December 5-9, 2022 • Austin, Texas, USA

ZeroDNS:

Towards Better Zero Trust Security using DNS

Levente Csikor

Sriram Ramachandran

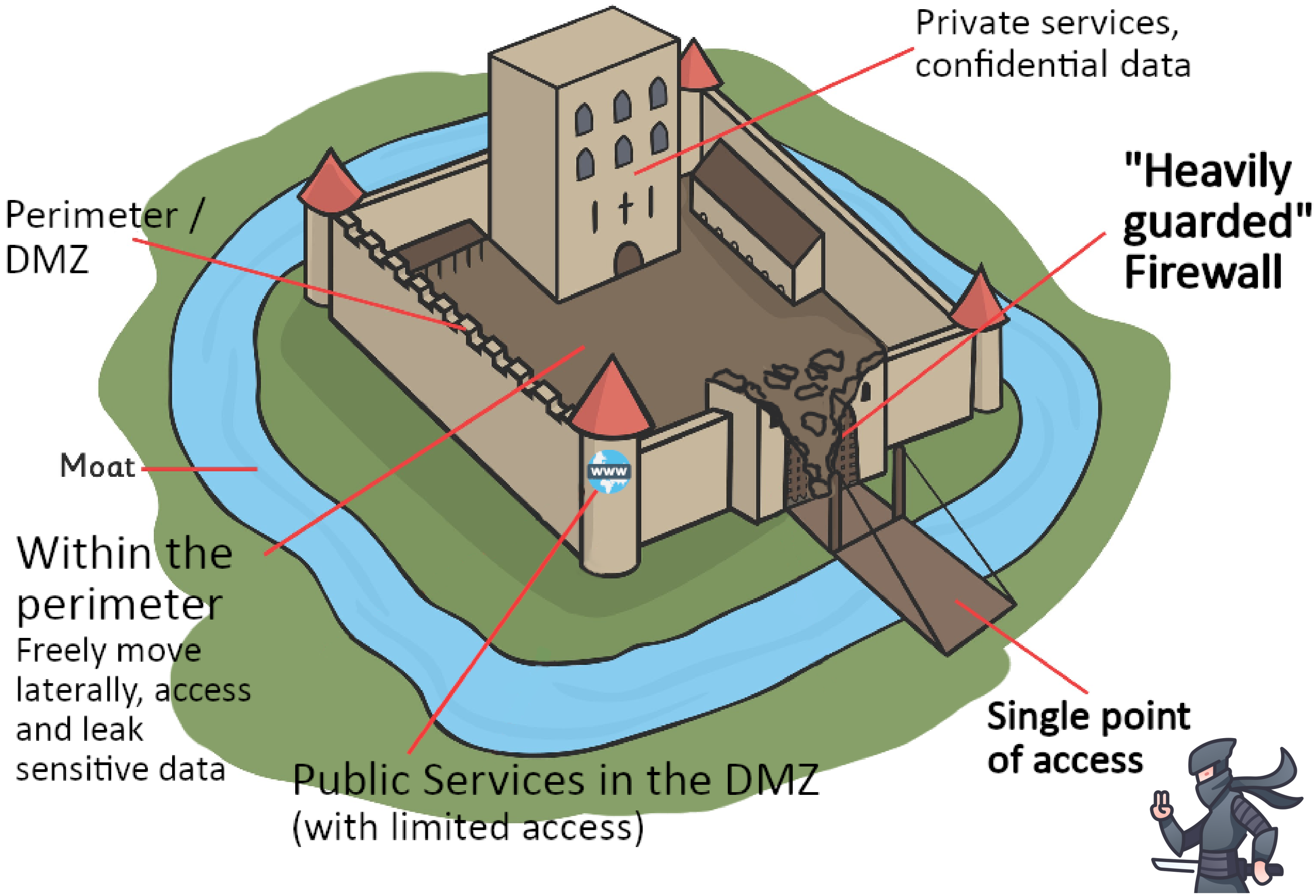
Anantharaman Lakshminarayanan

ARES PUBLIC

CREATING GROWTH, ENHANCING LIVES

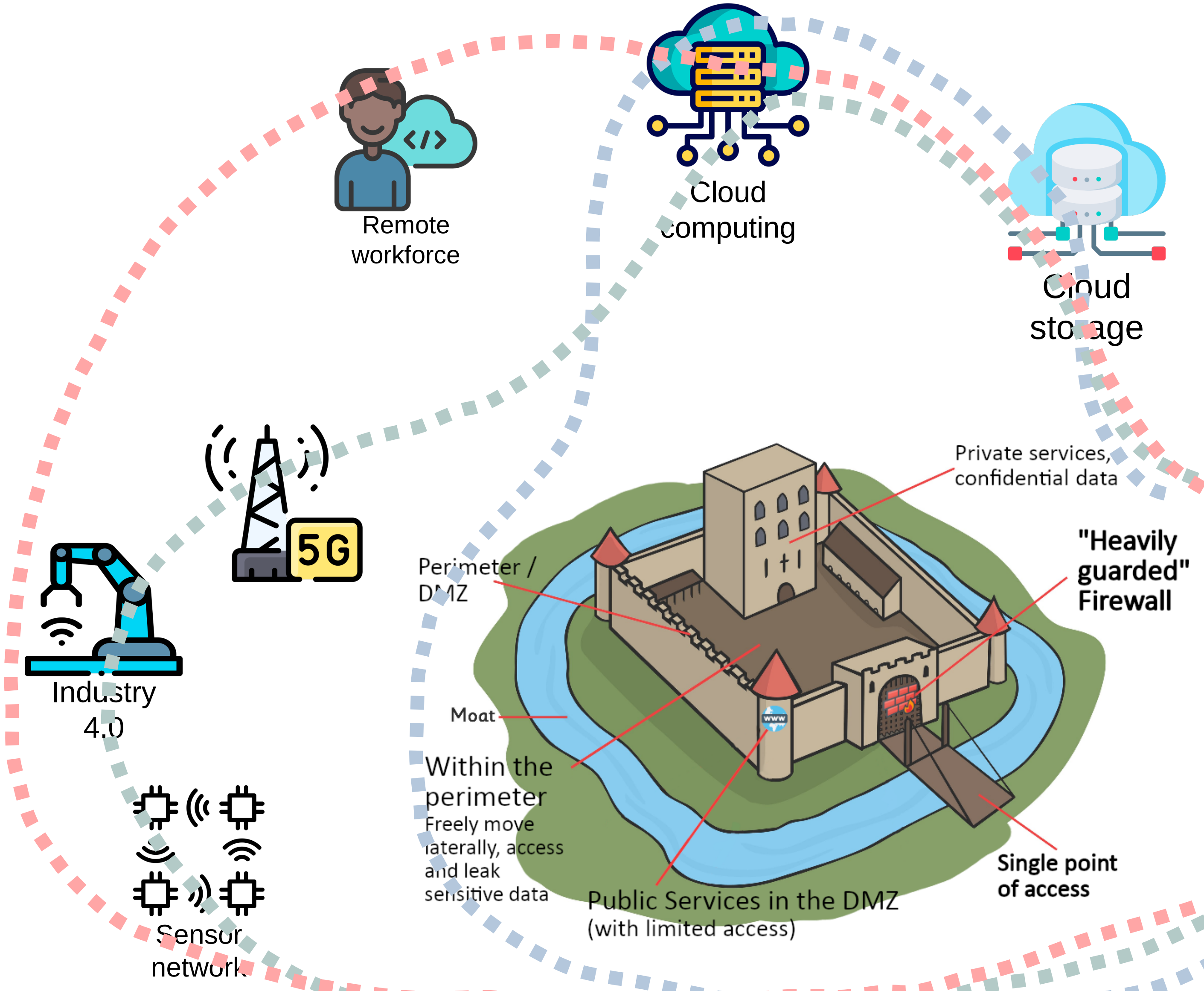
Traditional Perimeter-based Network Security

- **Similar to a medieval castle**
- **Perimeter strongly guarded**
- **Everything**
  - Inside is SAFE
  - Outside is DANGEROUS
- **Basically**
  - No access from outside unless authenticated
  - FULL access from inside
- **Severe flaw**
  - Once perimeter breached → adversaries can freely move laterally, access and leak sensitive data


Private services, confidential data
"Heavily guarded" Firewall
Perimeter / DMZ
Moat
www
Within the perimeter
