A Flushing Attack on the DNS Cache

Shoham Danino

Reichman University

Yehuda Afek

Tel-Aviv University

Anat Bremler-Barr

Tel-Aviv University

Yuval Shavitt

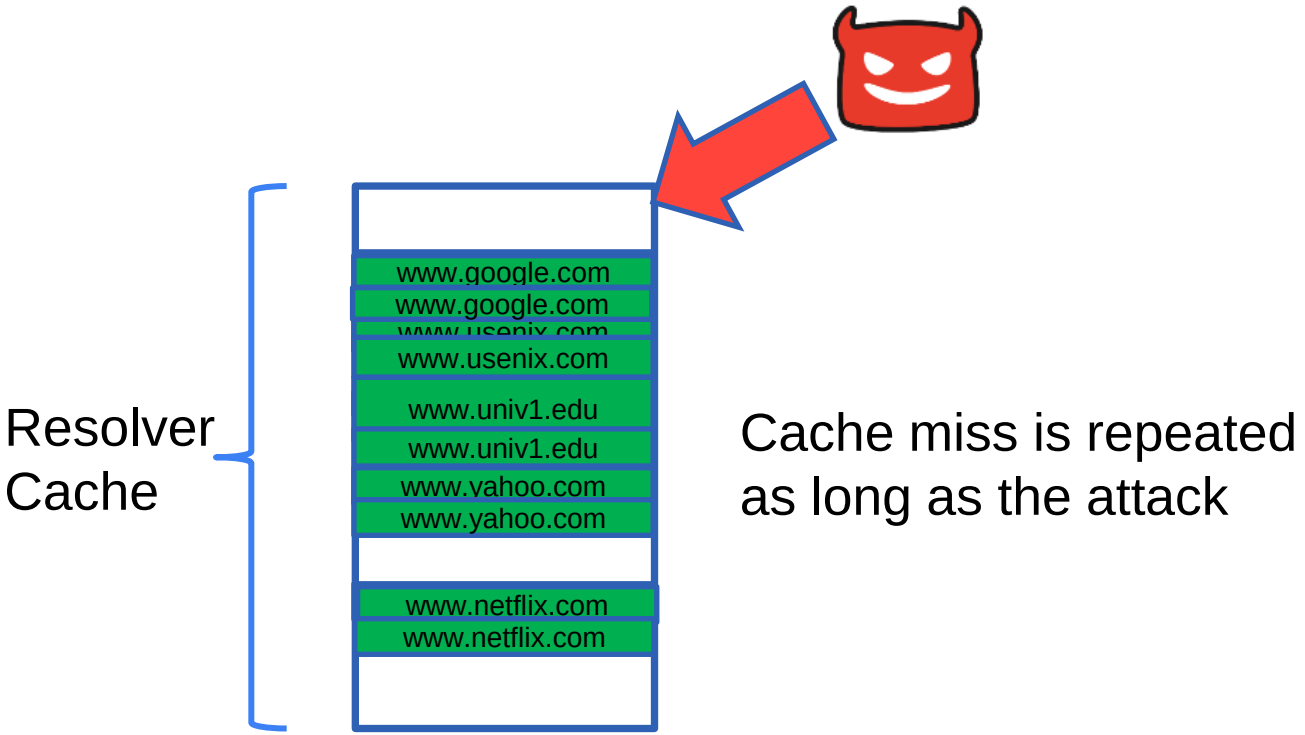
Tel-Aviv University

Flushing Attack on the DNS Cache

Unique new attack on DNS Resolvers

- **DDoS** on the resolver **cache**
  - Previous DDoS DNS attacks were: Communication (packet amplification) or CPU load(Complexity)
  - Cache is a key factor in the performance of DNS
- on the **benign** cache
  - (as opposed to the Ncache - Negative Cache)
- Malicious clients send small requests to malicious authoritative servers that repeatedly inject HUGE answers that are stored into the cache

What is attack on the DNS Cache?



