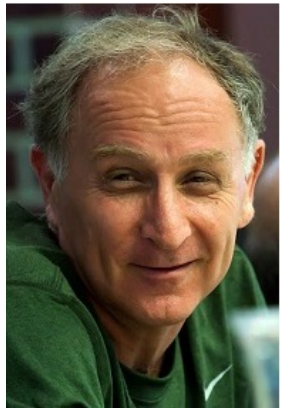
AdaDoQ: Adaptive DNSSEC



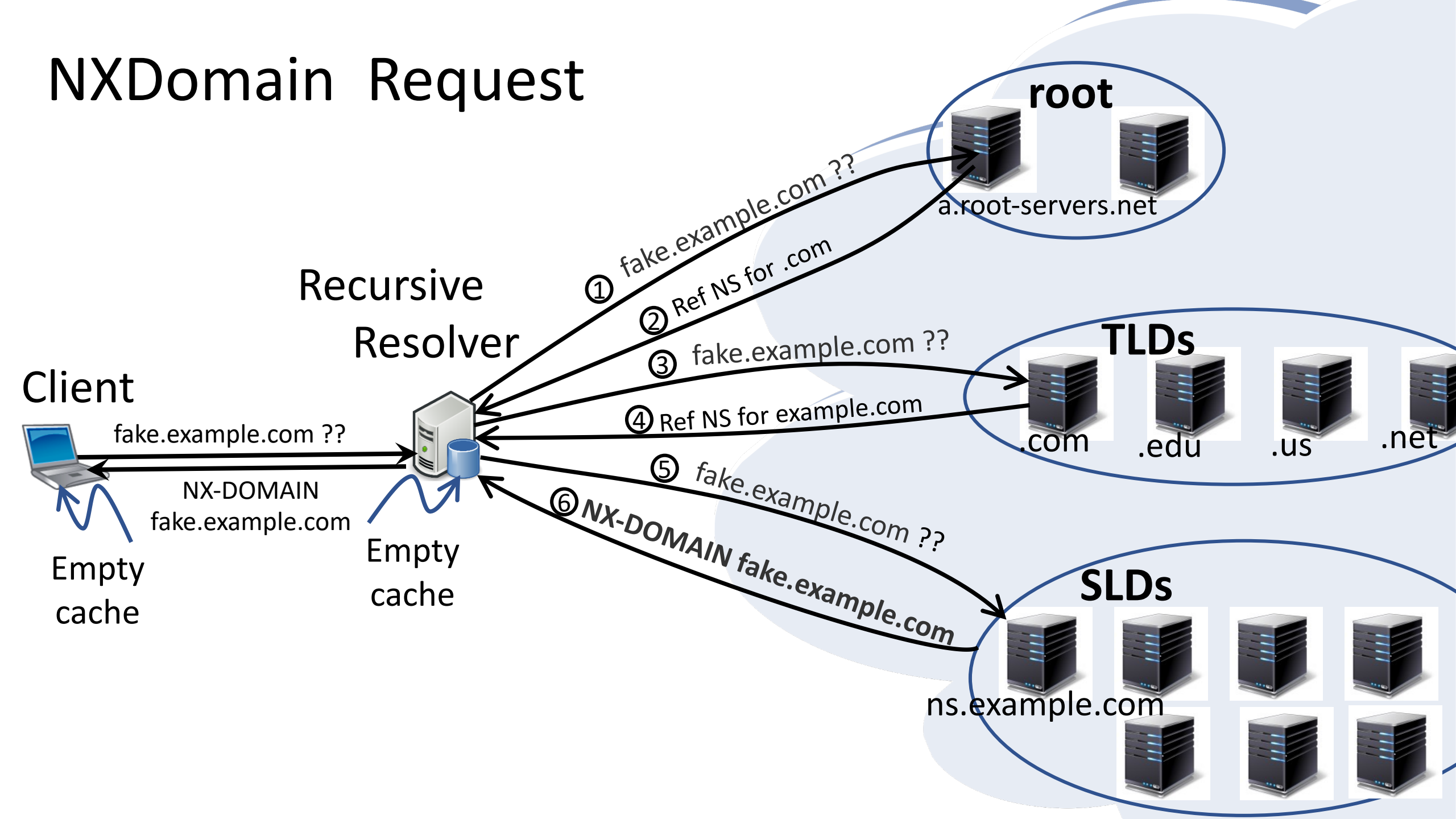
Yehuda Afek
Tel-Aviv University

Anat Bremler-Barr
Reichman University

Daniel Dubnikov
Tel-Aviv University

Supported By:

