Testing DNS resolvers

(as) in real world

Petr Špaček • **petr.spacek@nic.cz** • **17 May 2017 (speaking)**

Filip Široký • filip.siroky@nic.cz • (working :-)

Focus on functional testing

- Goal: “Support line should stay silent”
  - Are users able to resolve names they want?
- Ignoring
  - ~~Security~~
  - ~~Performance~~
  - ~~Usability~~
  - …

Challenges

- DNS cache
  - Lot of state
  - Ordering & timing matters
  - Forwarding → chain of caches → state explosion
- Query flags
  - RD, DO, AD, CD, …
- Weird implementations on authoritative side
- Network glitches

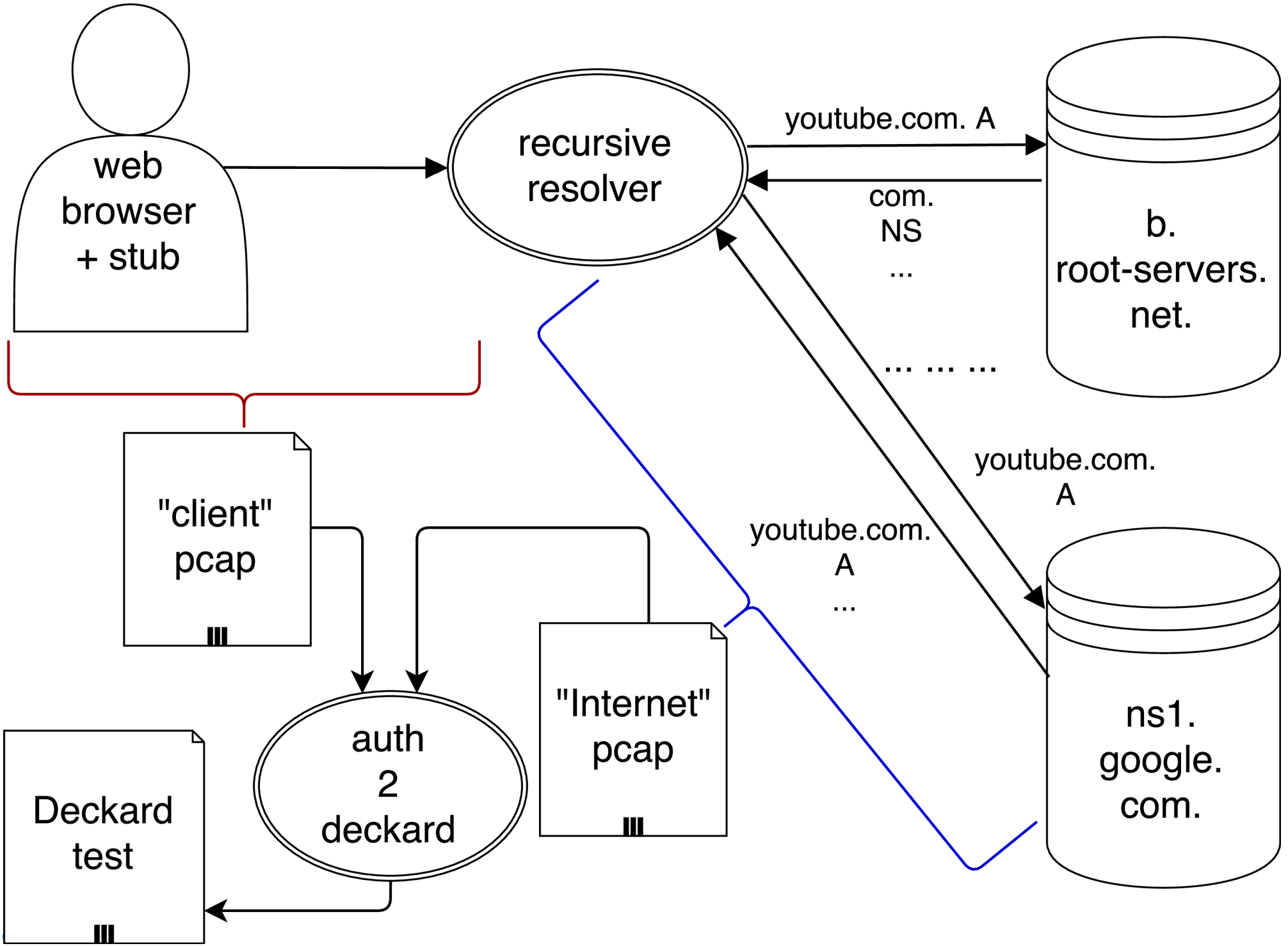
What users want?

- Open youtube.com
  - (using Firefox 52 as an example)
  - 15 DNS queries from stub resolver (2.3 seconds)
  - Some of them sent in paralell (race conditions)
  - Some repeated (cache)
- … and watch a video
  - 35 DNS queries from stub resolver (2.5 seconds)

Generating test for youtube.com

- Open a web site using Selenium (web test framework)
- Capture stub ↔ recursive resolver traffic
  - Including timing and parallel queries
- Capture resolver ↔ authoritative traffic
- Repeat with
  - Query name minimization on/off
  - Different resolvers (Knot resolver, Unbound, ...)
- Transform captured traffic into Deckard [1] test

[1] https://gitlab.labs.nic.cz/knot/deckard/blob/master/README.rst


web
browser
+ stub
recursive
resolver
youtube.com. A
com.
NS
...
b.
root-servers.
net.
... ...
youtube.com.
A
youtube.com.
A
...
ns1.
google.
com.
"client"
pcap
"Internet"
pcap
auth
2
deckard
Deckard
test

Testing youtube.com

- Use Deckard tool to simulate DNS client and replies from authorities
  - Replay sequence of queries from web browser
    - Including timing and parallel queries
  - Authorities reply with captured answers
  - Check if answers to the simulated client match
- Repeat the test with
  - query minimization off/on
  - forwarding off/on (two resolvers under test at once)

Anatomy of Deckard test

```
RANGE_BEGIN 0 1000 ADDRESS 2001:678:11::1
MATCH opcode qtype qname
REPLY NOERROR QR AA DO
SECTION QUESTION
turris.cz. IN DS
SECTION ANSWER
turris.cz. 18000 IN DS 54959 13 2 <...>

STEP 121 CHECK_ANSWER
MATCH all
REPLY RD RA QR AD
SECTION QUESTION
api.turris.cz. IN A
SECTION ANSWER
api.turris.cz. 1800 IN A 217.31.192.101
```

Further plans

- Make it work!
- Combine tests for multiple sites into one
  - Interleaving requests from multiple clients
  - Compare with captured data sets
- Mobile vs. desktop web browsers?
- E-mail?
- Other non-web clients?
- A better user simulation?

Get in touch

Deckard tool README
https://gitlab.labs.nic.cz/knot/deckard/blob/master/README.rst

Mailing list
knot-dns@labs.nic.cz

Speaker
Petr Špaček • petr.spacek@nic.cz

CZ DOMAIN REGISTRY