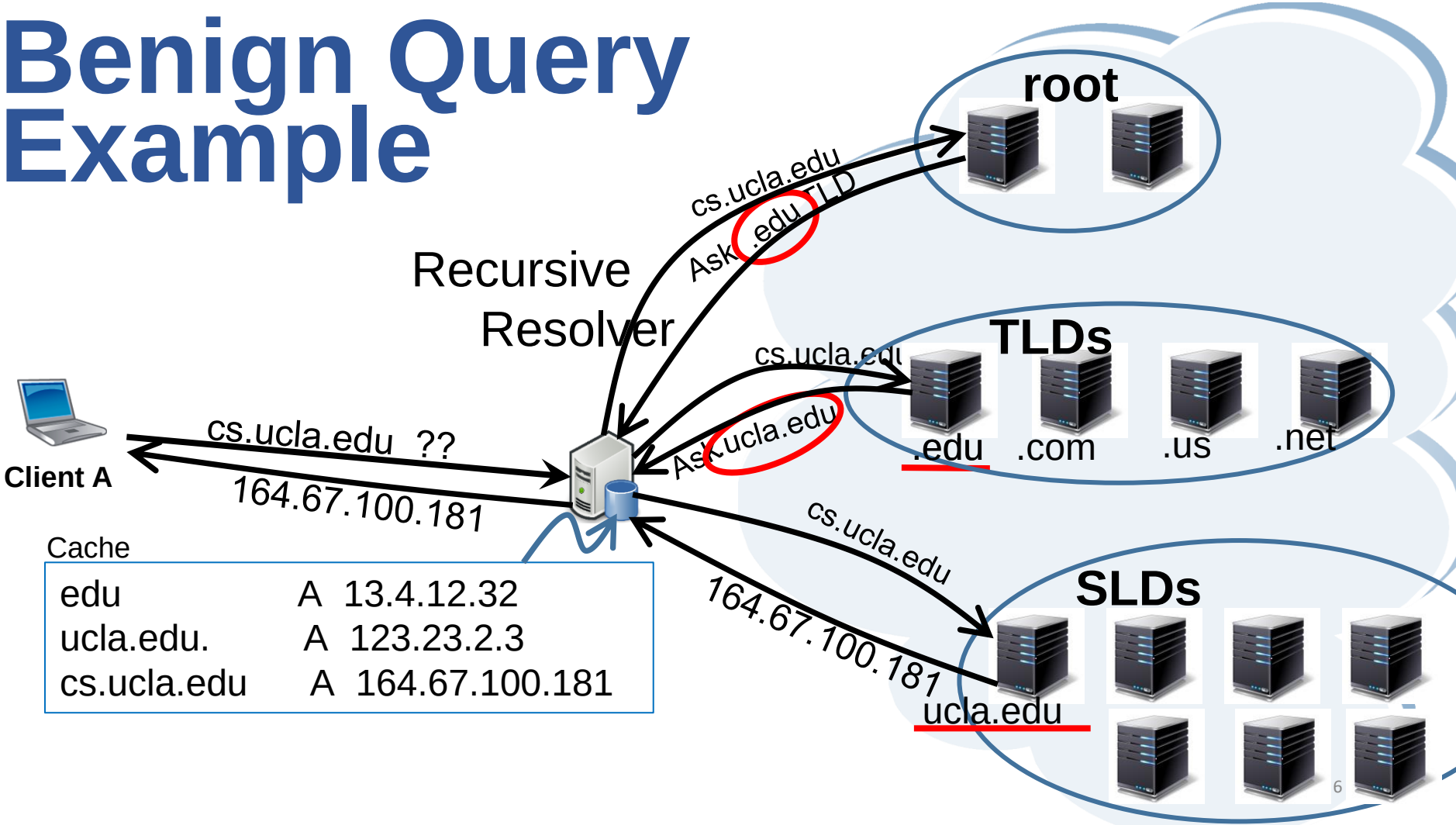
Flushing the DNS Cache

Flushing Attack on the DNS Cache

- **We show in the paper two versions of the attack:**
  - **CacheFlushNS attack**
    - 1 malicious request ~**1500**X records in the benign cache
  - **CacheFlush CNAME attack**
    - 1 malicious request ~**17**X records in the benign cache

