UNIVERSITÄT DUISBURG ESSEN

Measurement Survey of Server-Side DNSSEC Adoption

Matthäus Wander

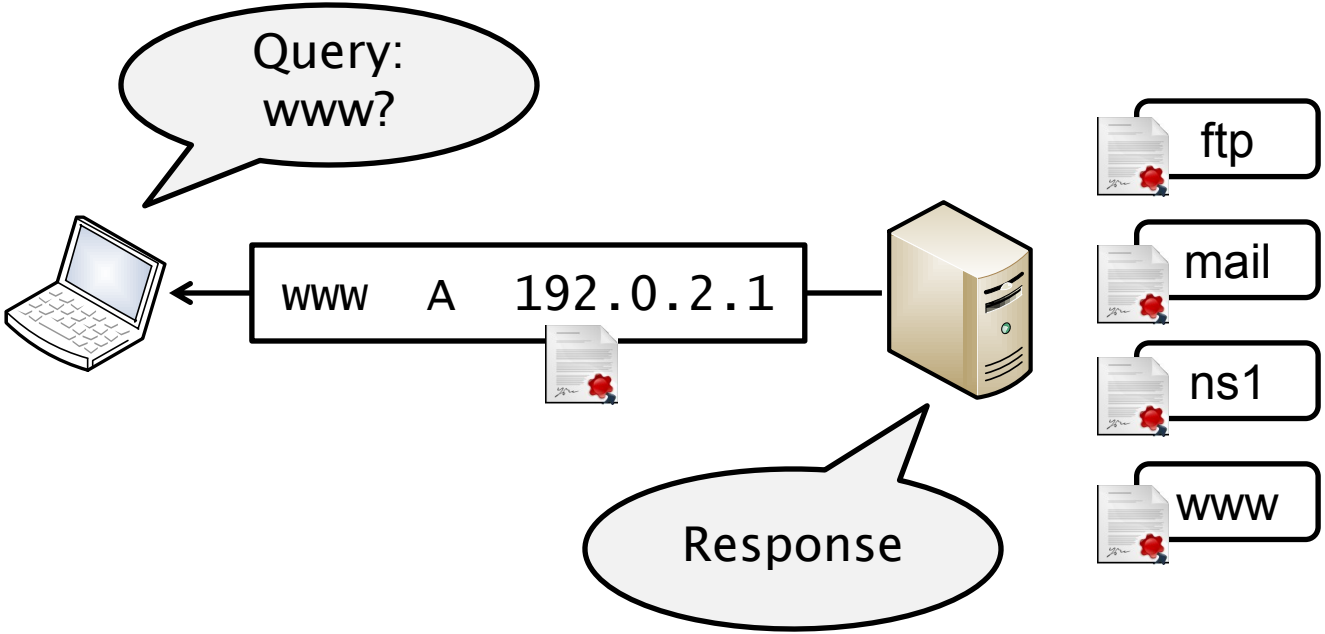
<matthaeus.wander@uni-due.de>

TMA Conference 2017

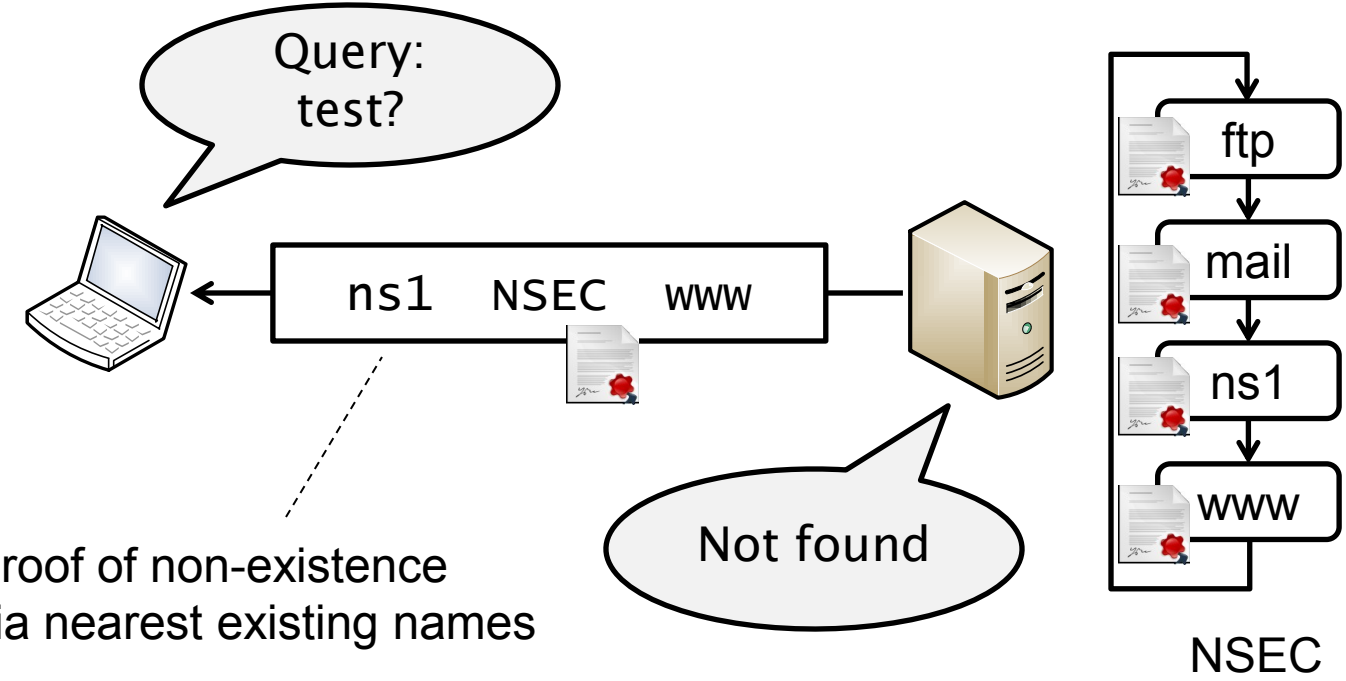
Maynooth, Ireland, June 23, 2017

DNSSEC

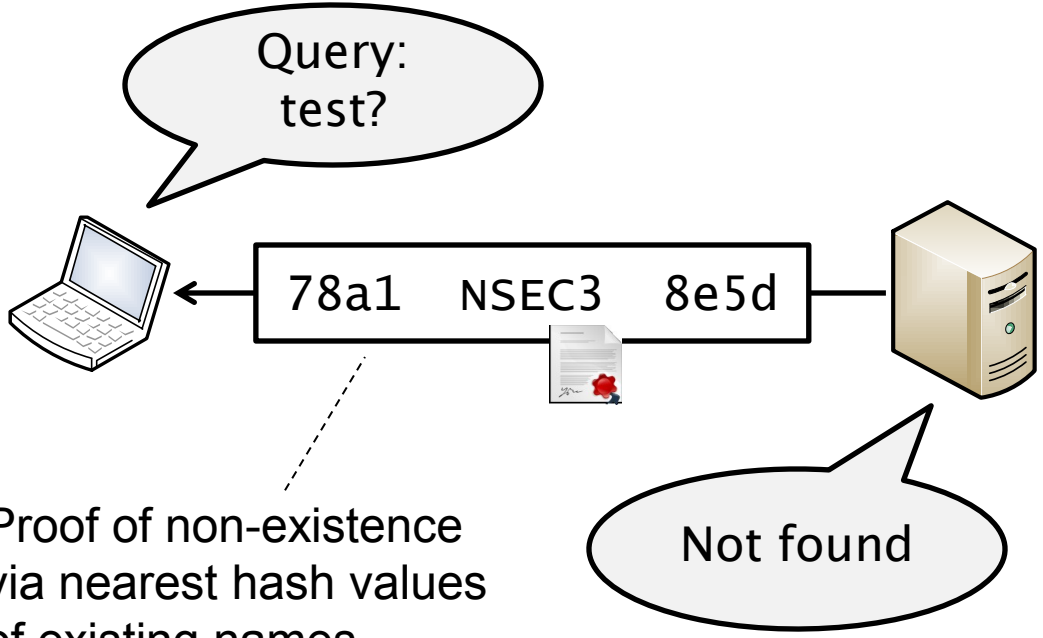