NXDomain Request



NXDomain Attack

RANDOM DNS Request Flood

Rxy1xhggsgVCER.sony.com

XVBY$&HGDRxy2.sony.com

FJH*^DHGAKRxy3.sony.com

RxUYQVMNLKAy4.sony.com

Resolvers

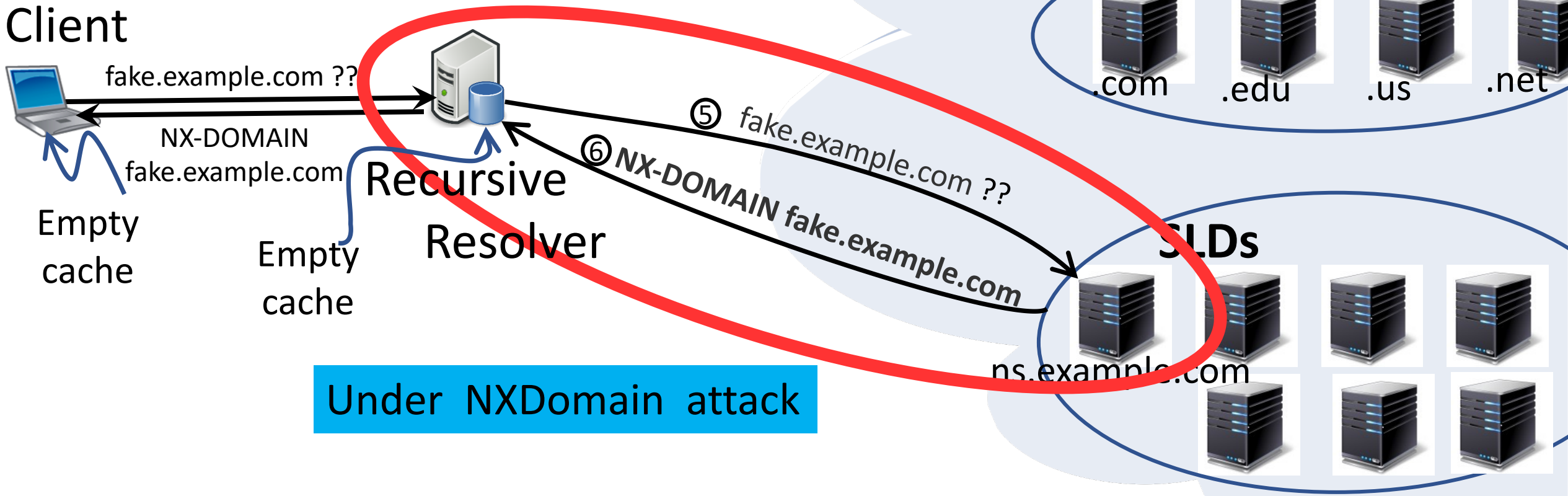
.com

ns.sony.com