DNS Preliminaries

Benign Query Example

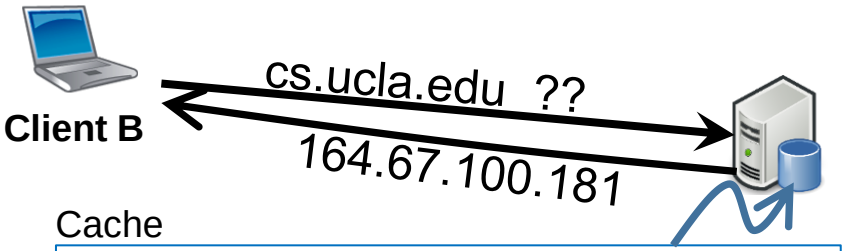


Cache

edu	A	13.4.12.32
ucla.edu.	A	123.23.2.3
cs.ucla.edu	A	164.67.100.181

Benign Query Example

Recursive Resolver



Cache

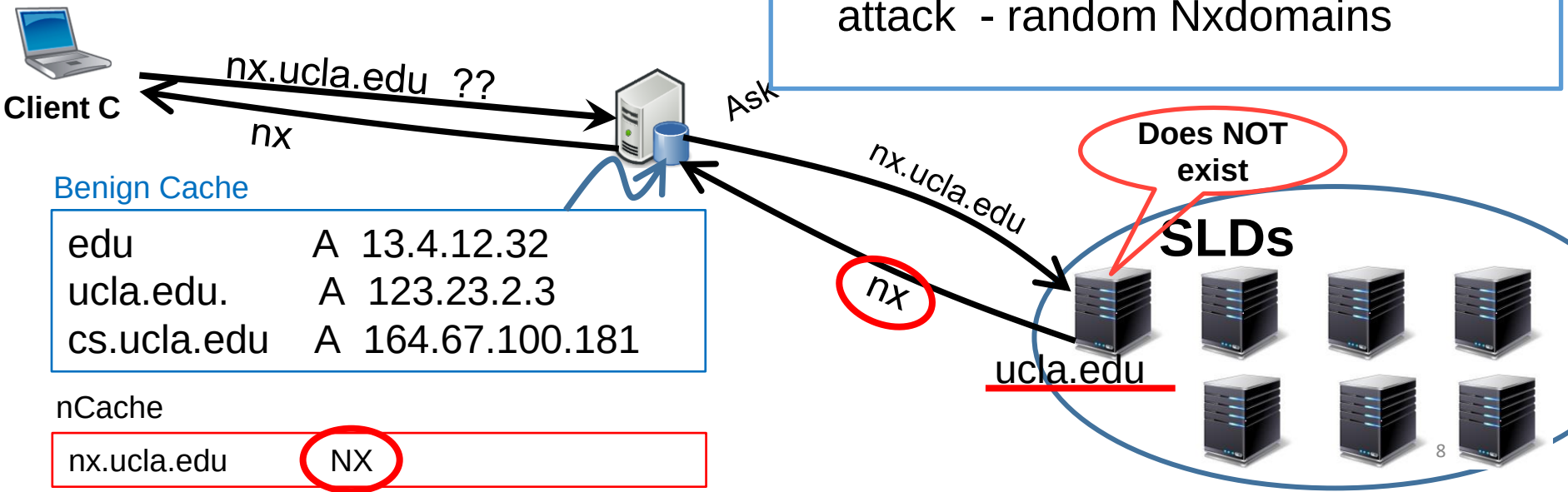
edu	A	13.4.12.32
ucla.edu.	A	123.23.2.3
cs.ucla.edu	A	164.67.100.181

Cache:

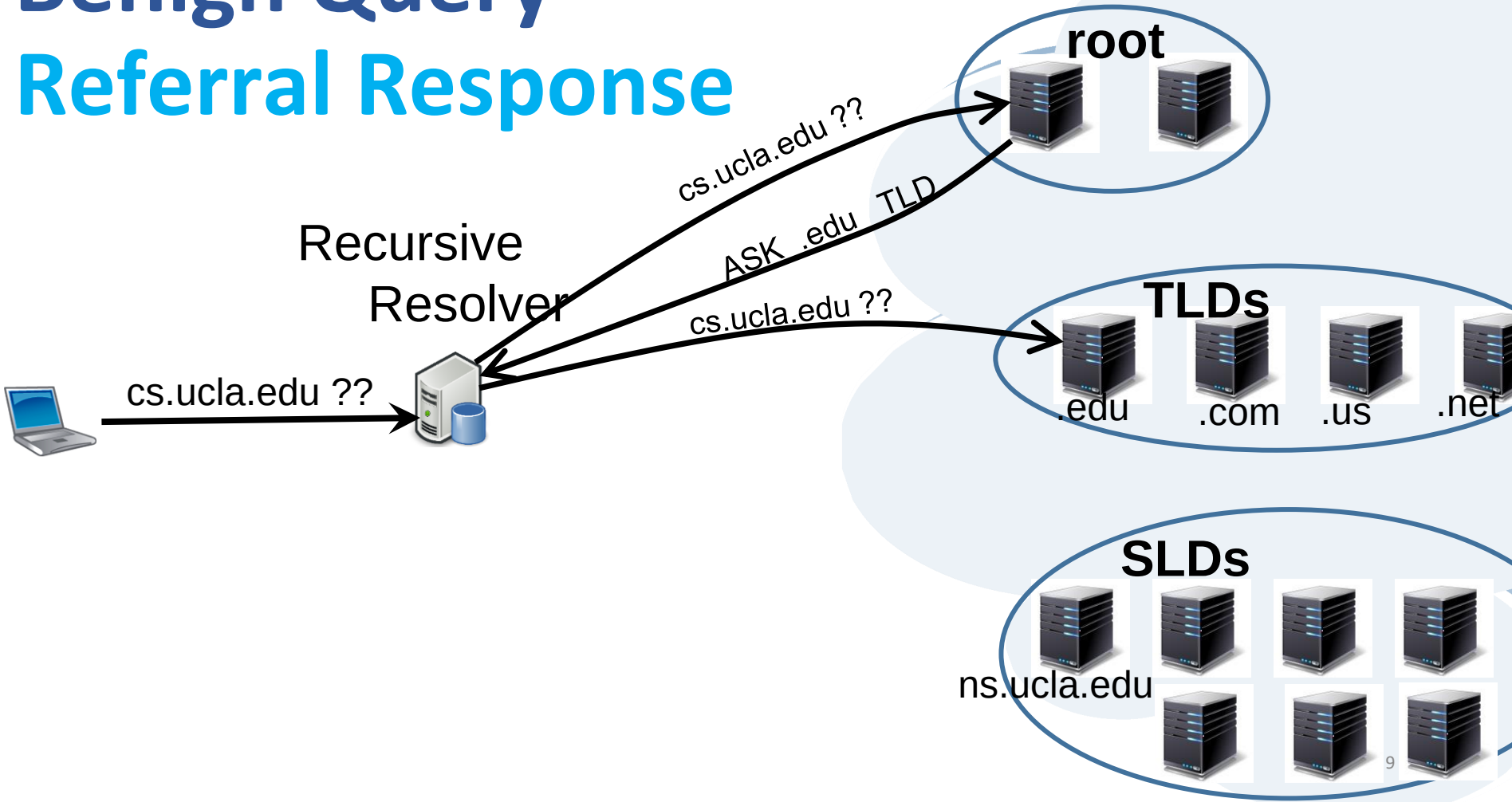
- Crucial for resolver efficiency (throughput).
- Essential for delivering low-latency responses to clients.