Freely move laterally, access and leak sensitive data
Public Services in the DMZ (with limited access)
Single point of access

Perimeter-based model is getting OBSOLETE

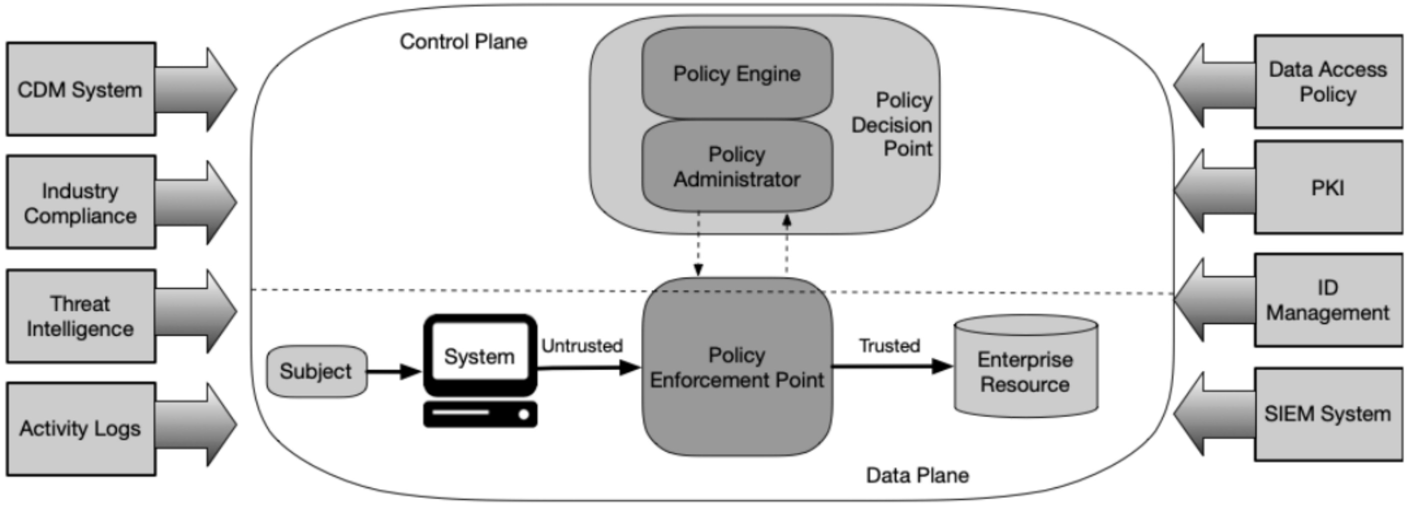
- **Perimeter definition is getting blurred**
- **Virtualization and cloud computing**
  - 23% of network is kept on-premise [1]
- **5G makes it "even worse"**
  - Massive deployment of enterprise (I)IoT devices, practically anywhere
- **Pandemic → remote workforce**
- **INTERNAL NETWORK ???**


Remote workforce
Cloud computing
Cloud storage
5G
Industry 4.0
Sensor network
Private services, confidential data
"Heavily guarded" Firewall
Perimeter / DMZ
Moat
Within the perimeter
Freely move laterally, access and leak sensitive data
Public Services in the DMZ (with limited access)
Single point of access