Signed Response



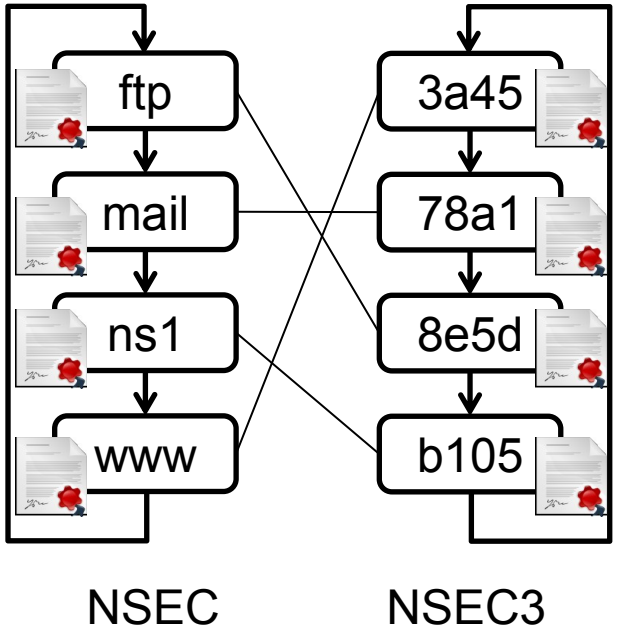
NSEC: Denial of Existence



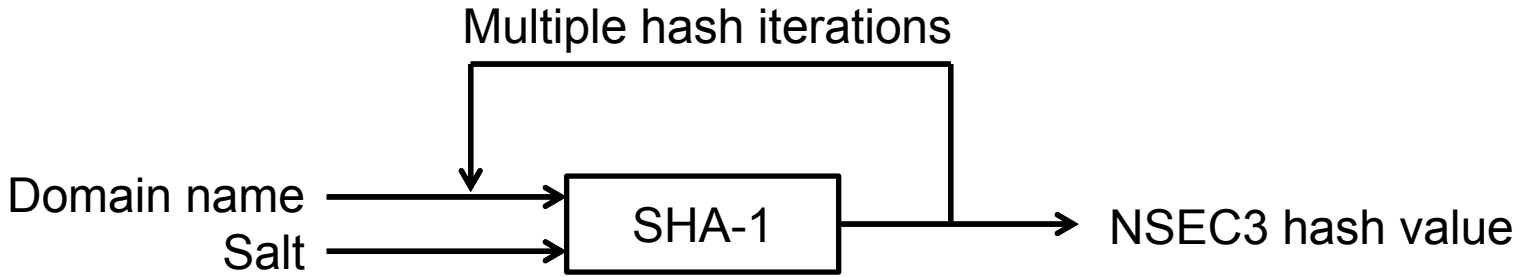
NSEC3: Hashed Denial of Existence



Proof of non-existence via nearest hash values of existing names



NSEC3: Hash Function



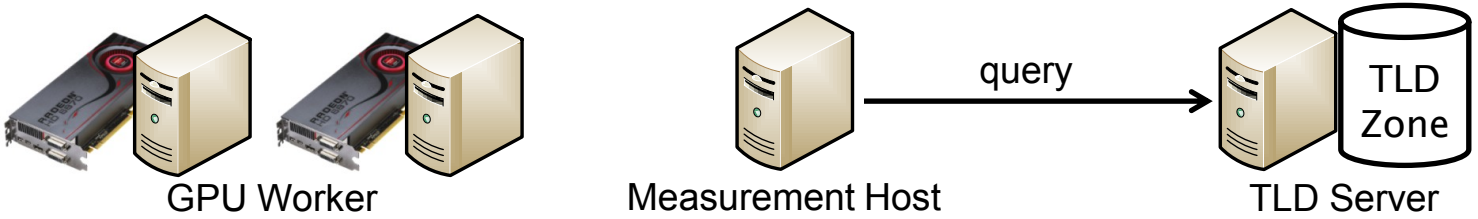
