Encrypted DNS Research @ nic.at

EDNS Padding, Experiments, Cost Simulation

2017-07-06 · Alexander Mayrhofer · Head of R&D

Agenda

- About nic.at

- ENDS Padding is required for Privacy!
  - Motivation / History
  - RFC7830
  - Padding Size Considerations
- Practical experiments @ nic.at
  - Stubby
  - Knot Resolver
- TLS/TCP Cost Simulation
  - Current UDP-based volume
  - Client Behaviour - Assumptions
  - TLS/TCP Traffic Simulation

About nic.at

.at

1.3M domains

gTLDs

Backend + Registry

RcodeZero

DNS Services

R&D

4 FTEs

EDNS(0) Padding

It‘s required for privacy – but, why?

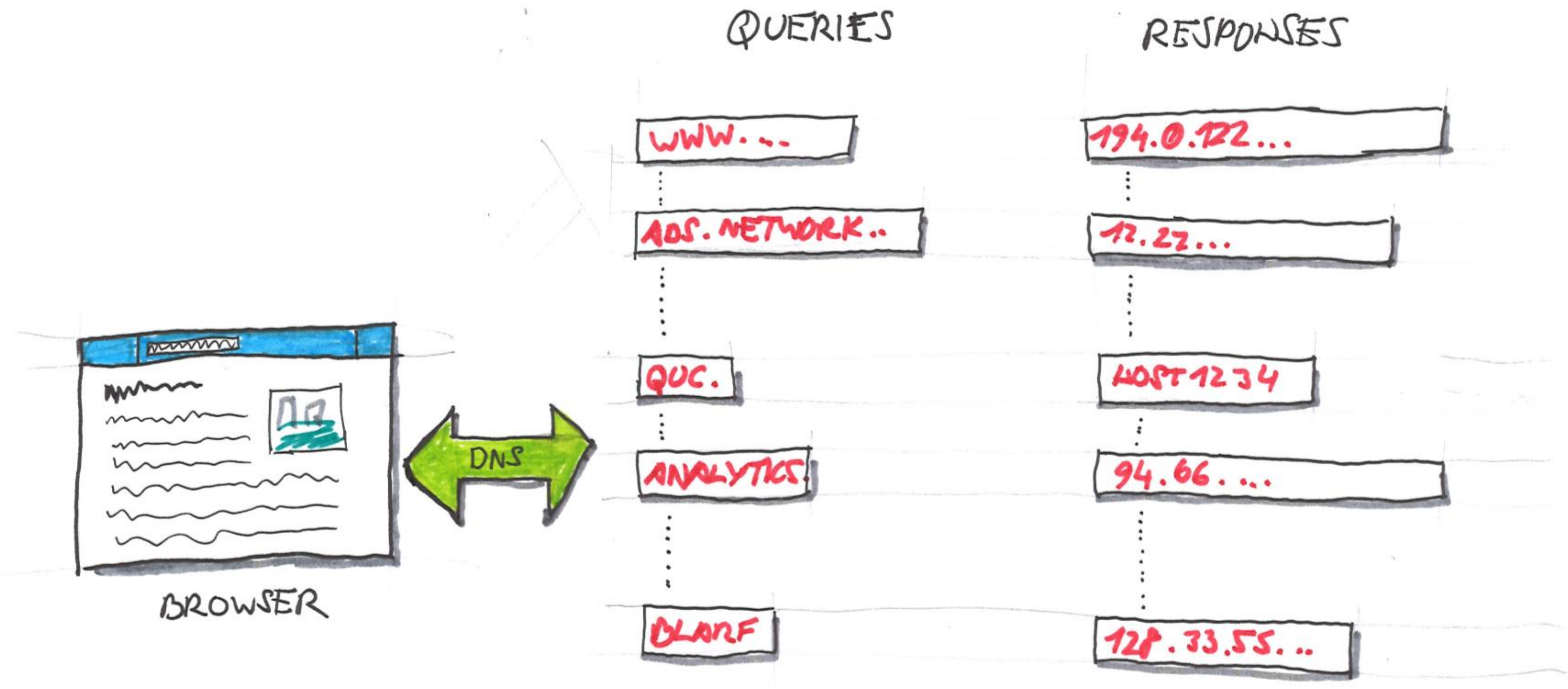
EDNS(0) Padding – why?

- Encryption removes „direct“ access to the information
  - What‘s left for the Attacker?
- „Pretty Bad Privacy – Pitfalls of DNS Encryption“*
  - Haya Shulman @ IETF 93
  - Applied Networking Research Price – IRTF
- Side Channel information is key!
  - Countermeasures