nCache
Non-eXsistnet (NX) Domains

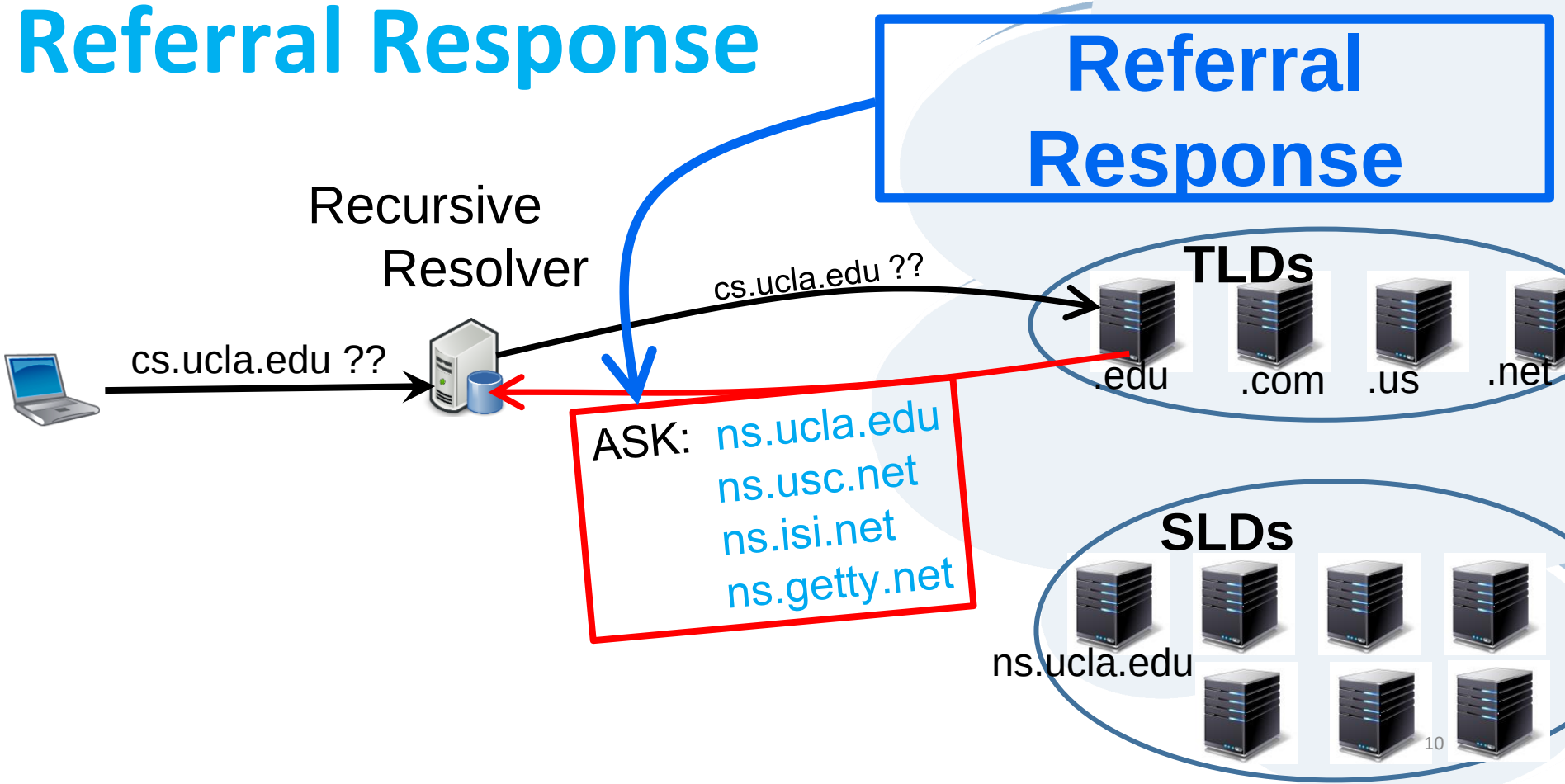
nCache:
- Sperate cache for non-existent
- Important against Water torture attack - random Nxdomains