Zone Enumeration

Research Questions

1. Can we perform zone enumeration over all top-level domains?
   - Will it work for NSEC3?

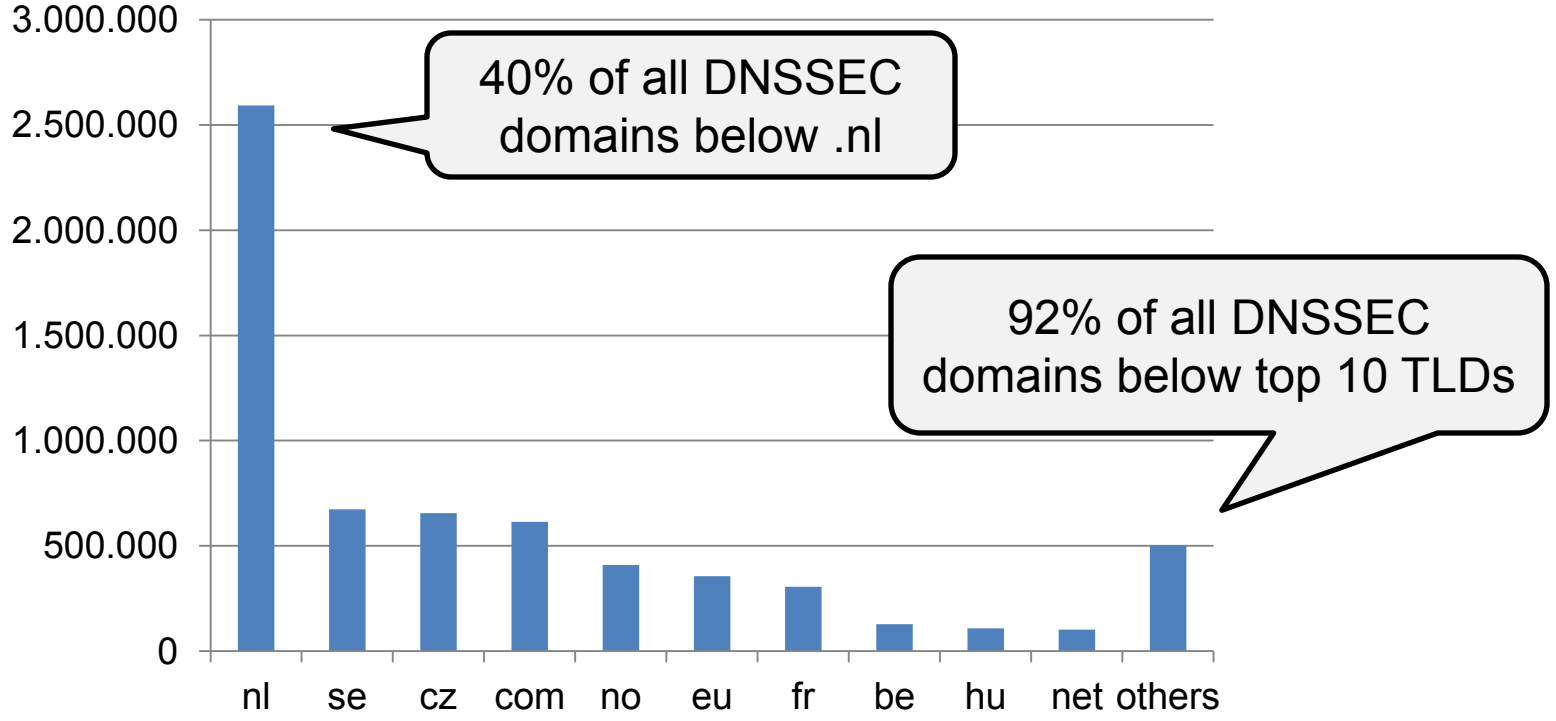
2. What is the DNSSEC deployment state?
   - How many domains are signed?
   - How prevalent are validation failures?