*https://www.ietf.org/proceedings/93/slides/slides-93-irtfopen-1.pdf

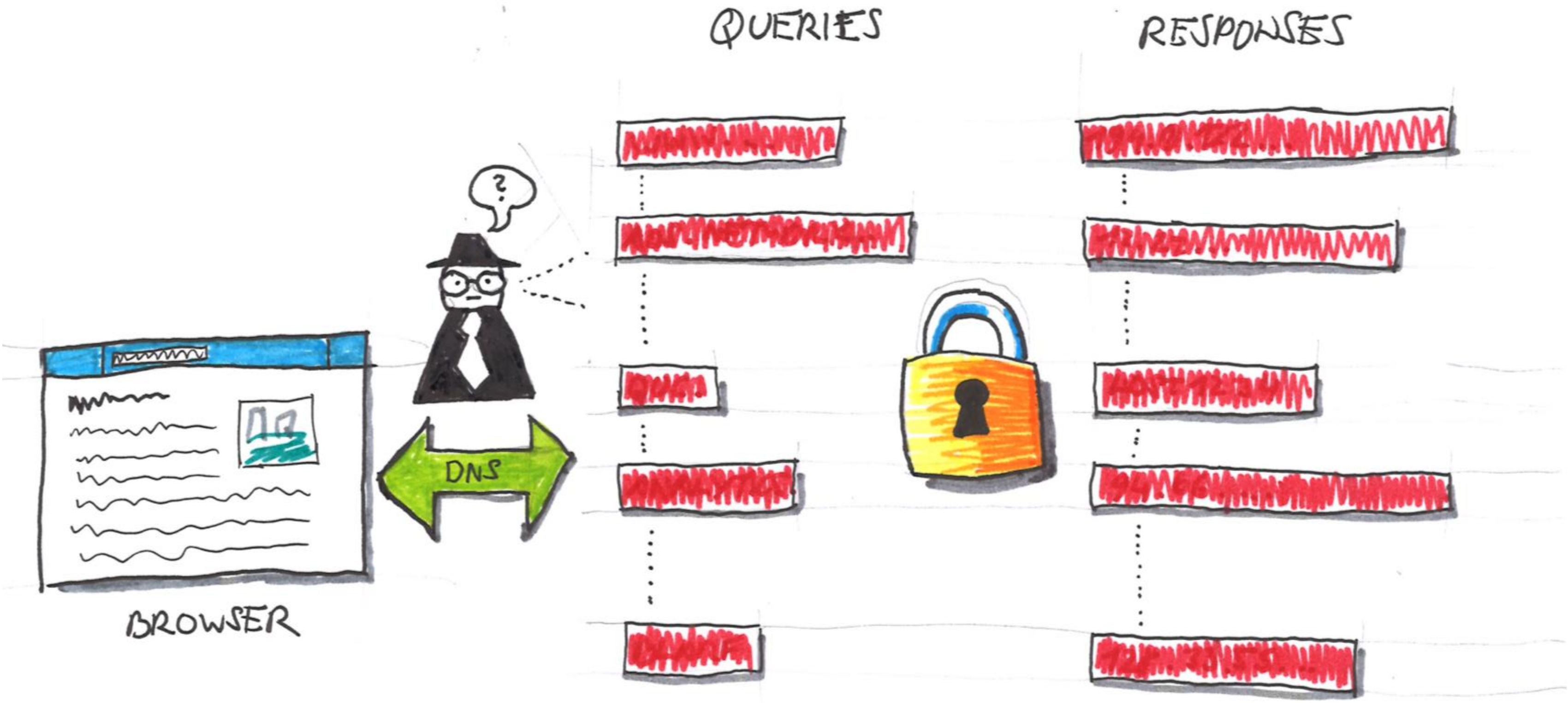
Application Queries – it‘s a stream

- A Pattern - Not just a single query/response pair



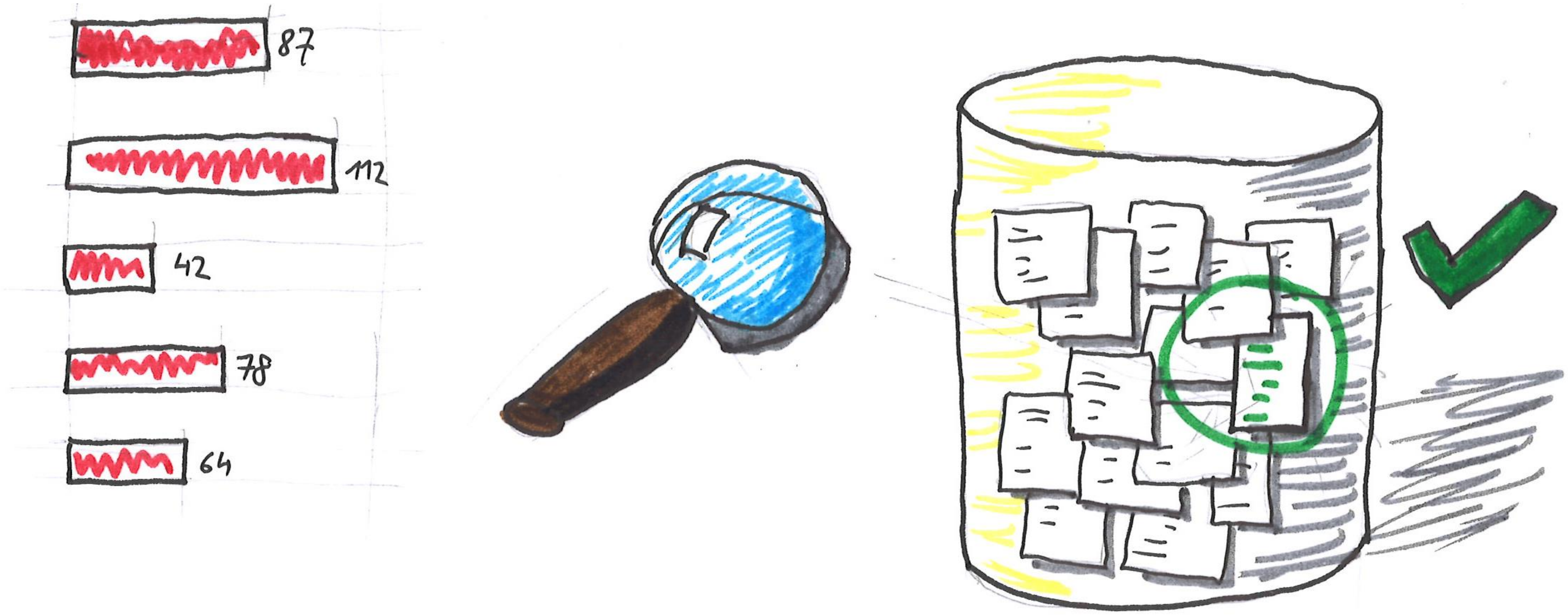