RzHW$RE43CBJs$7.sony.com

With DNSSEC

	Max Queries Per Second
Plain DNS	23,524
DNSSEC: NSEC	9,510
DNSSEC: NSEC3	8,989



Motivation

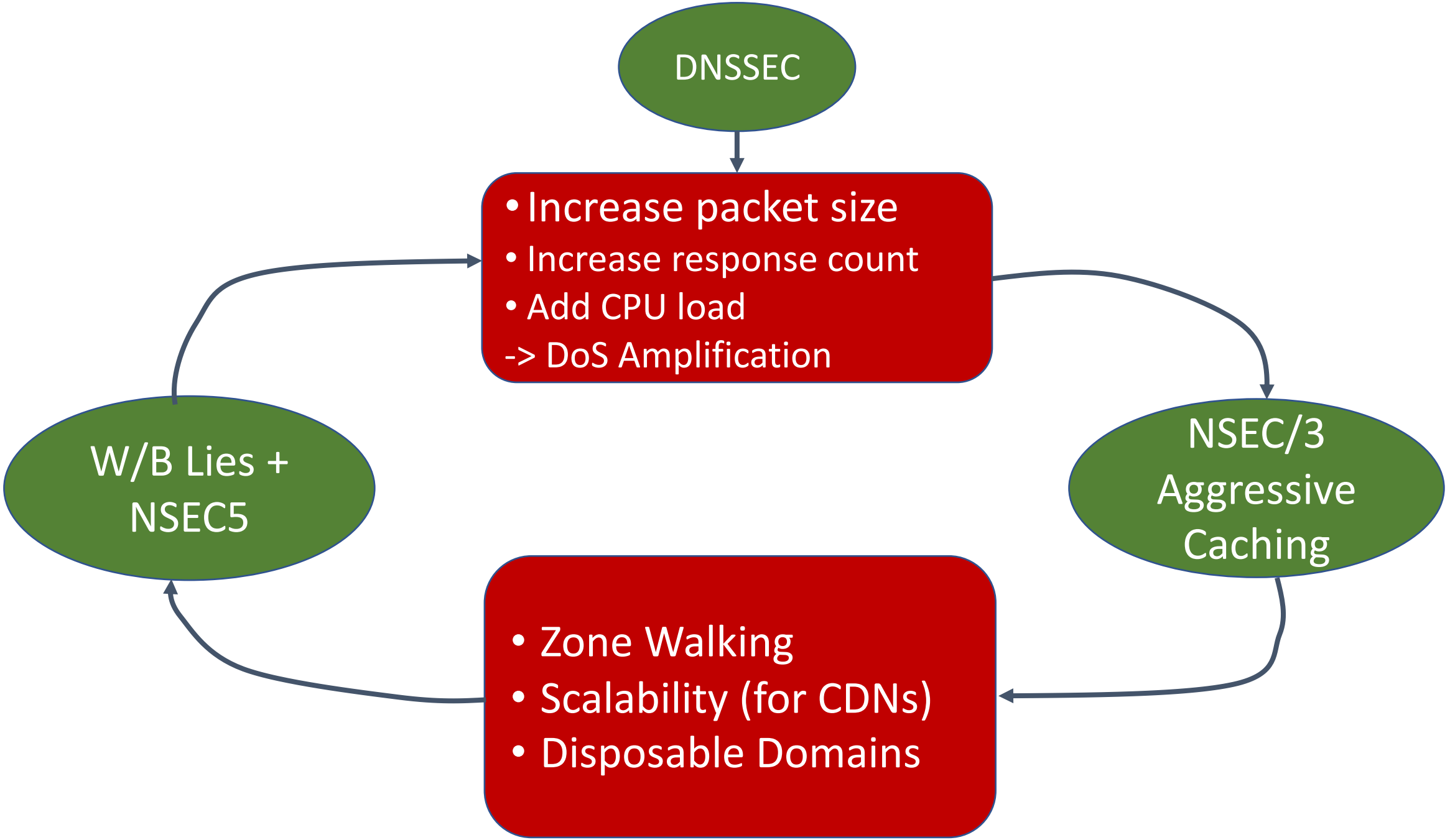
- DNSSEC is important
- DNS with DNSSEC does not scale, specifically,

