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”)

monitoring pervasive attack
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
  • 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
• It seems like we have found an opportunity for evolution

• With significant end-user improvements in sight

• Some concerns, exist, however:
  • Fragmentation of host OS resolution services (browser vs. other apps, debugging, etc.)
  • New tech coincides with a centralisation trend
  • Resolution services via 1000s of ISPs vs. few players creates a large, attractive target
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 or data store through one point

    • While web tech and e2e encryption helps protect against some attacks, it does not help protect against all (e.g., government, commercial)
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, please design something that can provide both improved security, efficiency and continue the distributed Internet model.
DISCUSS!