[1] A10 Networks. Jun 2022 [Accessed: Sep 2022]. Enterprise Perspectives 2022: Zero Trust, Cloud, and Remote Work Drive Digital Resiliency. Enterprise Report

Zero Trust – the state of the art

- **2014 – Google's BeyondCorp initiative**
- **REMOVE IMPLICIT TRUST FROM THE NETWORK → NEVER TRUST, ALWAYS VERIFY!**
- **Strong authentication**
  - X.509 certificates
  - Strong user credentials
- **Strong authorization**
  - Fine-grained access control
- **Strong encryption**
  - Transport Layer Security (TLS)



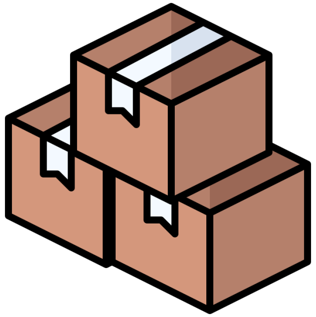
Core Zero Trust Logical Components according to NIST [2]

- **Several companies embraced the ZT architecture**
  - Cloudflare, Google, Microsoft, etc.

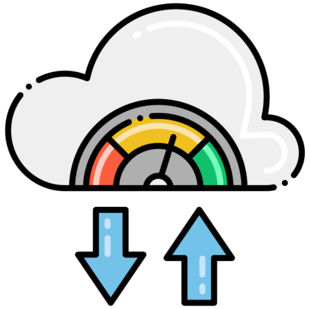
[2] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. Zero Trust Architecture. NIST Special Publication 800-207,https://doi.org/10.6028/NIST.SP.800-207.

Three problems regarding the deployment of ZT

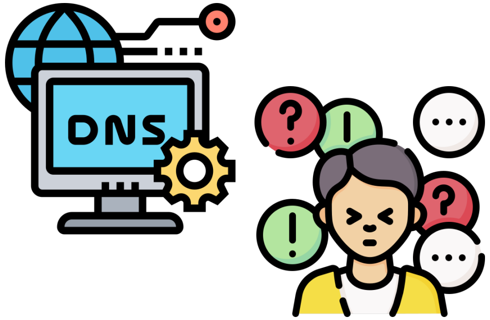
1) **Extra authorizations require new entities in the network**
   - Default routes can be affected, traffic engineering might be required, new entity can be a bottleneck or victim of a DoS attack, yet another server to maintain/traffic to monitor/set of logs to parse



2) **Increased Security → increased number of components/layers involved → more round-trips → increased communication overhead → increased *Time-To-First-Byte (TTFB)***



3) **DNS infrastructure is always left intact**
   - Usually unsecured by default
   - Critical role ↔ network operators are reluctant to interfere



ZeroDNS: Zero Trust in the DNS infrastructure

1) Extra authorizations require new entities in the network

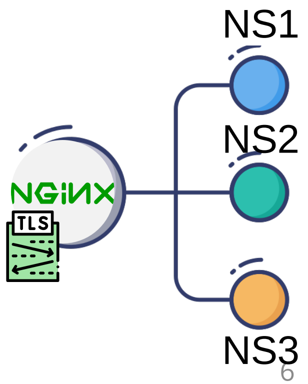
2) increased *Time-To-First-Byte (TTFB)*

3) DNS infrastructure is always left intact

1) New Zero Trust control plane component realized in the DNS infrastructure
   1) authN/authZ tokens distributed via DNS responses upon successful authentication

2) Piggybacking DNS packets to significantly reduce the required number of round-trips

3) Offload TLS termination
   1) + additional authentication via mTLS
   2) DNS back-end remains intact



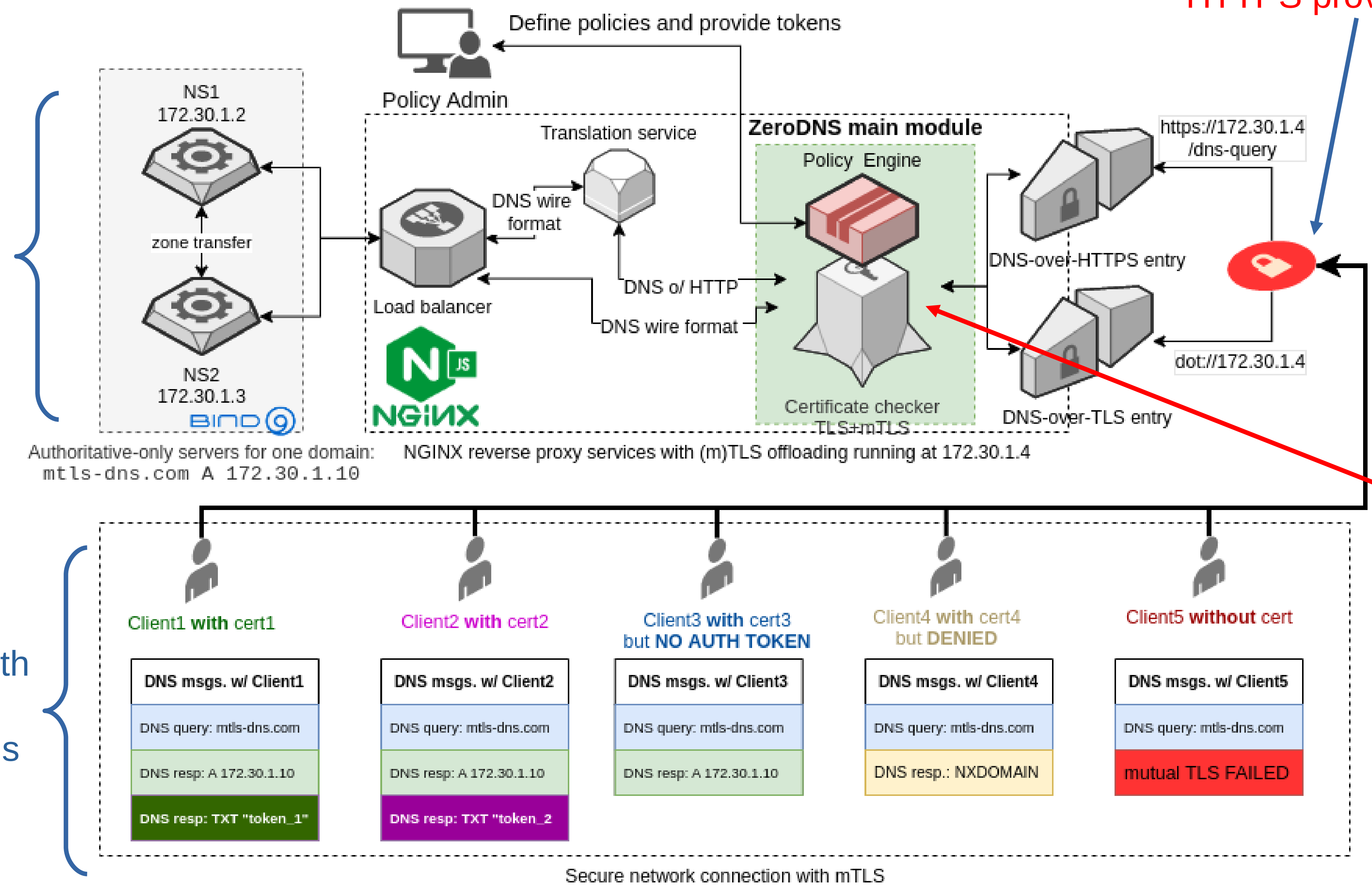
Levente Csikor, *"ZeroDNS: Towards Better Zero Trust Security using DNS"*, ACSAC, 2022