Encrypted DNS

- Streams still create size/timing „patterns“



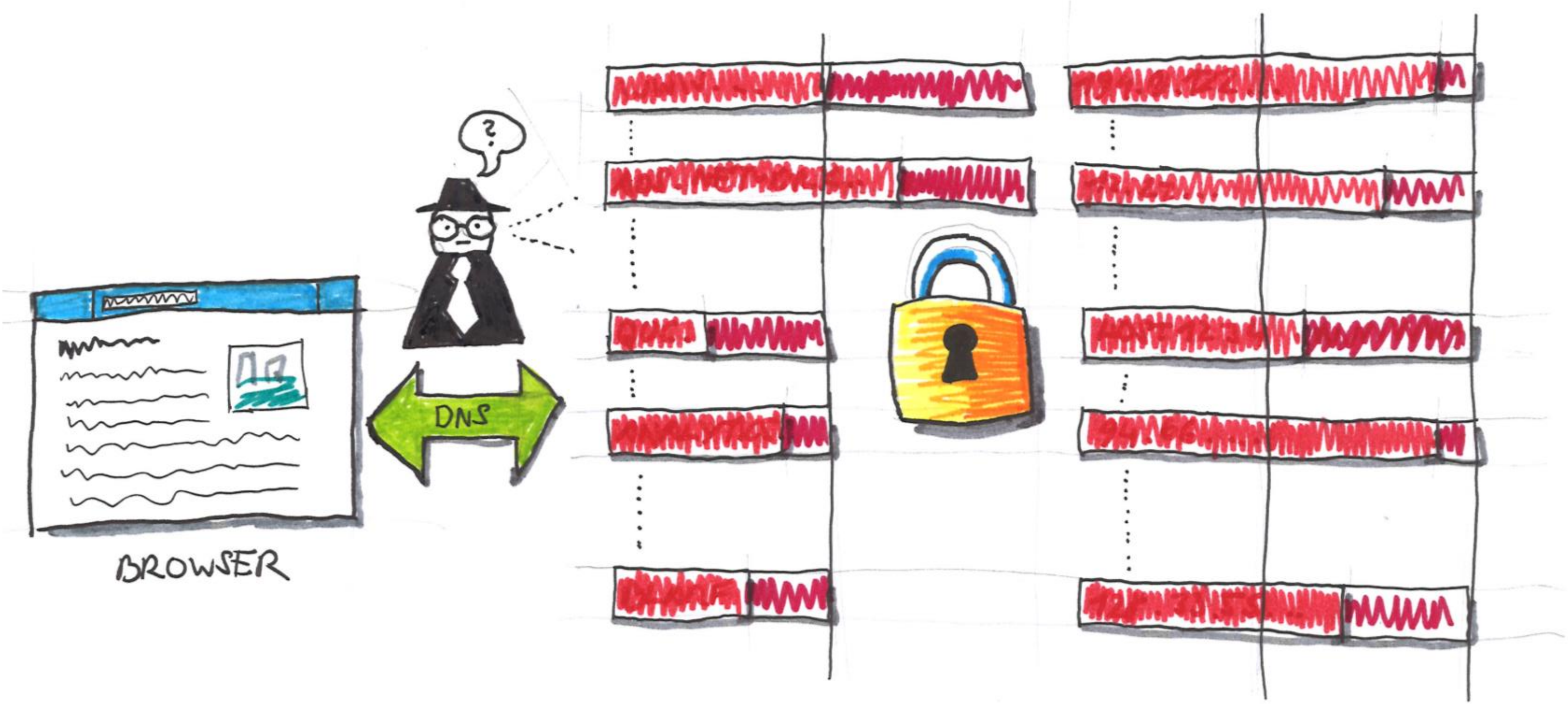
Size based Correlation

- Compare with known clear text patterns
- Even works with a subset of message sizes



