DNS privacy problem statement

Peter Koch - DENIC & Stéphane Bortzmeyer - AFNIC

dnsop - IETF 89 - London

Open data

An actual DNS query reveals:

1. Who is requesting (yes, I know, the status of the source IP address is complicated. . .)
2. What is requested (the QNAME)

It may defeat, at least partially, some security measures (such as HTTP**S**)

QNAME is revealing

1. `www.political-party.example` ← Sensitive information
2. `_bittorrent-tracker._tcp.domain.example` ← MPAA may be interested
3. `le-pc-de-pascal.domain.example` ← Personal information
4. PGP keys in DNS (indexed by user's email, see DANE WG) ← More personal information

Who can listen?

1. Name servers (both recursors and authoritative) sysadmins. "Enablers" in RFC 6973 parlance.
2. Third-parties sniffing the cable

We need solutions for "on the wire" and "on the server".

Two cases

May require different solutions

1. Client machine $\leftrightarrow$ full resolver (no caching to protect you) (you talk only to a few resolvers)
2. Resolver $\leftrightarrow$ auth. name server (some protection because of caching and relaying by the resolver) (needs scalability)