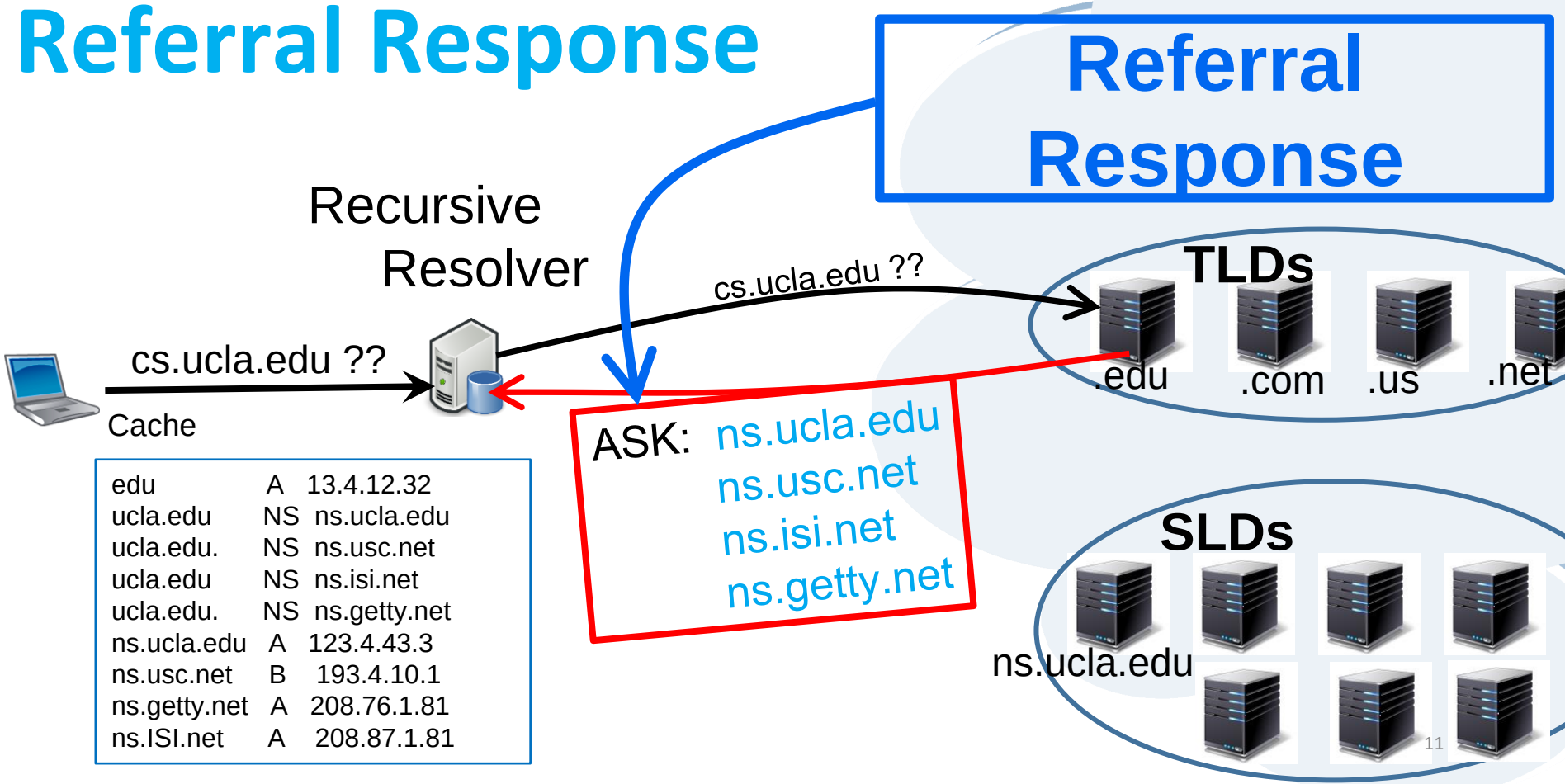
Benign Query – Referral Response



Benign Query – Referral Response



Benign Query – Referral Response



edu	A	13.4.12.32
ucla.edu	NS	ns.ucla.edu
ucla.edu.	NS	ns.usc.net
ucla.edu	NS	ns.isi.net
ucla.edu.	NS	ns.getty.net
ns.ucla.edu	A	123.4.43.3
ns.usc.net	B	193.4.10.1
ns.getty.net	A	208.76.1.81
ns.ISI.net	A	208.87.1.81

CacheFlushNS Attack

CacheFlushNS attack

Referral Response

Recursive Resolver

e1.attack.com??

NX

ASK: X1.delegation.attack
X2.delegation.attack
…
X1500.delegation.attack

1500

attack.com

delegation.attack

Cache

e1.attack.com NS x1.delegation.attack
e1.attack.com NS x2.delegation attack
…
e1.attack.com NS x1500.delegation.attack

x1.delegation.attack A 1.3.2.4
…
x20.delegation.attack A 7.8.9.20

1500

delegation attack ?

x1.delegation.attack A 1.3.2.4

20

. . .

x20.delegation.attack ?