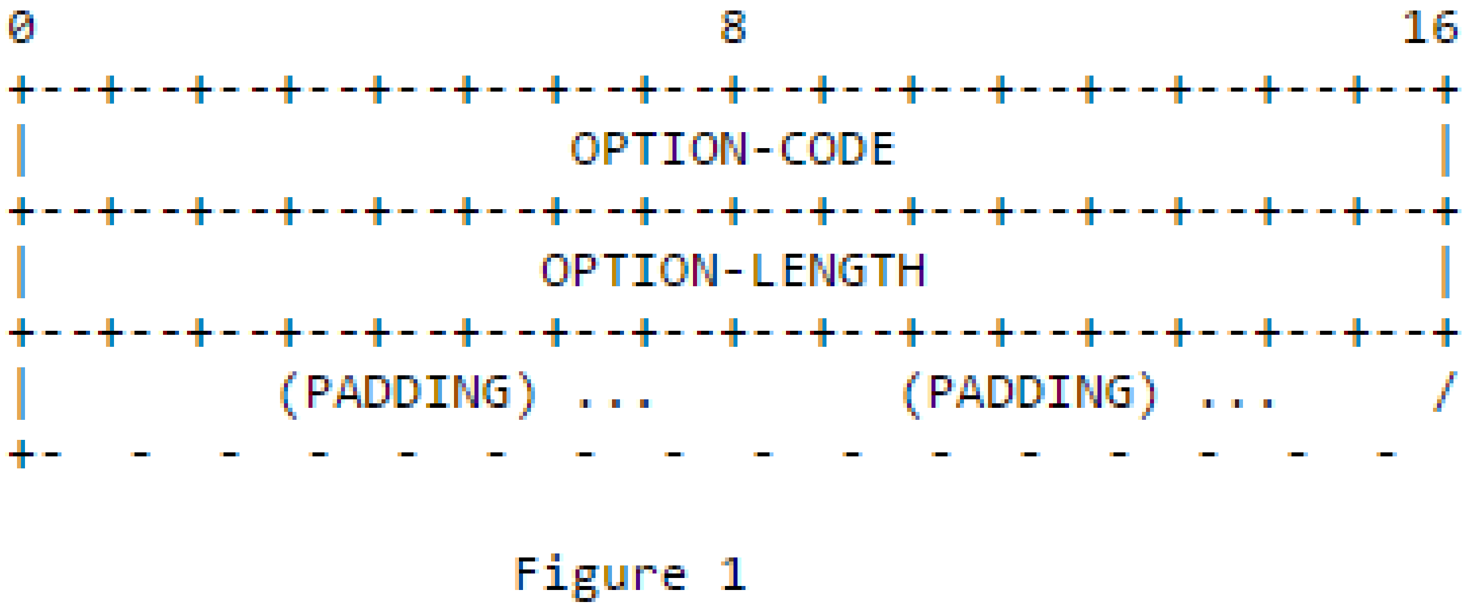
Introducing Padding

- Obfuscates the size pattern -> Hampers correlation
- More „hits“ -> less likely that identification is possible



RFC 7830 – EDNS(0) Padding Option

- EDNS Option code 12



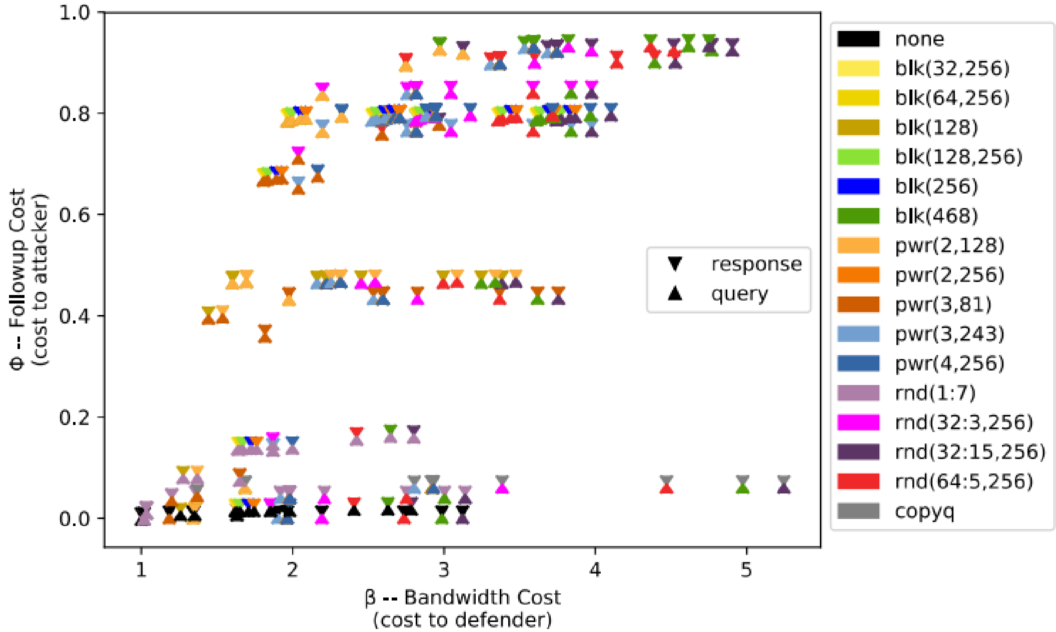
```
0                       8                      16
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                  OPTION-CODE                  |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                 OPTION-LENGTH                 |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|        (PADDING) ...         (PADDING) ...    /
+-  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -

                  Figure 1
```

https://tools.ietf.org/html/rfc7830

Size of Padding?

- Block? Random? Power of 2? Maximum?
  - Tradeoff resources vs. Identifcation potential
- Empirical Research Work by Daniel K. Gillmor*
  - Evaluates strategies against Attacker / Defender Costs
- IETF: Padding Policy Draft** (wip)



*https://dns.cmrg.net/ndss2017-dprive-empirical-DNS-traffic-size.pdf

**https://tools.ietf.org/id/draft-ietf-dprive-padding-policy

Experiments with encrypted DNS

Stubby + Knot Resolver

Pssst… nothing new here… move on…

Encrypted DNS Cost Simulation

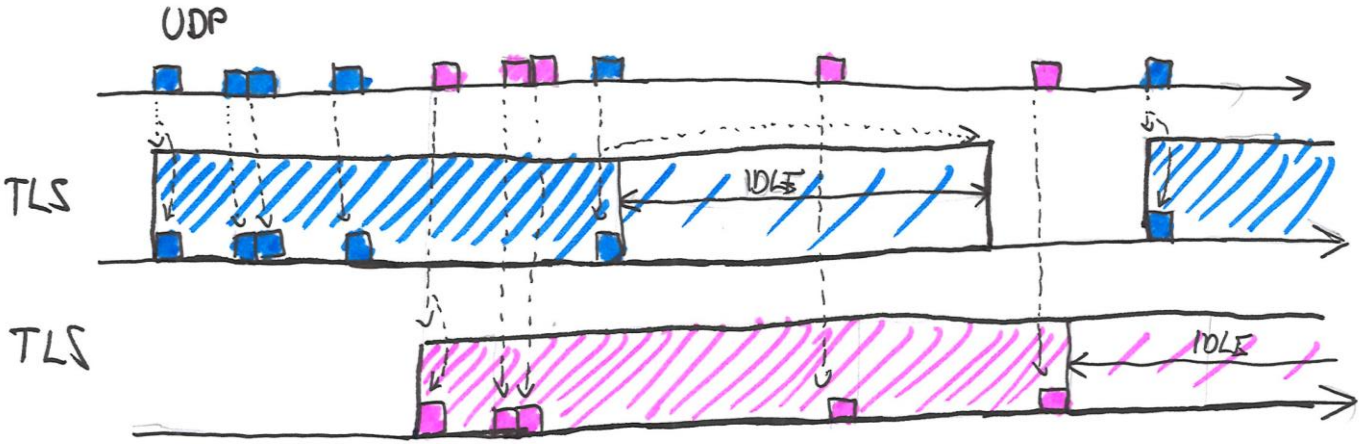
There‘s no Free Lunch in Security

Basic Question & Idea

- „What if 100% of all DNS queries would reach us via TCP/TLS?“
- Let‘s simulate it!

```
Assumption of client behaviour +
Real world packet traces =
---------------------------------
Simulated TLS/TCP Traffic/events *
Estimated cost factors
---------------------------------
„Guesstimated‟ TLS/TCP Costs
```