Methodology

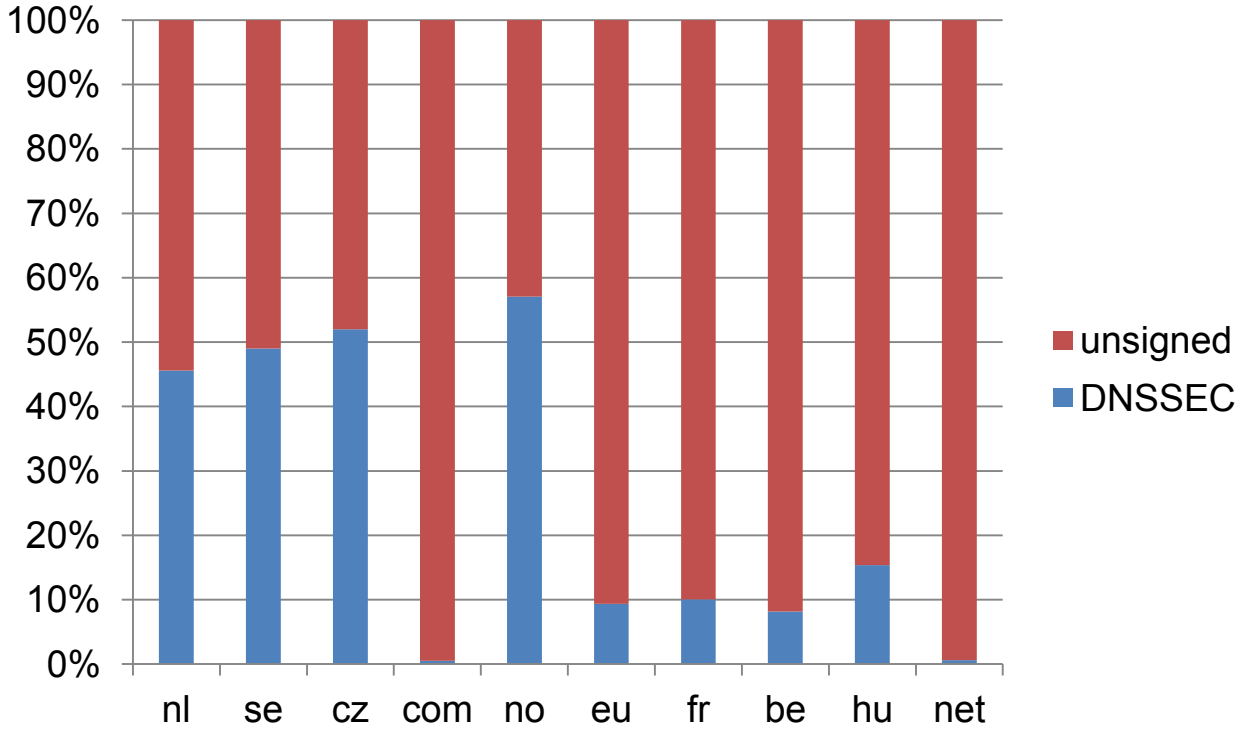


- Send queries for non-existing domain names
- NSEC zone enumeration yields domain names
- NSEC3 zone enumeration yields hash values
  - Recover cleartext names with GPU hashing power