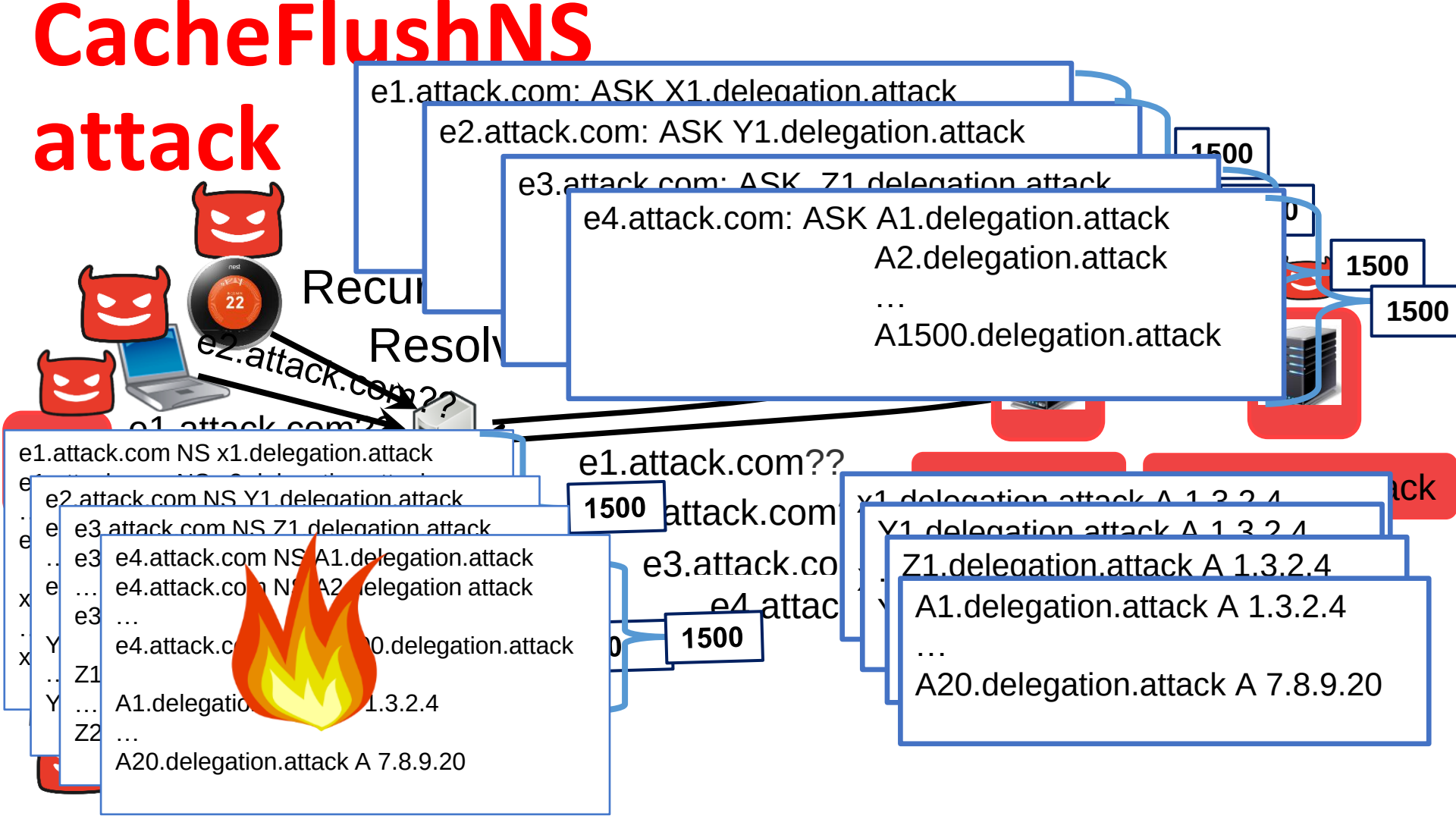
x20.delegation.attack A 7.8.9.20

NS limit 20
NXNSAttack 2000
To prevent Packet amplification

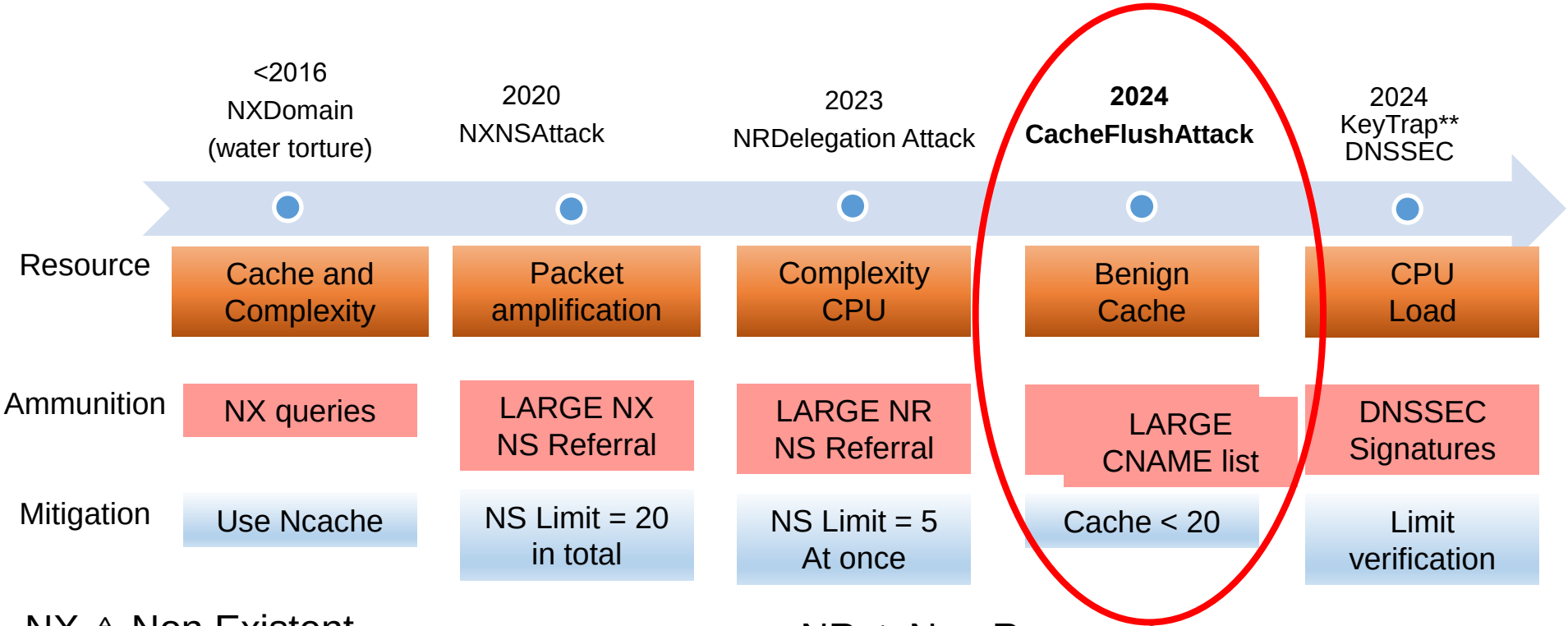
nCache

e1.attack.com NX

CacheFlushNS attack



Background and evolution



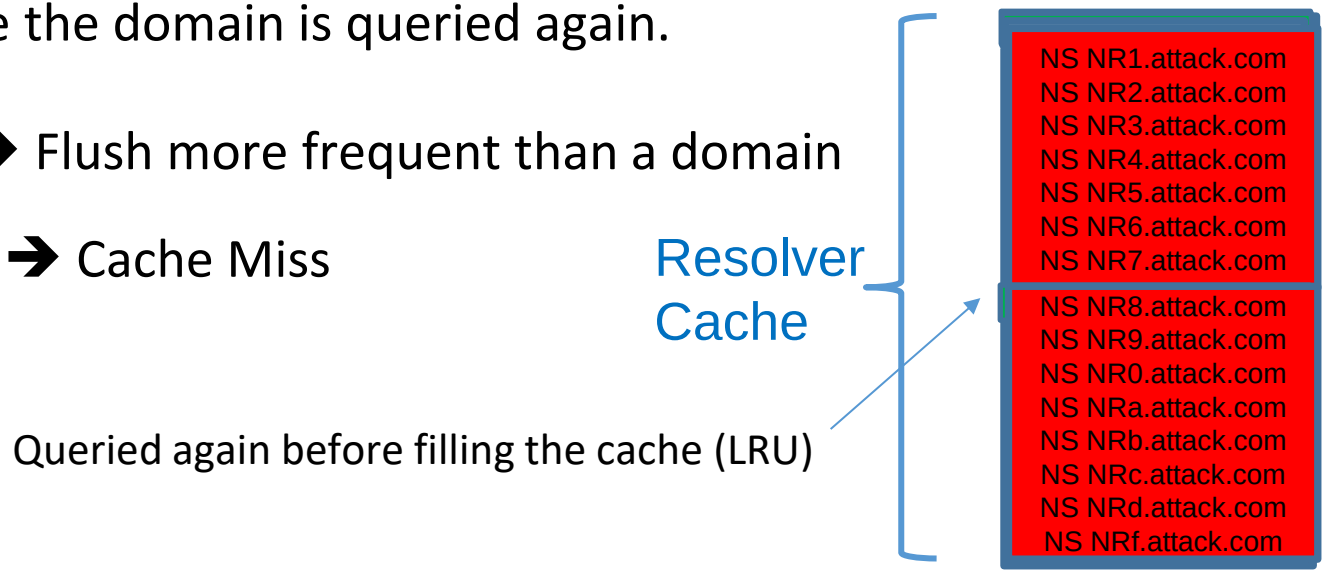
NX ≙ Non Existent
NS ≙ Name Server

NR ≙ Non Responsive

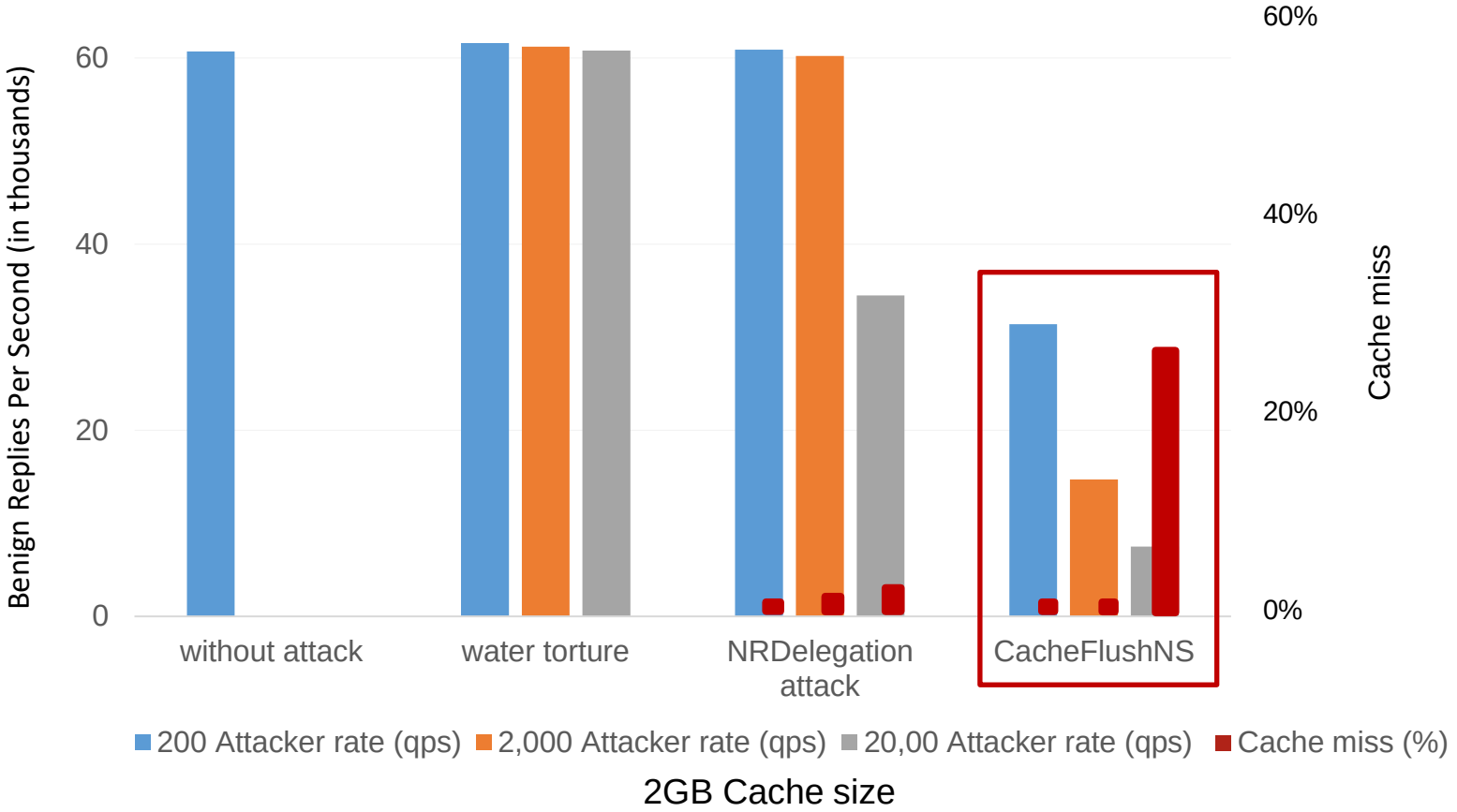
