DoQ on authoritative

perspective, initial implementation, performance, DoS resilience

Libor Peltan • libor.peltan@nic.cz • 2022-07-30

CZ DOMAIN REGISTRY

Zone transfers over QUIC

- AXFR+IXFR over QUIC (XoQ)
  - Relatively trusted counterpart
    - Avoid DoS from outside
  - Certificates easily established
  - Slightly better than XoT
    - # of pkts, latency
  - Enables intermingled XFR query/responses

DoS attacks against DNS over UDP

- Flood attack (optional: spoofed source IP)
  - Optimize DNS answering
  - Optimize networking (XDP)
  - Handle 10^7 qps

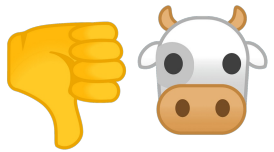
DoS attacks against DNS over TCP

- SYN attack
  - SYN cookies (firewall)
- Slowloris &Co.
  - Custom TCP stack, connection table
    - Helps against SYN attack too
  - XDP etc.
  - Handle 10^6 connections

DoS-resistant DoQ server

- Same attacks as TCP ⇒ same approach
- Knot DNS + libngtcp2
- Custom connection tables
- XDP

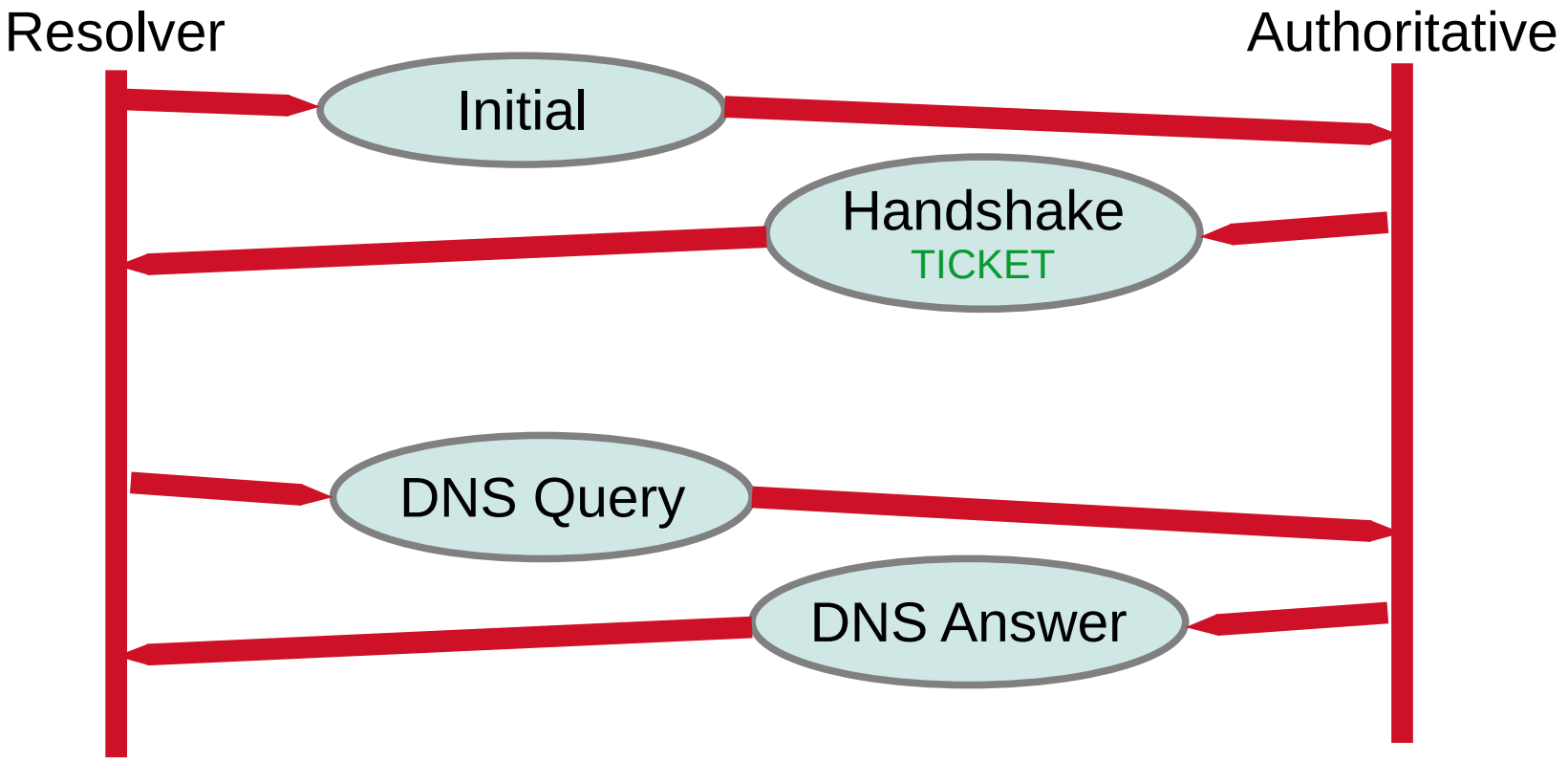
DoS-resistant DoQ server

- 10^4 connections per sec 
  - CPU usage by crypto
- Memory cosumption in magnitude 10 GiB 