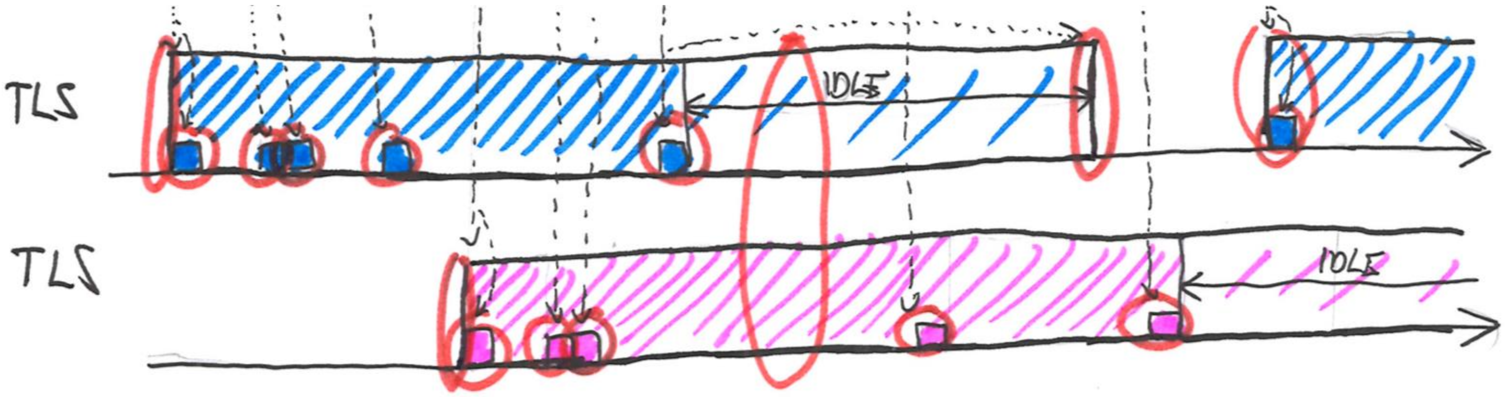
Simulation „Rules“ / Assumptions



- Sessions & Queries:
  - First query from an IP starts TLS session
  - Subsequent queries use existing session
  - One session per client IP
  - Assumes pipelining etc..

- Session will terminate after:
  - N seconds idle time
  - M seconds max session length (M > N)
  - X number of max. queries

Simulated Events / data

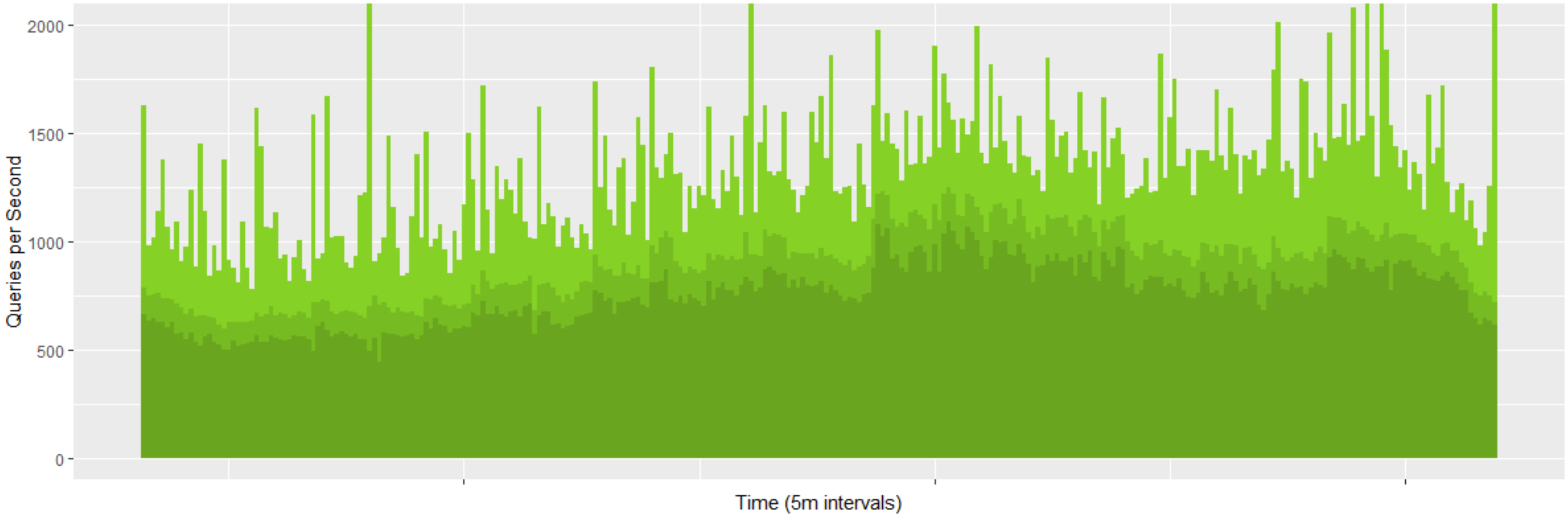


- Session Setup
- Session Teardown
  - Idle timeout
  - Max. session duration
  - Max. session queries