ZeroDNS: The Architecture

mTLS termination, DNS-over-TLS / DNS-over-HTTPS provision

Original DNS servers left intact

Clients with different credentials

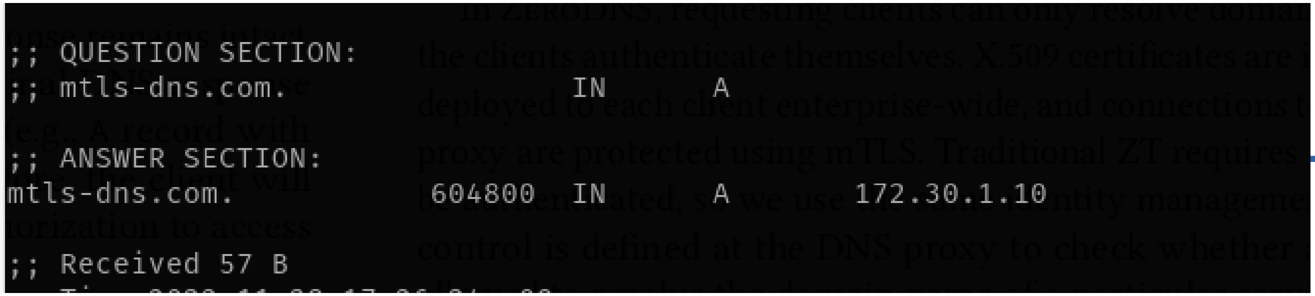


DNS msgs. w/ Client1	DNS msgs. w/ Client2	DNS msgs. w/ Client3	DNS msgs. w/ Client4	DNS msgs. w/ Client5
DNS query: mtls-dns.com	DNS query: mtls-dns.com	DNS query: mtls-dns.com	DNS query: mtls-dns.com	DNS query: mtls-dns.com
DNS resp: A 172.30.1.10	DNS resp: A 172.30.1.10	DNS resp: A 172.30.1.10	DNS resp.: NXDOMAIN	mutual TLS FAILED
DNS resp: TXT "token_1"	DNS resp: TXT "token_2			

Extend original DNS responses with authN/authZ tokens

Levente Csikor, *“ZeroDNS: Towards Better Zero Trust Security using DNS”*, ACSAC, 2022

ZeroDNS: Example communication

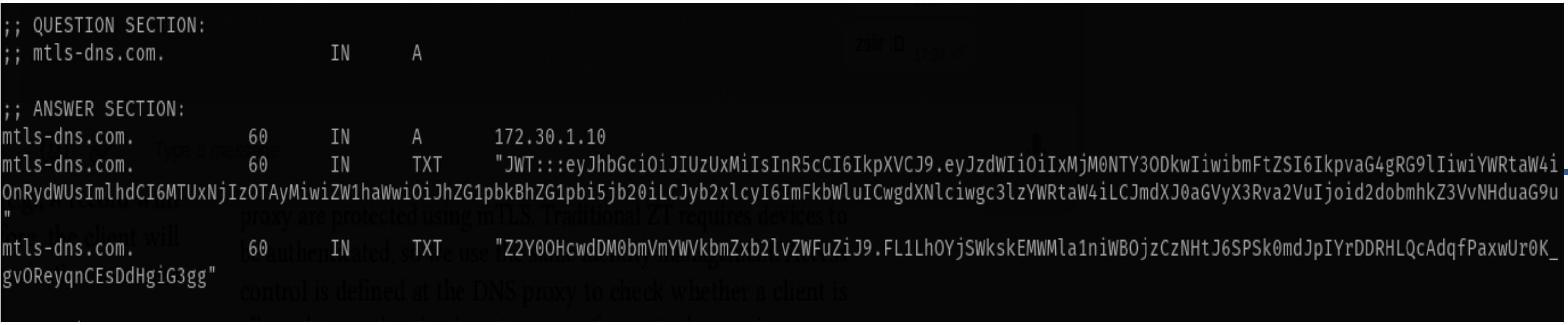


```
;; QUESTION SECTION:
;; mtls-dns.com.                IN      A

;; ANSWER SECTION:
mtls-dns.com.           604800  IN      A       172.30.1.10

;; Received 57 B
```