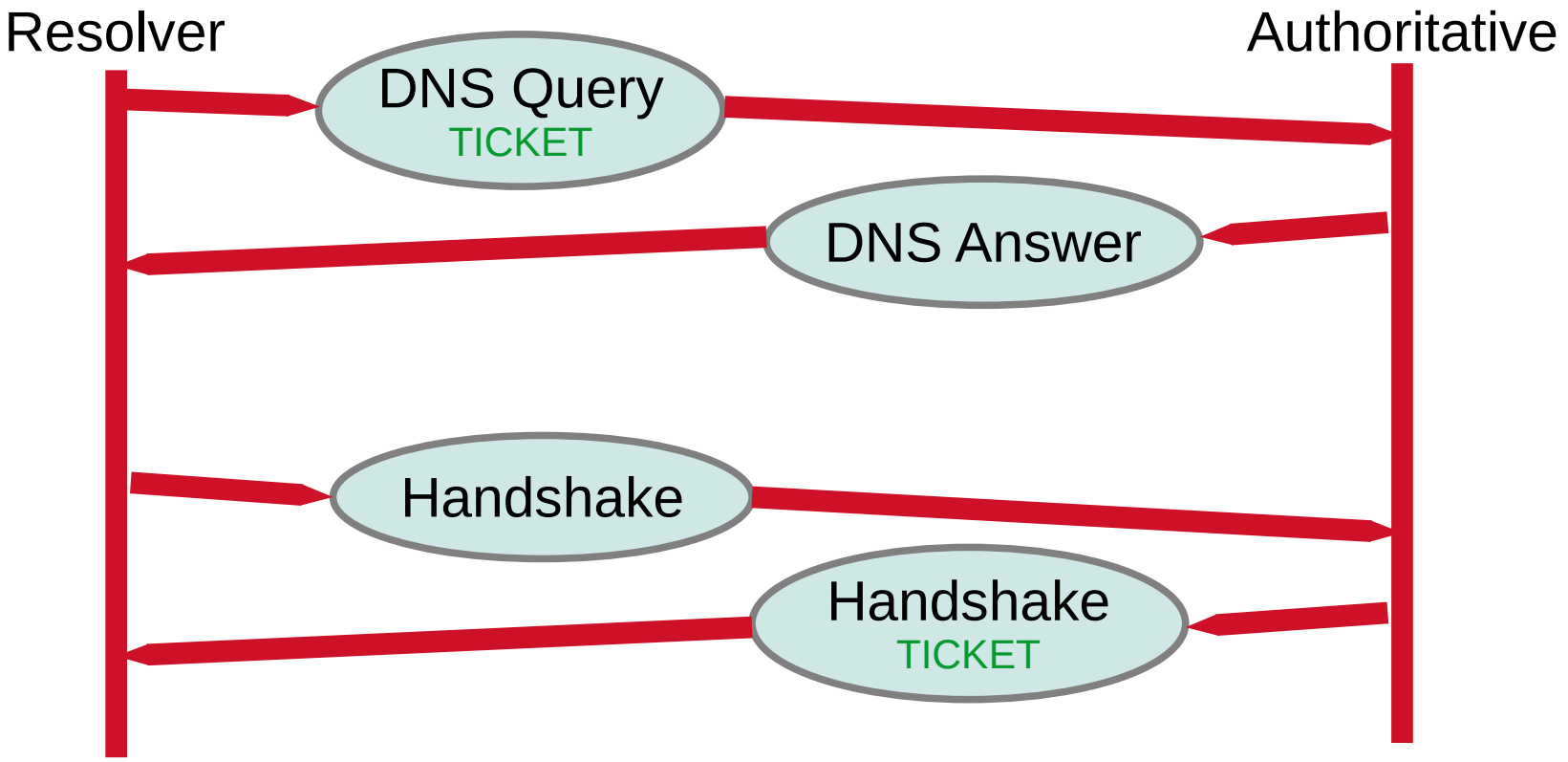
DoS attacks against DNS over QUIC

- „SYN“ attack – flood with unencrypted Initial
  - Retry packet
    - Ensures source IP not spoofed
    - Adds 1 RTT to legitimate connections
    - Not sure if helps
- Slowloris & Co.
  - Have more CPU than attacker

DoQ Full Handshake



DoQ Quick Handshake



DoQ Quick Handshake

- Lower latency (immediate DNS)
- Not fewer packets
- Resolver remembers token
- Authoritative „stateless“

DoQ Server Certificate

- Researched by IETF DPRIVE group
- So far: negative
  - Server to use self-signed cert
  - Encryption established
  - Vulnerable to active MitM
  - https://www.ietf.org/archive/id/draft-ietf-dprive-unilateral-probing-00.html

Libngtcp2

- Handling single QUIC connection
- Congestion control
- No connections management
- No events scheduling
- Needs glue to interoperate with OpenSSL/GnuTLS
  - Improved recently

Knot DNS DoQ architecture

- Libngtcp2 + GnuTLS
- Connection tables/management
  - Similar to TCP-on-XDP
- XDP
  - Soon: conventional (in-kernel) UDP as well

Try it out!

- Build Knot DNS from git master

```
xdp:
    listen: enp0s8      # XDP interface
    quic: on            # QUIC port 853
    quic-log: on        # lots of debug logs
```

- Kdig supports DoQ (also useful to query resolvers)

```
$ kdig @203.0.113.5 example.com. +quic
```

Measure it!

- Use Knot DNS kxdpgun utility

```
# kxdpgun 203.0.113.5 \
    --port 853 \
    -i /example/queries.txt \
    --duration 10 \
    --qps 1000 \
    --quic
```

- Normal legitimate traffic

  `--quic`
- Always full handshake

  `--quic=0`
- „SYN“ attack

  `--quic=1`
- Slowloris

  `--quic=5`

ADoQ Wrap-up

- Encryption & low-latency
- Performance good for ALL legitimate traffic
  - May displace UDP, TCP, etc.
- XDP benefits negligible
- DoS vulnerable FIXME
- Other quirks FIXME

libor.peltan@nic.cz

Thank you!