
# DNS Privacy: Problem and solutions

*A presentation by Dmitry Belyavsky, TCI*

*TLDCON 9*
*Tbilisi, Georgia, 2016*

# Age of privacy

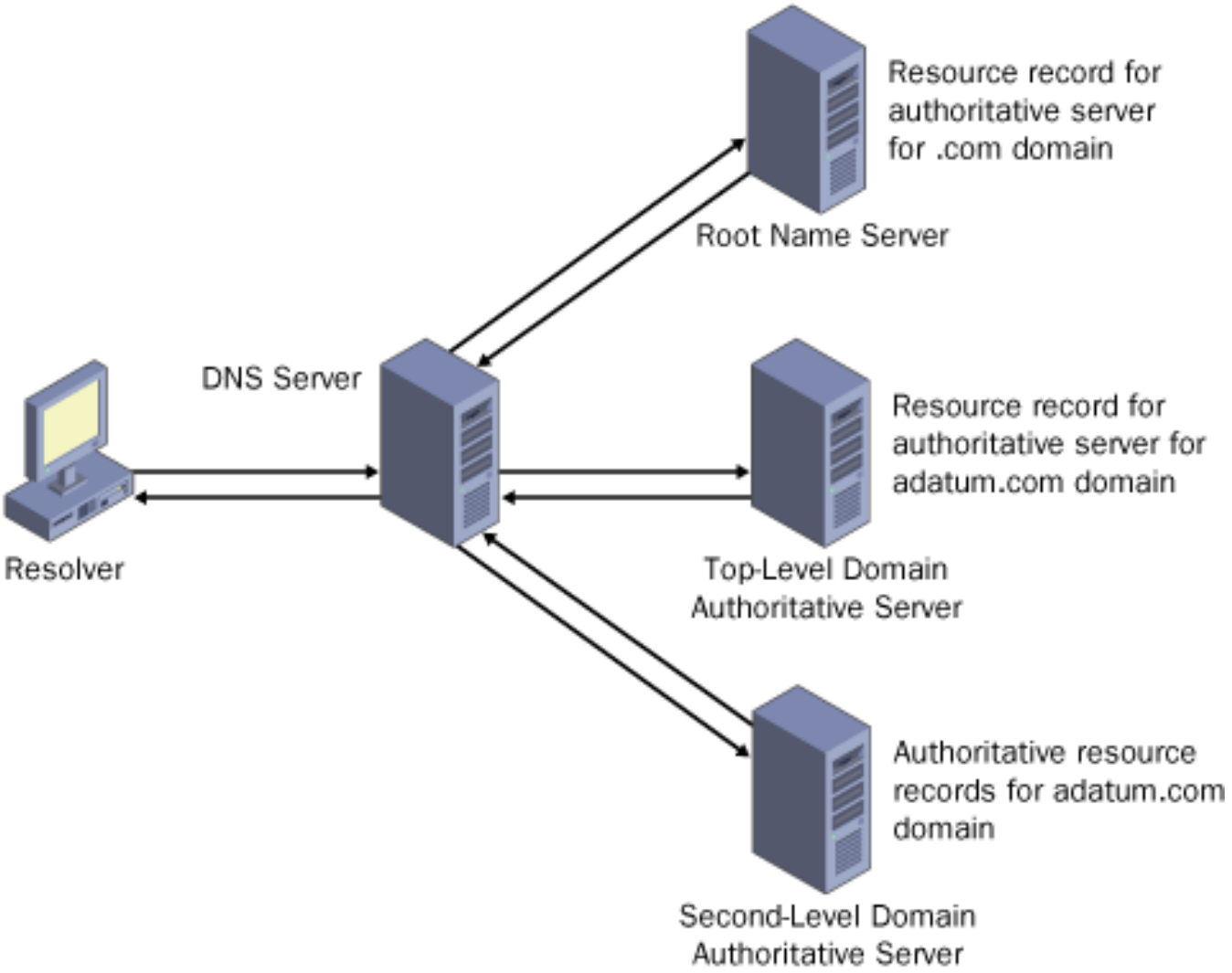
- Internet has changed the world
- What is privacy now?
  - Personal data
  - Metadata (Whom did you contact to?)
  - Cookies, web-counters…
- Nation-wide eavesdroppers
- Protecting privacy
  - Safe protocols:
    - HTTPS, IMAPS, SFTP, SSH…
    - All but DNS!

# Problem with DNS

- DNS – very old protocol
- Is DNS Data sensitive?
- DNSSec does not protect data exchange from monitoring

- Send as little data as possible!
- Encrypt it!

# Normal resolving process



# DNS Privacy: history

- Initiated by Stephane Bortzmeyer (2013)
  - IETF working group **dprive** (2014)
    https://datatracker.ietf.org/wg/dprive
- Threat model: RFC 7626 (2015)
- QNAME minimization: RFC 7816 (2016)
- EDNS(0) Padding Option: RFC 7830 (2016)
- DNS over TLS: RFC 7858 (2016)

# DNS Privacy: Threat model

- Described in RFC 7626
  - DNS data is public,
  - Your DNS request is NOT Public
    - QNAME
    - Source IP
  - DNS and data routing may differ
  - DNS requests are not encrypted
  - Up to 70% of users can be recognized by their queries.

# DNS Privacy: QNAME minimization

- Described in RFC 7816 (Experimental)

  If you want to access l5.l4.l3.example.com,

  - root DNS servers can answer about .com
    - .com – about example.com
      - …
  - No extra privacy leaks
  - May increase or reduce number of requests
  - Problems with some CDNs – to be fixed

- Supported in
  - Knot Resolver 1.0+
  - Unbound 1.5.7+

# DNS Privacy: DNS over (D)TLS

- Described in RFC 7858
  - TCP: DNS over TLS
  - UDP: DNS over DTLS
  - Port 853
- Implemented in
  - Unbound 1.4.7+ - server
  - Getdns – client
  - Go library
- Questions
  - Policy of trust to resolver's certificate?

# Related technologies: DNSCrypt

- No RFC, https://dnscrypt.org/
- Protects communication between client and resolver
- 443 port, both TCP/UDP
- Implemented in many routers and Yandex.browser (port 15353)

# DNS Privacy: conclusions

There are all the necessary standards

It's time to switch them on

# Q&A

**Questions?**

**Drop ‘em at:**

**beldmit@tcinet.ru**