Client3 with cert3
but NO AUTH TOKEN

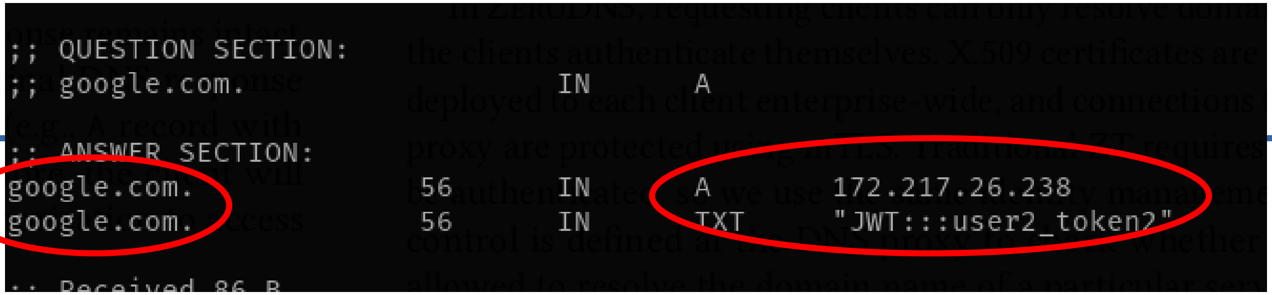


```
;; QUESTION SECTION:
;; mtls-dns.com.                IN      A

;; ANSWER SECTION:
mtls-dns.com.           60      IN      A       172.30.1.10
mtls-dns.com.           60      IN      TXT     "JWT:::eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4i
OnRydWUsImlhdCI6MTUxNjIzOTAyMiwiZW1haWwiOiJhZG1pbkBhZG1pbi5jb20iLCJyb2xlcyI6ImFkbWluICwgdXNlciwgc3lzYWRtaW4iLCJmdXJ0aGVyX3Rva2VuIjoid2dobmhkZ3VvNHduaG9u
"
mtls-dns.com.           60      IN      TXT     "Z2Y0OHcwdDM0bmVmYWVkbmZxb2lvZWFuZiJ9.FL1LhOYjSWkskEMWMla1niWBOjzCzNHtJ6SPSk0mdJpIYrDDRHLQcAdqfPaxwUr0K_
gvOReyqnCEsDdHgiG3gg"
```

Client2 with cert2

Arbitrary extension to any response



```
;; QUESTION SECTION:
;; google.com.                  IN      A

;; ANSWER SECTION:
google.com.             56      IN      A       172.217.26.238
google.com.             56      IN      TXT     "JWT:::user2_token2"

;; Received 86 B
```

Client2 with cert2

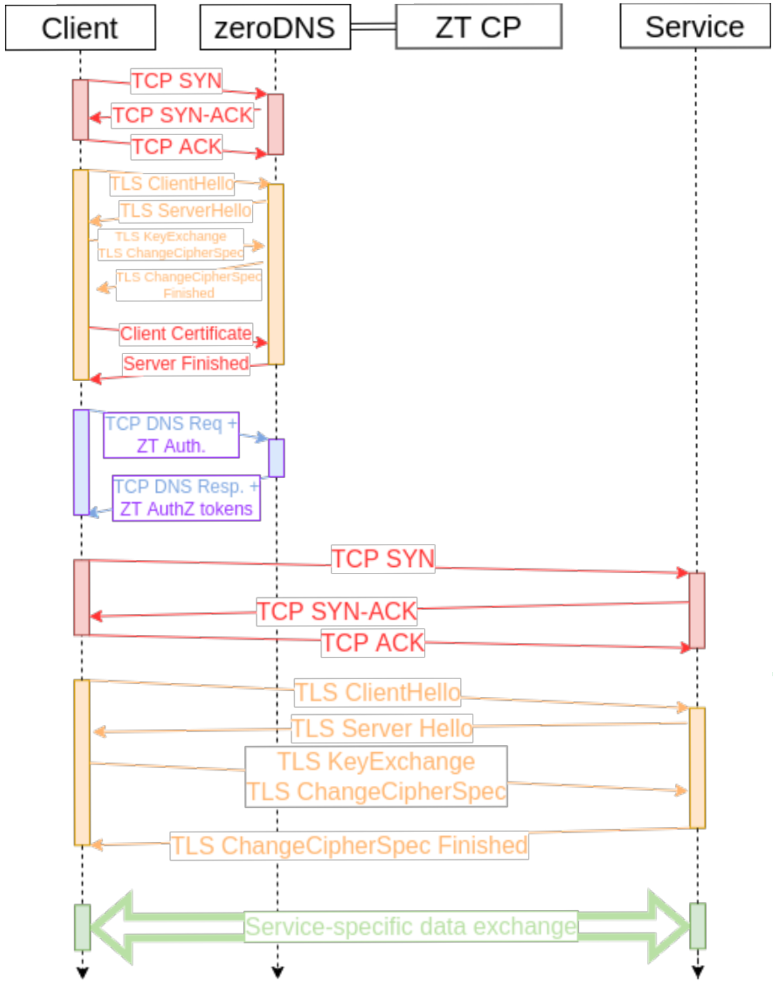
Levente Csikor, *"ZeroDNS: Towards Better Zero Trust Security using DNS"*, ACSAC, 2022

