grade NATs are probably not sufficient to mitigate the issues



Picture credit: https://oneweekinaugust.com/2015/05/06/gods-yellow-post-it-notes/

ARCHITECTURE

- We need to think about security not from a narrow protocol layer point of view

- There are a number of components

  - Protecting the integrity of information (DNSSEC)

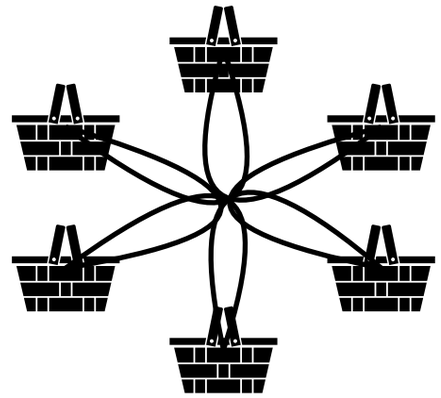
  - Protecting against on-path privacy or other security problems (TLS, web tools)

  - Avoiding the creation of large concentrated traffic flows through one point or centralised data stores

    - While web tech and e2e encryption helps protect against some attacks, it does not help protect against all (e.g., government, commercial)

DIRECTIONS FOR POTENTIAL SOLUTIONS

- It is not just about communication security!
- Not all all eggs in one basket



- Distribution & collaboration
- Discovery of DNS services rather than hard bindings
- Separation of functions to different parties
    - Reduce ability to correlate
    - E.g., obfuscation of source address vs. what is being asked as in ODNS

THE ASKS

1. Please provide feedback — are the concerns outlined here valid, or mitigated by technology or other factors?

2. If the concerns are valid, can we design something that can provide both improved security, efficiency **and** continue the distributed Internet model

DISCUSS!