**[KeyTrap Attack E Heftrig, H Schulmann, N Vogel, M Waidner]

When are domains evicted from the cache?

- Cache-miss occurs when the cache is flushed before the domain is queried again.
- LRU ➔ Flush more frequent than a domain query ➔ Cache Miss



Cache Miss and Throughput (Unbound)



Mitigation: Bounding entries in the cache

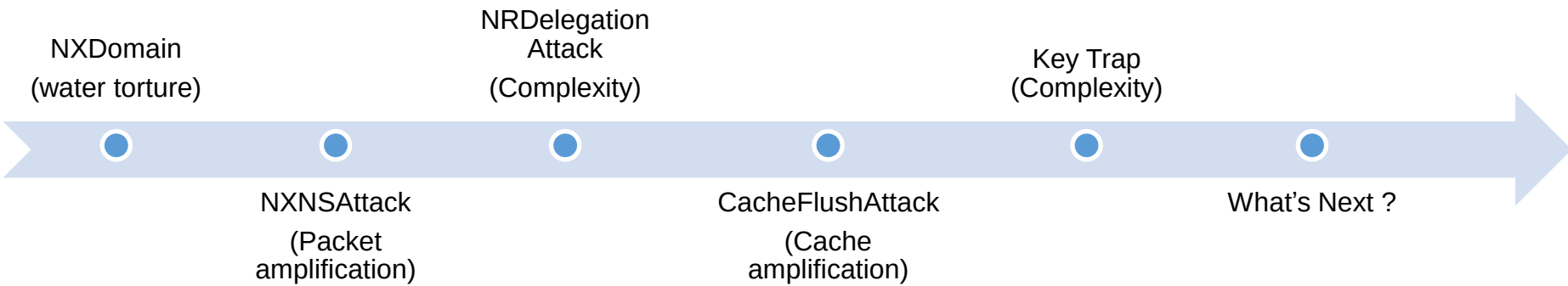
- Core Problem:
  - 1500 are cached, entire referral response, only 20 are used.
- Mitigation:
  - Bound number entries cached, e.g., 20.

- Responsible Disclosure:
  - Bind and Unbound patch: $|\text{entries cached}| < 100$
  - CVE-2024-1737

Summary

- *CacheFlush* is a new type of attack, that targets the cache.

- Our Attack Setup & Measurements -> Usenix Security 24’ Artifact
  - https://github.com/shohamda/CacheFlushSimulator



Questions?

For more info: DEEPNESS lab