- Queries (Responses)
- Concurrent session count
  - at a given time
  - Idle vs active
  - Session duration

(Etc. etc. etc)

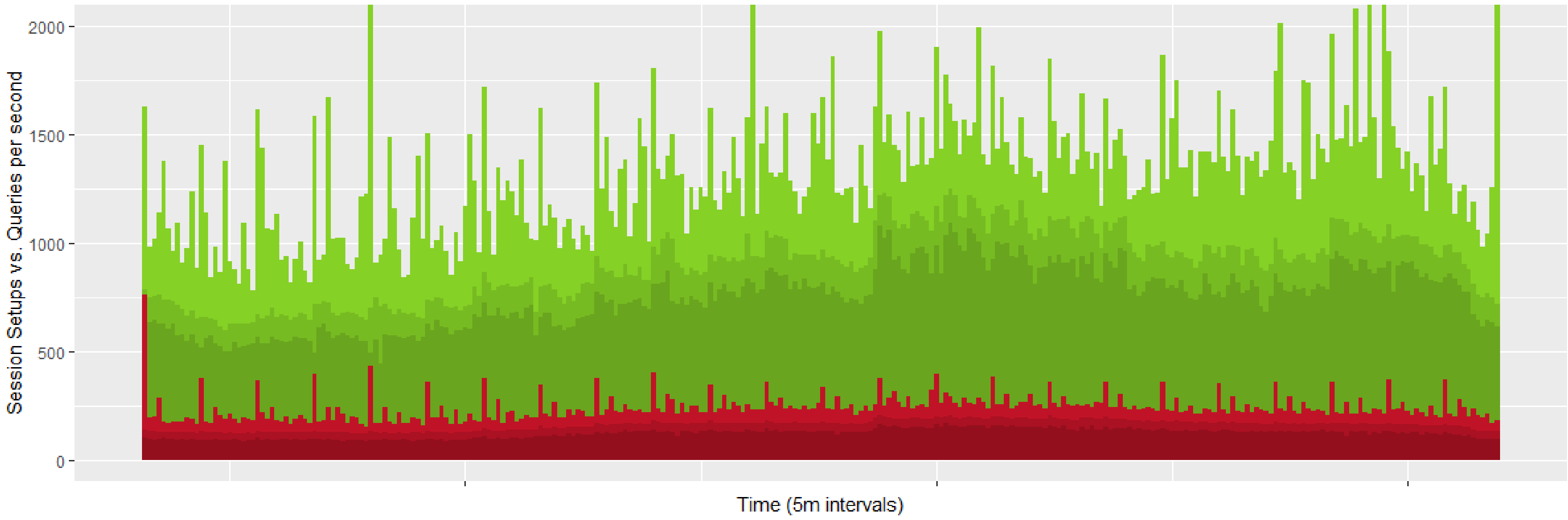
Input Data



- .at PCAP data
  - Authoritative!
  - Single server
  - 78M queries (~1000qps)
  - IPv4 / UDP only

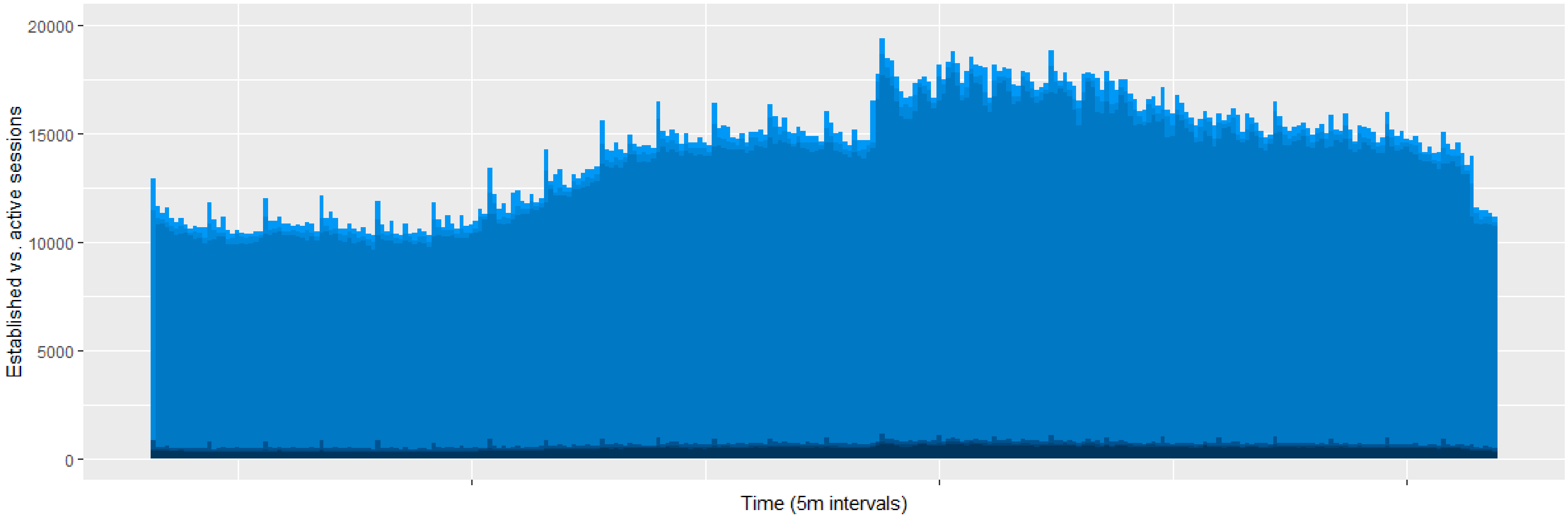
- Traffic properties
  - „normal“ day (20170620)
  - Few spikes / no DDoS
  - Biggest spike: 11k qps
  - ~7% of .at total traffic