ZeroDNS: Benefits

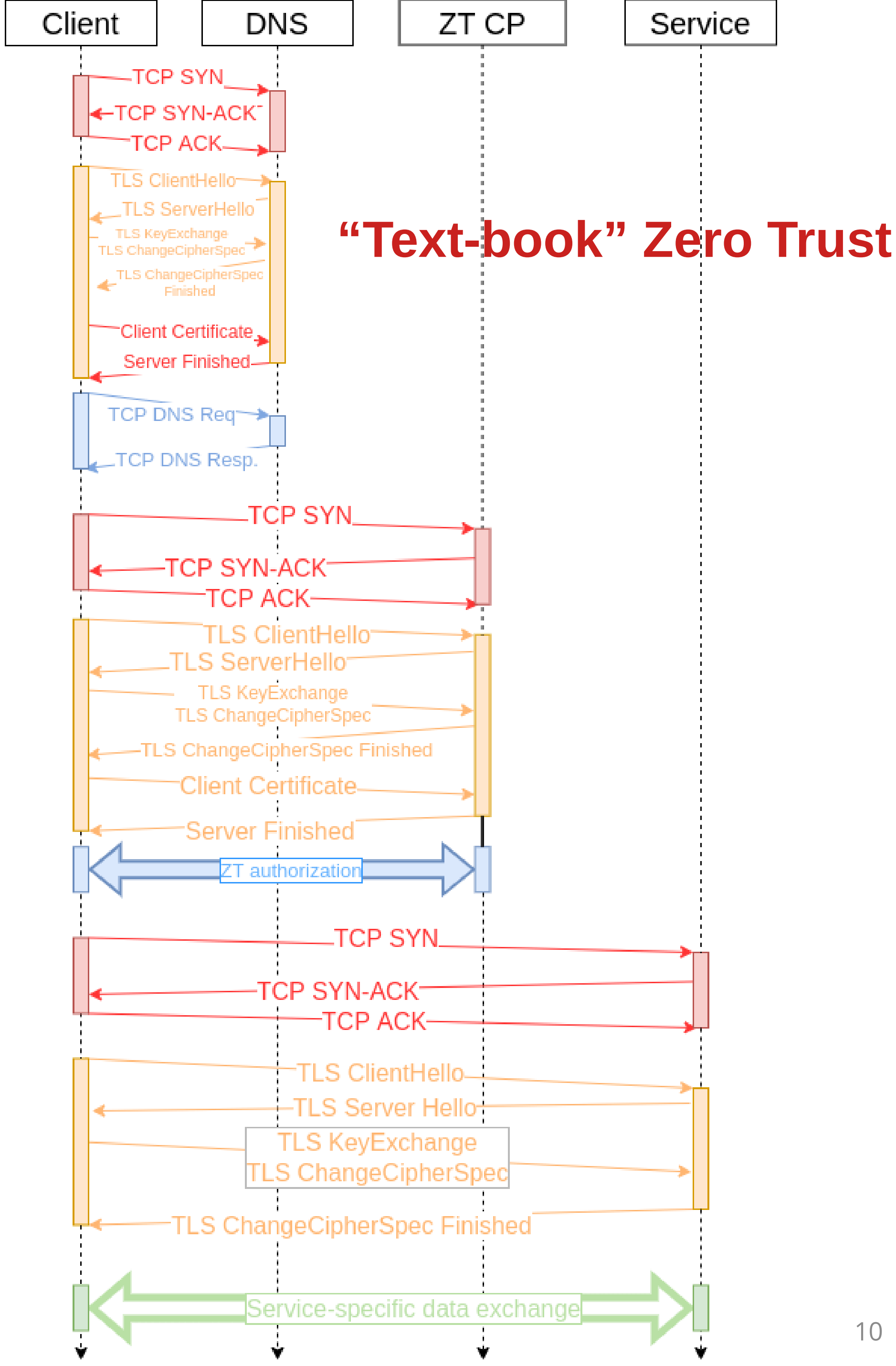
- **Minimal modification to existing infrastructure**
  - Add NGINX plugin, reconfigure DHCP to advertise it as DNS (instead of the original DNS)
- **Reduced Zero Trust bottleneck**
  - NGINX is a load-balancer by default → better resource utilization, maximized throughput, reduced latency, simple scale-out of back-ends w/o complex certificate management
  - Piggybacking DNS traffic → no extra (type of) traffic
- **Being true to Zero Trust**
  - DNS with mTLS → clients cannot resolve a domain name unless authenticated themselves
- **Offloading TLS processing**
- **DNS back-end server implementation-agnostic**
  - ZeroDNS only requires a nameserver to proxy the queries to and responses from

ZeroDNS: Benefits (cont'd)

- **Reduced TTFB (Time-to-first-byte)**

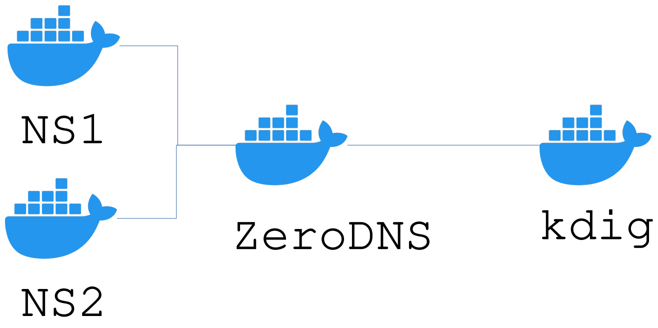


Almost identical to *non-Zero Trust* access with encrypted DNS



Levente Csikor, *"ZeroDNS: Towards Better Zero Trust Security using DNS"*, ACSAC, 2022

