Problem statement

Peter Koch - DENIC & Stéphane Bortzmeyer - AFNIC

IETF 89 - London

DNS traffic is revealing

We want to protect **traffic** rather than **data**

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

A sniffing 3rd party can learn what you're doing

Eve (who runs a sniffer) knows the hostname you connect to even if you use HTTPS or SMTP over TLS.
There are other leaks (SNI...) but we focus on our responsibility: the DNS

Two cases

May require different solutions

1. Client machine ↔ full resolver (no caching to protect you) (you talk only to a few resolvers)
2. Resolver ↔ auth. name server (some protection because of caching) (needs scalability)

Other issues

It’s a problem statement, not a formal requirements list.
For instance, monitoring and statistics issues, or behavior of resolver when no encryption available are not discussed yet.