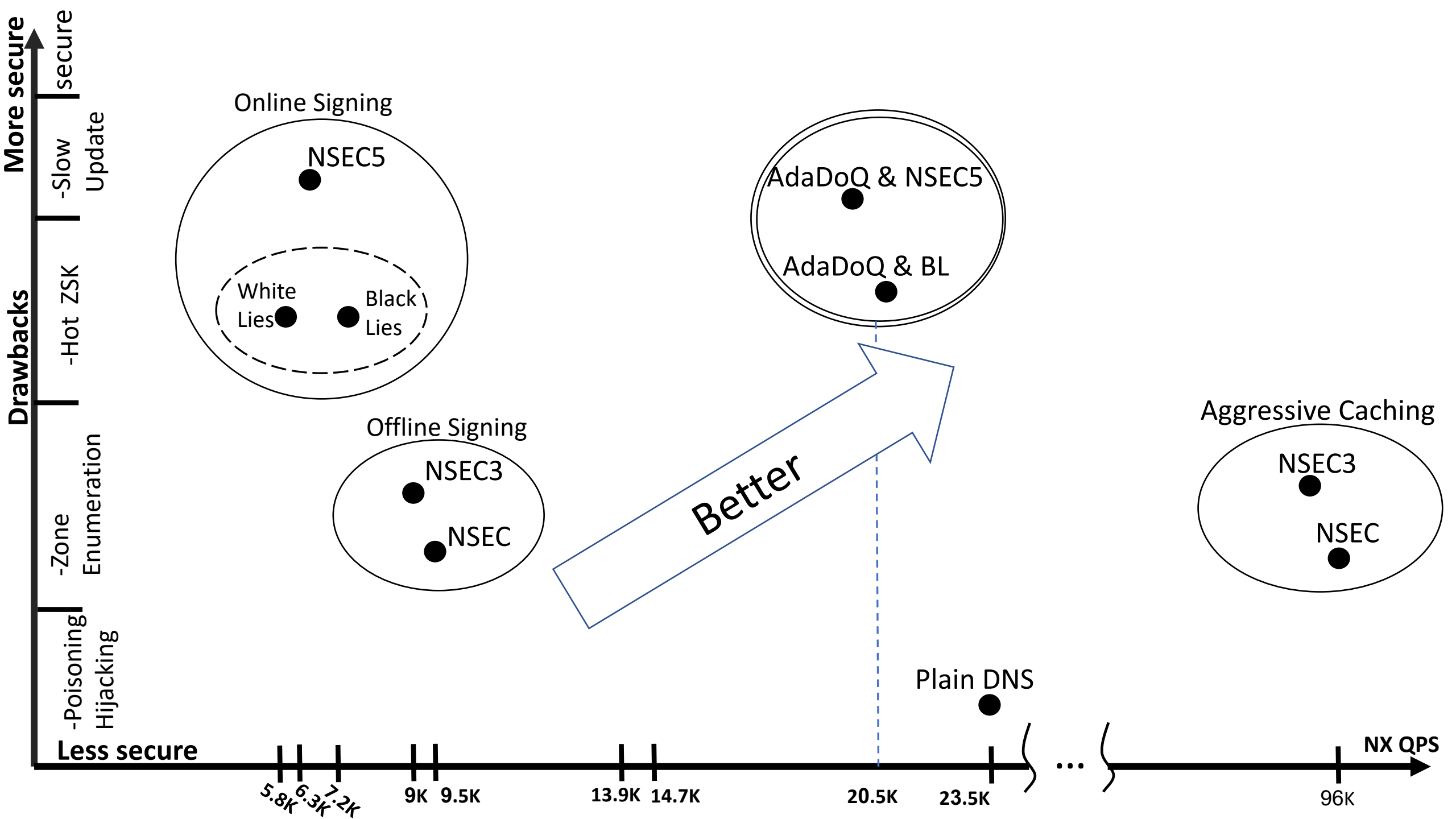
  ➔Vulnerable to NXDomain flood attacks

Goal

1. To measure DNSSEC scalability relative to Plain DNS
2. Develop a method for <resolver ←→ authoritative> collaboration that is (a) Scalable, (b) as secure as DNSSEC, and (c) introduces no new vulnerabilities.

   a. Provides the same security level as DNSSEC, and
   b. Provides performances close to that of Plain-DNS, and
   c. Does not enable new vulnerabilities.


DNSSEC
• Increase packet size
• Increase response count
• Add CPU load
-> DoS Amplification
NSEC/3 Aggressive Caching
• Zone Walking
• Scalability (for CDNs)
• Disposable Domains
W/B Lies + NSEC5


More secure
secure
-Slow Update
-Hot ZSK
Drawbacks
-Zone Enumeration
-Poisoning Hijacking
Less secure
Online Signing
NSEC5
White Lies
Black Lies
Offline Signing
NSEC3
NSEC
AdaDoQ & NSEC5
AdaDoQ & BL
Better
Aggressive Caching
NSEC3
NSEC
Plain DNS
...
NX QPS
5.8K
6.3K
7.2K
9K
9.5K
13.9K
14.7K
20.5K
23.5K
96K

Conclusions

- DNSSEC degrades DNS performance
  - Make NXDOMAIN attacks worse (DDoS amplification)
- AdaDoQ – Hybrid Solution
  - Light and fast connections
  - One time encryption overheads
  - Close to Plain DNS throughput
  - No Security Compromises
    - No Zone Walking
  - No Scalability Issues

Questions?