DNSSEC Domains



DNSSEC vs. unsigned Domains

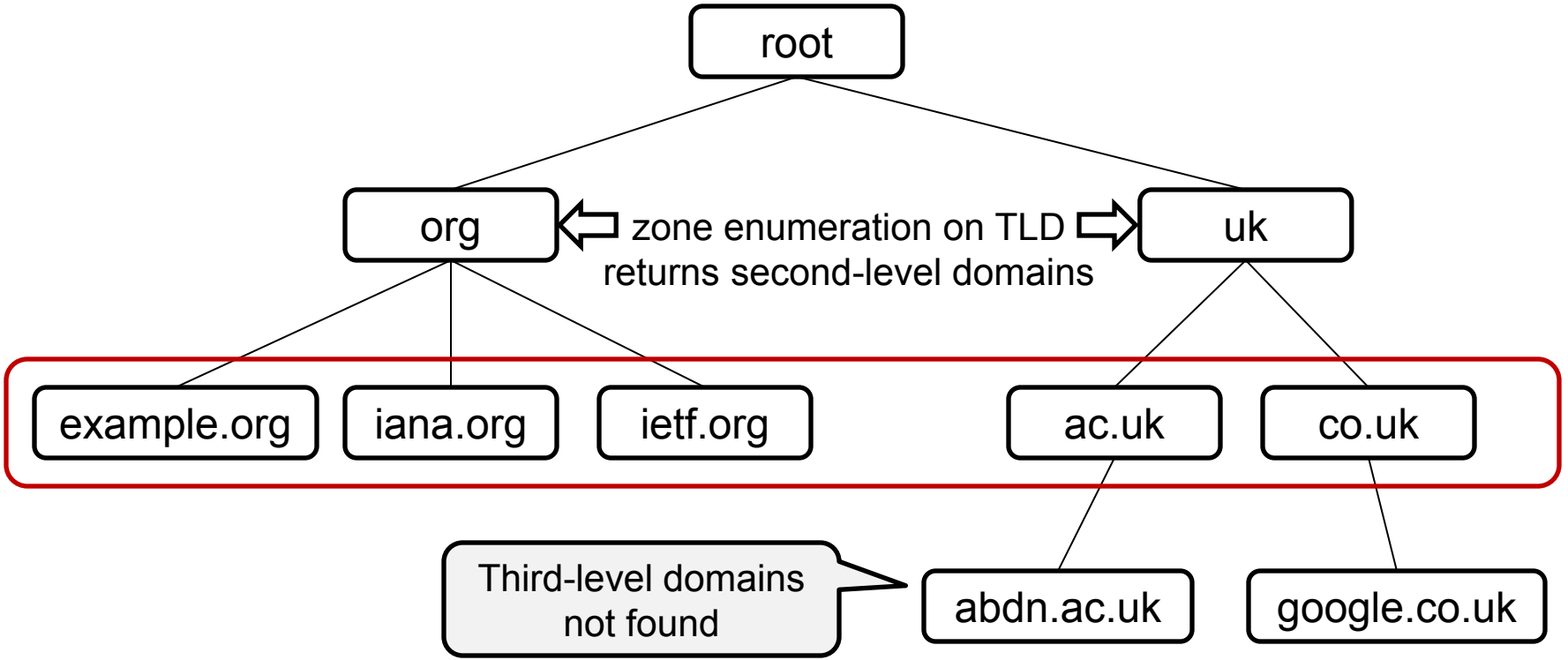


Total Number of DNSSEC Domains:
6.4 million

Complete* figure as of January 2017

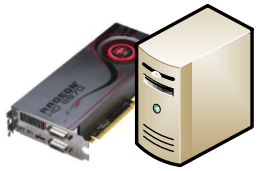
* limitations apply

Figure includes only Second-Level Domains



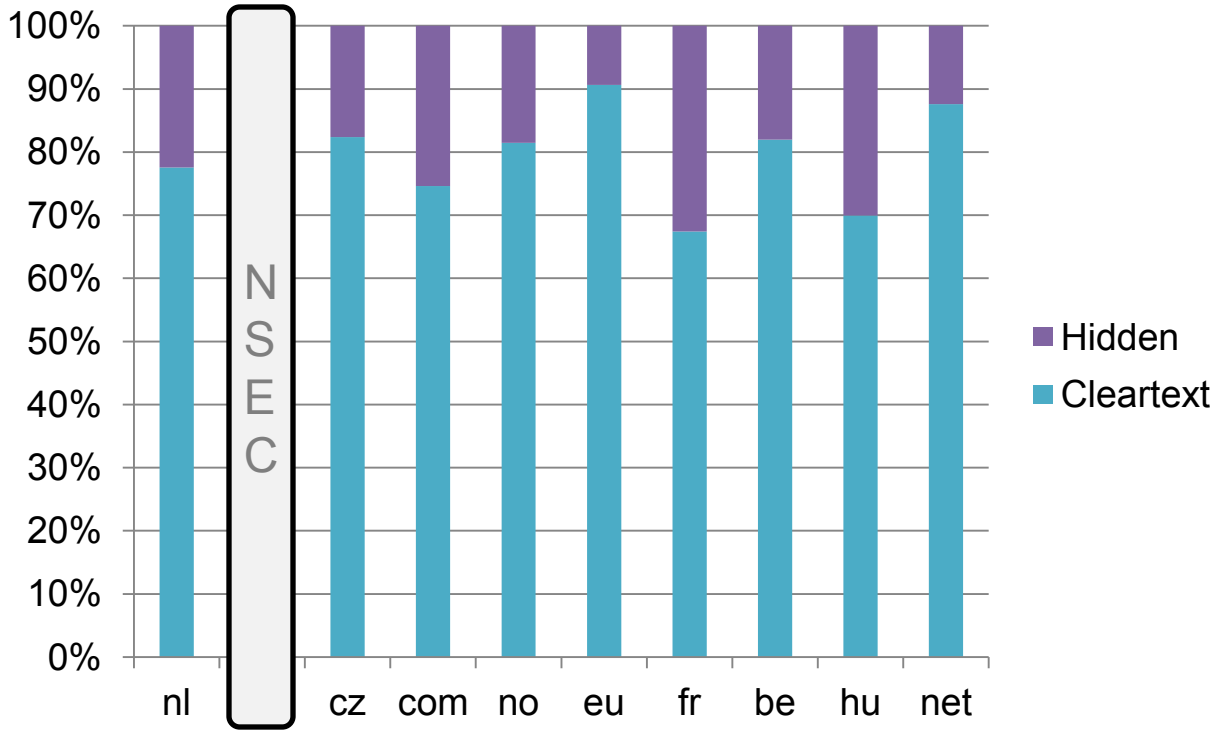
NSEC3 Cleartext Recovery

- 5.7 million NSEC3 hash values from 1196 TLDs
  - Partial brute-force and dictionary attack
  - 7 graphic cards running for two weeks
  - 4.5 million DNSSEC names recovered (79%)



- NSEC3 has hidden 21% DNSSEC names from us
  - At higher operational costs (server must compute NSEC3 hash value for each negative response)

Cleartext Recovery Ratio



What helps against Zone Enumeration?

- Broken NSEC/NSEC3 chain 

  - Not practical: validation will fail on benign clients
- Frequent re-signing with new salt 

  - Expensive: new signatures every few seconds/minutes
  - Beware: malicious attacker will increase query rate
- Online signing with NSEC3 or NSEC5
  - Expensive: new signature for each negative response

What helps not against Zone Enumeration?