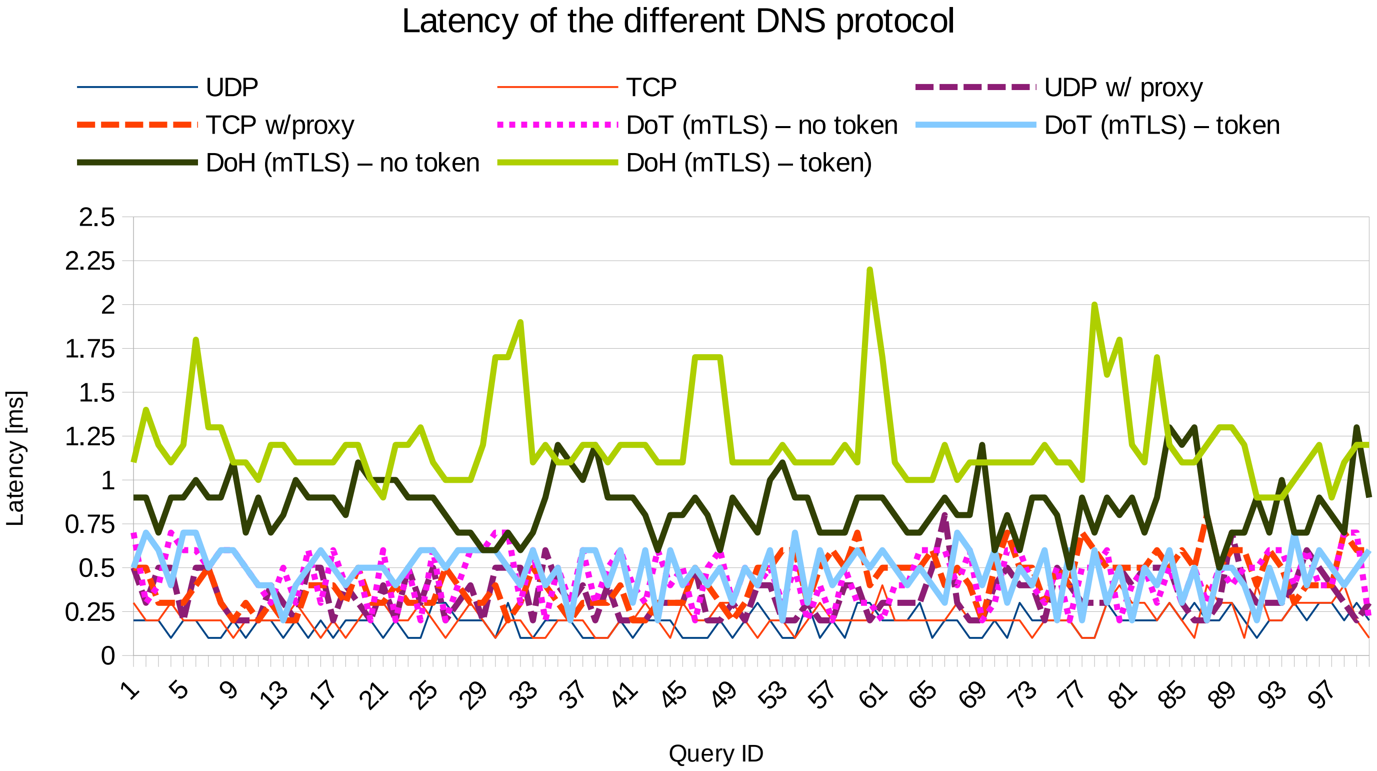
ZeroDNS: Evaluation



- **`kdig` command line utility - supports mTLS**
  - Connection established from scratch each time (worst-case performance measured)
  - 100 consecutive queries sent to the DNS server / zeroDNS NGINX plugin → *relatively low QPS*
- **Measured: Response times of each protocol**
  - Optimized code since paper submission
    - Better average results obtained

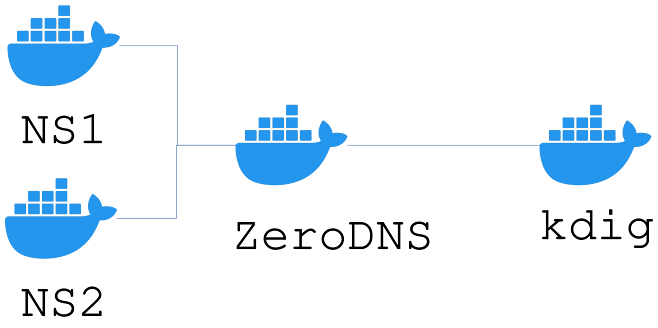
UDP	0.185 ms
TCP	0.215 ms
UDP w/ proxy	0.347 ms
TCP w/ proxy	0.421 ms
DoT w/ proxy (no token)	0.447 ms
DoT w/ proxy (token)	0.476 ms
DoH w/ proxy (no token)	0.852 ms
DoH w/ proxy (token)	1.207 ms

Code execution involved (e.g., packet parsing)


Latency of the different DNS protocol

Levente Csikor, *“ZeroDNS: Towards Better Zero Trust Security using DNS”*, ACSAC, 2022