Simulation Results: Session setups



Idle = 60s; maxduration=3600s; maxqueries=10.000

Sessions: Established vs. Active



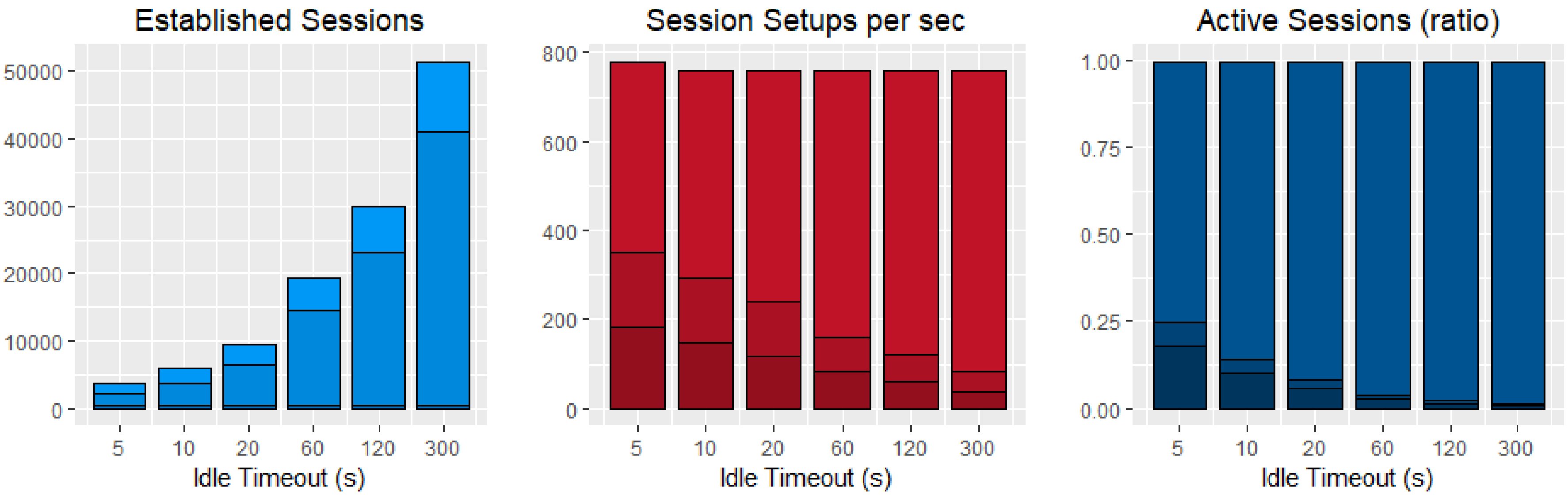
Idle = 60s; maxduration=3600s; maxqueries=10.000

Session Teardown Details

- Reasons:
  - Idle Timeout: 13.8M sessions (99.98%)
  - Maximum Duration: 16222 session (0.12%)
  - Maximum Queries: 1339 sessions (0.0097%)
- Idle Timeout – by „usage intensity“:
  - Short sessions (d < 2*idle): 12.6M (91.3%)
  - „Burst“ sessions (active < 3s): 10.6M (77,0%)
- # of Queries: 38.25 per session (avg.)

-> Idle Timeout has the biggest impact!

Vary the Idle Timeout



- Simulate for 5, 10, 20, (60), 120, 300s idle timeout
  - Retain other parameters (max duration, max queries)
  - Tradeoff Established Sessions vs. Session Setups
  - Where‘s the „Sweet Spot“?

Beware! Guesstimate!

Cost Estimation

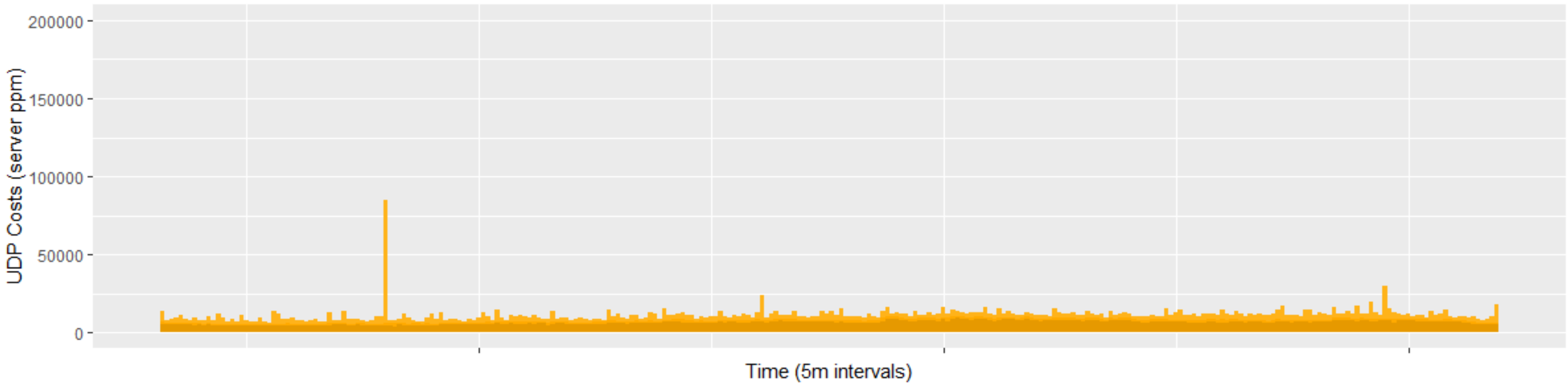
- Packets per Second (pps – 600kpps capacity)
  - Query/Response: 2 packets / 3.3 ppm
  - TCP/TLS setup: 6 packets (…) / 10 ppm
  - Teardown: 3 packets / 5 ppm
- CPU/IO/ …*
  - Query: 200k qps/server 5 ppm
  - TLS Setup: 3300 sps/server 300 ppm
  - Session Teardown: ? 20 ppm (guess!!)
- Memory - 2GB capacity (for TLS)
  - TLS Session: 3kB/session** 1.5 ppm