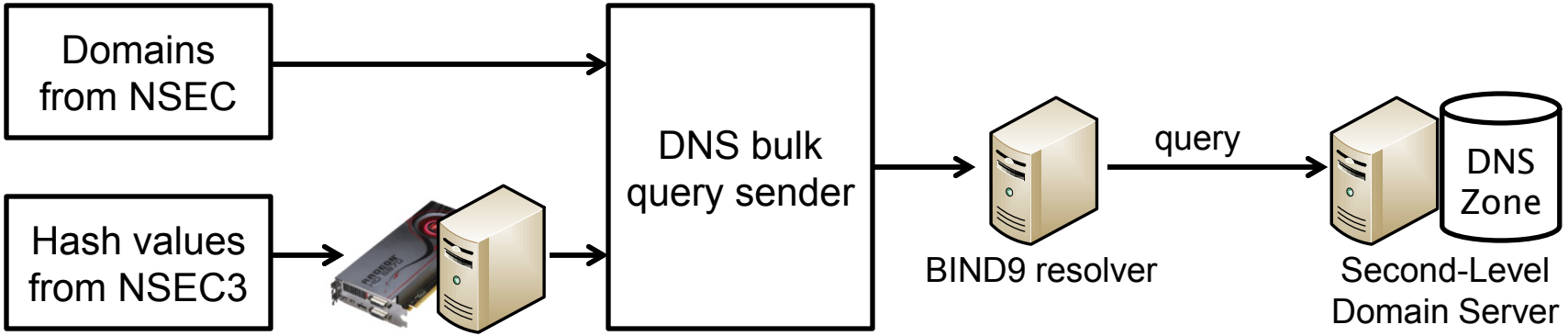
- Increase hash iteration count?
  - Slows down attack but not to a degree that helps

	TLD	NSEC or NSEC3?	DNSSEC Domains	Cleartext Recovery
22.	mx	NSEC3, opt-out, i=100	7,924	80%
132.	lat	NSEC3, opt-out, i=100	200	79%
187.	la	NSEC3, opt-out, i=150	105	96%
40.	name	NSEC3, opt-out, i=0	1,694	43%
71.	jp	NSEC3, opt-out, i=8	453	39%
112.	xn--3e0b707e	NSEC3, opt-out, i=10	257	8%