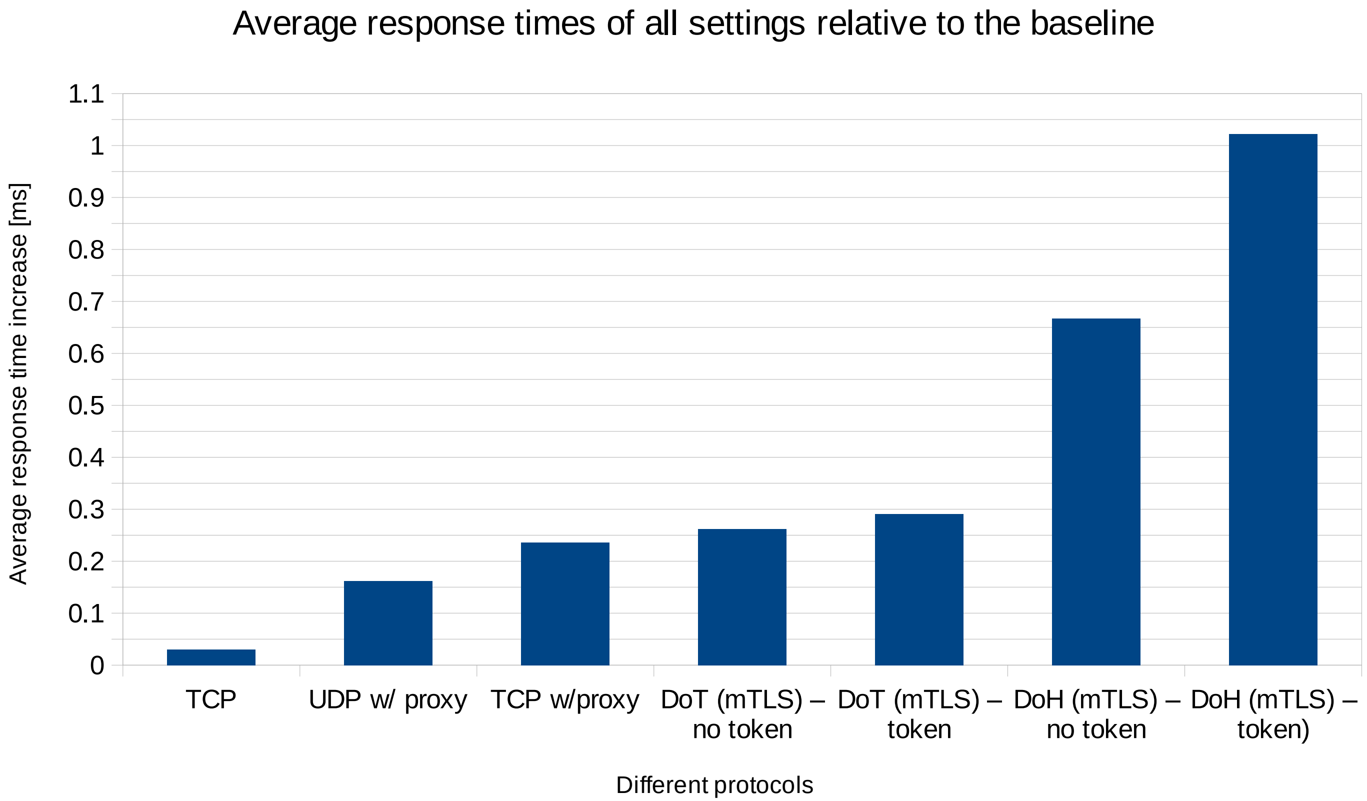
ZeroDNS: Evaluation



- `kdig` **command line utility - supports mTLS**
  - Connection established from scratch each time (worst-case performance measured)
  - 100 consecutive queries sent to the DNS server / zeroDNS NGINX plugin → *relatively low QPS*
- **Measured: Average response times of each protocol relative to the baseline**
  - Baseline: unencrypted UDP w/o proxy
  - Optimized code since paper submission
    - Better average results obtained

UDP	BASELINE
TCP	+ 0.03 ms
UDP w/ proxy	+ 0.162 ms
TCP w/ proxy	+ 0.236 ms
DoT w/ proxy (no token)	+ 0.262 ms
DoT w/ proxy (token)	+ 0.291 ms
DoH w/ proxy (no token)	+ 0.667 ms
DoH w/ proxy (token)	+ 1.022 ms

Code execution involved (e.g., packet parsing)



Levente Csikor, "ZeroDNS: Towards Better Zero Trust Security using DNS", ACSAC, 2022

CREATING GROWTH, ENHANCING LIVES

Conclusion

- **Traditional perimeter-based network security model is obsolete**
  - Hard to define perimeter → cannot assume that everything inside a network is safe anymore
- **New Zero Trust (ZT) paradigm removes the implicit trust in the network**
  - Strong authentication, strong authorization, strong encryption → Never trust, always verify!
- **Typical security trade-off: better security → more layers → impact on speed**
- **ZeroDNS: to overcome *three main practical issues* of ZT deployments**
  1) Extend Zero Trust principles to the critical DNS infrastructure → authenticate DNS queries
  2) Offload Zero Trust control plane functions to the DNS → authZ/authN tokens distributed via DNS
  3) Reduce the number of networking elements → reduced number of round-trips → reduced TTFB
- **ZeroDNS introduces negligible overhead**
  - Less than `0.3 ms` additional computational latency (in the case of DNS-over-TLS)
  - If NGINX is deployed already: less than `0.03 ms` additional latency
    - DNS-over-HTTPS involves more processing due to HTTP → DNS translation (`+ ~1 ms`)

ZeroDNS: Discussion and Future Work

- **ZeroDNS replaces the ZT control plane ONLY**
  - Zero Trust data plane components, i.e., Policy Enforcement Points, are still needed
- **Multiple services behind the same domain name / IP address**
  - `https://example.com/api/v1/update` ↔ `https://example.com/staff-portal/`
  - Utilize EDNS extension (OPT RR) in the query to indicate the service
- **ZeroDNS is transparent**
  - Non-enterprise domains are still resolved as usual
- **ZeroDNS is resilient against replay attacks**
  - mTLS ensures that traffic is secure and trusted in both directions between client and ZeroDNS
- **Bypassing ZeroDNS and use plain-text back-end servers for domain resolution?**
  - ZeroDNS requires back-end servers to accept queries only from ZeroDNS
- **Denial-of-service attacks**
  - Response time of ZeroDNS can be increased by sending tens of thousands of queries per second
  - However, queries must be authenticated (due to mTLS) → simple detection and filtering can be applied
- **ZeroDNS concept can be realized with other systems: HAProxy, Traefik, etc.**

CREATING GROWTH, ENHANCING LIVES

Institute for
Infocomm Research

I²R

MEMORIES
FOR THE
FUTURE
2002 - 2022

THANK YOU

www.a-star.edu.sg

Levente Csikor

Some slides have been designed using images from Flaticon.com