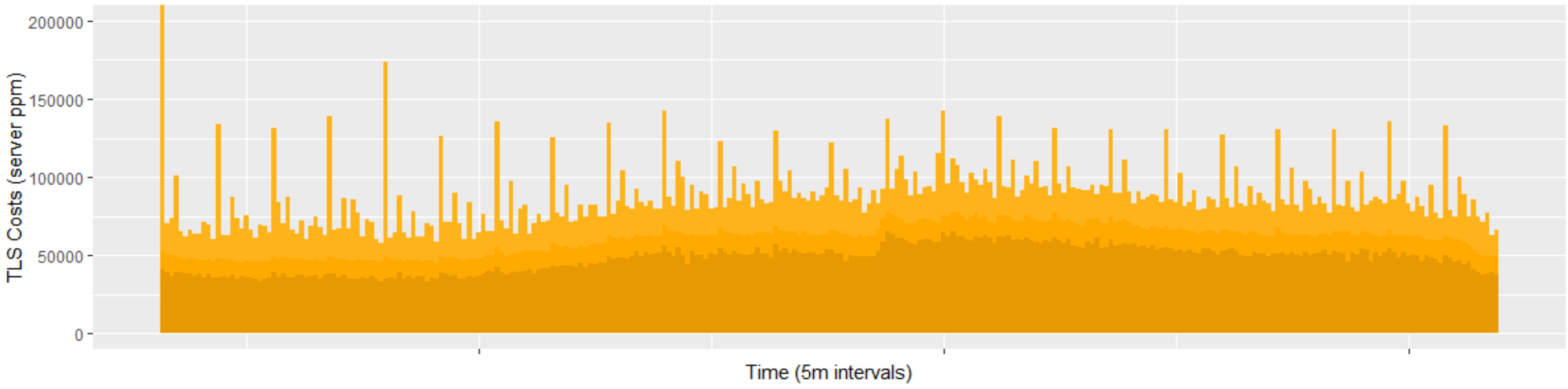
*https://cdn-1.wp.nginx.com/wp-content/files/nginx-pdfs/Sizing-Guide-for-Deploying-NGINX-on-Bare-Metal-Servers.pdf

**https://www.wolfssl.com/wolfSSL/benchmarks-wolfssl.html

Cost Comparison

Beware! Guesstimate!



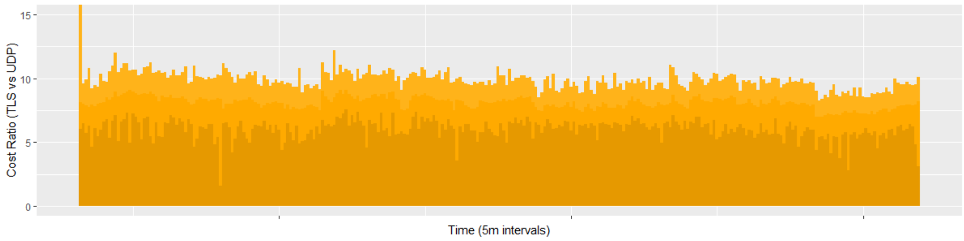


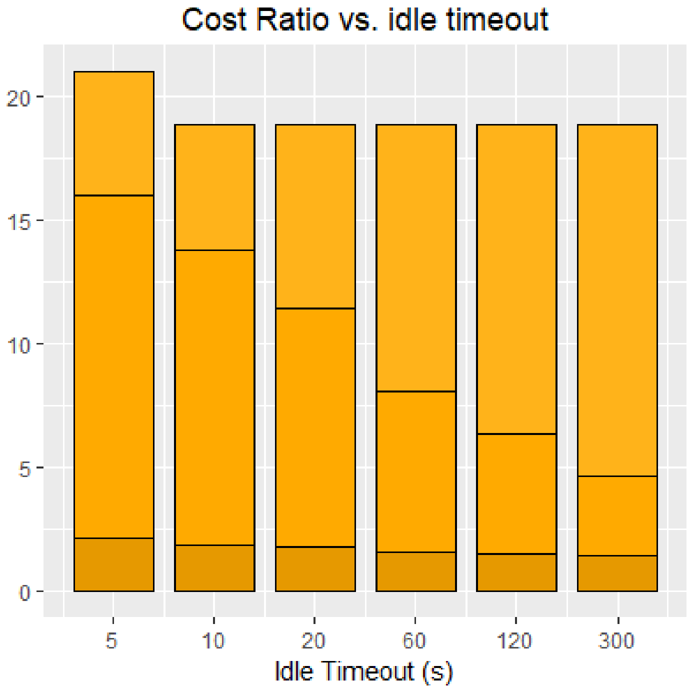
What‘s the „Magic Number“?

- TLS vs. UDP Cost Ratio

~8

(60s idle timeout)





Summary

- ENDS Padding – required for Privacy!
  - RFC7830 - Size recommendations in progress
- TLS-DNS Experiments
  - Use Stubby + Server of your choice
- TLS Cost Simulation
  - The Magic Number is roughly 8.
  - And, it depends. TLS optimization, cost assumptions
  - Future work: Better simulation (vary client behaviour), more precise cost factor estimation

nic.at GmbH

Jakob-Haringer-Str. 8/V · 5020 Salzburg · Austria

T +43 662 4669 -DW · F -29

alexander.mayrhofer@nic.at · **www.nic.at**

.at Domain Registry by nic.at · .versicherung by nic.at · RcodeZero DNS by nic.at · TLD Box by nic.at