Many iterations, high recovery

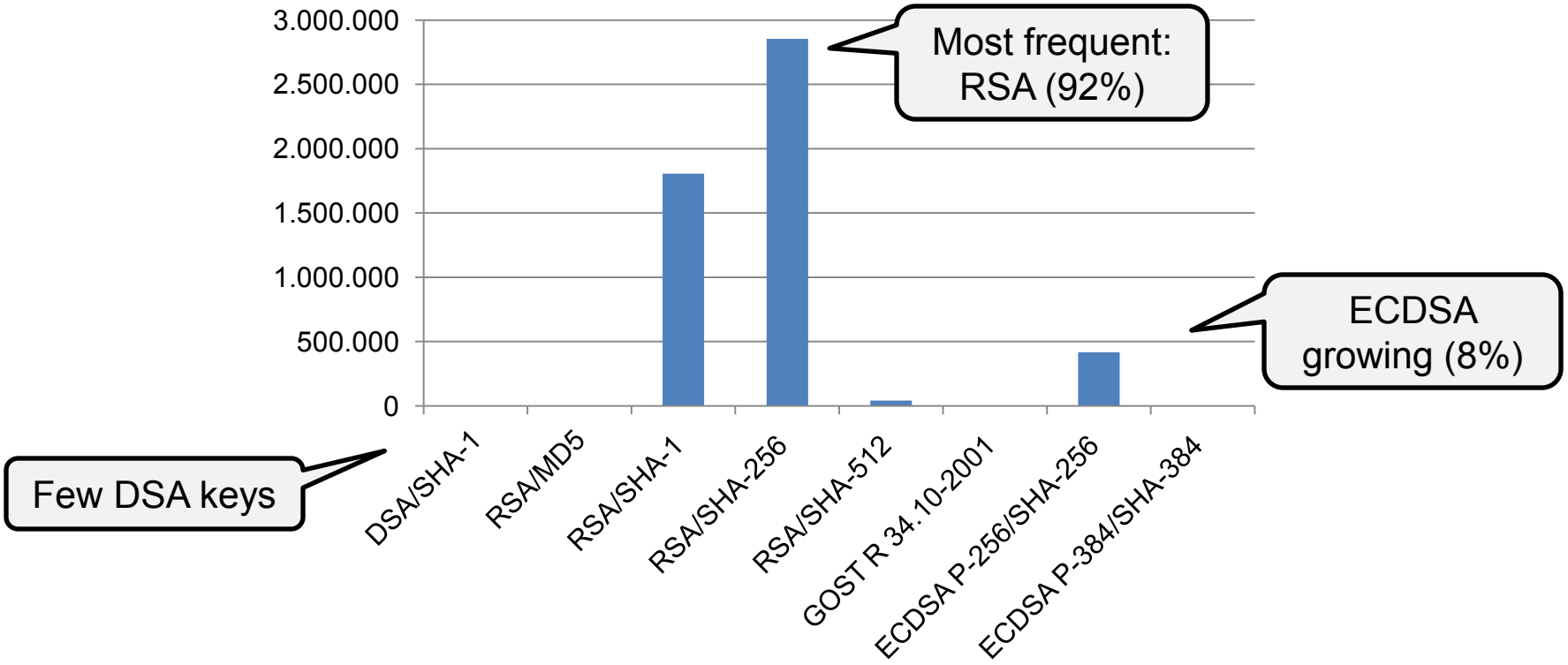
Few iterations, low recovery

Analysis of Signed Second-Level Domains



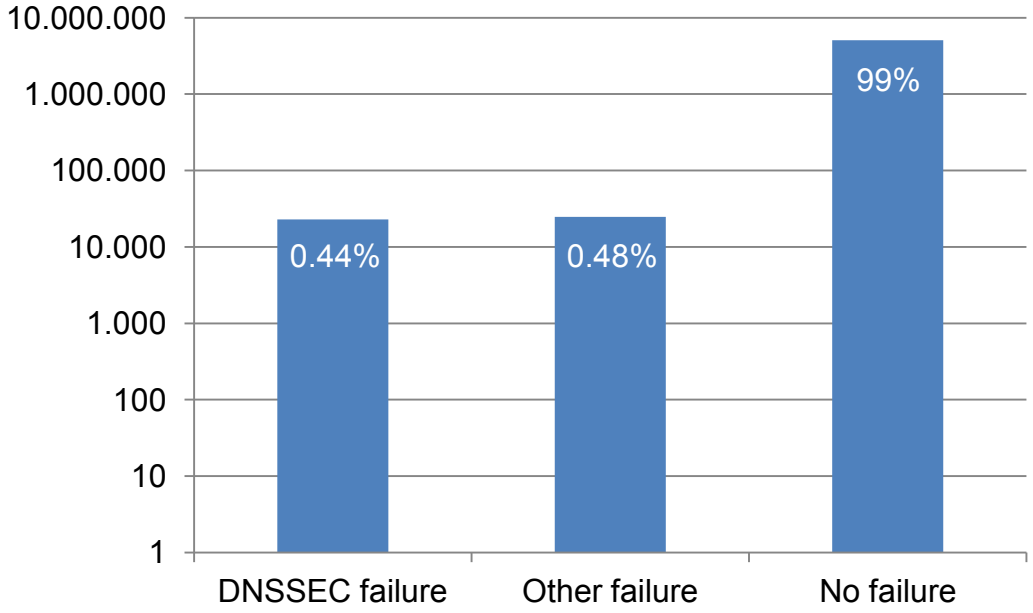
- Query 5.1 million signed second-level domains for their DNSSEC configuration
  (DS and DNSKEY record sets)

Signing Algorithms



Validation Failures

Result	Count
No DNSKEY (dangling DS)	19,386
No trusted DNSKEY (dangling DS)	1,216
No RRSIG for trusted DNSKEY	380
Signature expired	1,799
Signature ahead of time	1
Signature verify failure	49
Validation failure	**22,831**
Validation success	**5,092,022**



Conclusions 1/2

- DNSSEC signing is common among a few TLDs
  - 6.4 million signed second-level domains
- Validation failures are rare (0.44%) but visible
- NSEC3 protects minor portion of names (21%)
  - Hash iteration count does not affect the recovery ratio
- Effective protection is expensive (online signing)

Conclusions 2/2

- Zone enumeration is useful for debugging
  - Find broken NSEC/NSEC3 chains or erroneous servers
- TLD measurements give an incomplete picture
  - How to get a list of associated second-level domains?
- Suggestion: Use Mozilla‘s Public Suffix List
  - First section (ICANN domains), omit private domains

Top-Level Domain Statistics

	TLD	NSEC or NSEC3?	DNSSEC Domains	Adoption Ratio	Cleartext Recovery
1.	nl	NSEC3, opt-out, i=5	2,592,219	45%	78%
2.	se	NSEC	673,262	49%	all
3.	cz	NSEC3, i=10	655,529	52%	82%
4.	com	NSEC3, opt-out, i=0	614,209	<1%	75%
5.	no	NSEC3, opt-out, i=5	409,416	57%	81%
6.	eu	NSEC3, opt-out, i=1	355,157	9%	91%
7.	fr	NSEC3, opt-out, i=1	304,663	10%	67%
8.	be	NSEC3, opt-out, i=5	127,177	8%	82%
9.	hu	NSEC3, opt-out, i=5	107,434	15%	70%
10.	net	NSEC3, opt-out, i=0	101,872	<1%	88%
[1357 others omitted]			**Total: 6,441,427**		