UNIVERSITÄT DUISBURG ESSEN

GPU-based NSEC3 Hash Breaking

Matthäus Wander, Lorenz Schwittmann,
Christopher Boelmann, Torben Weis

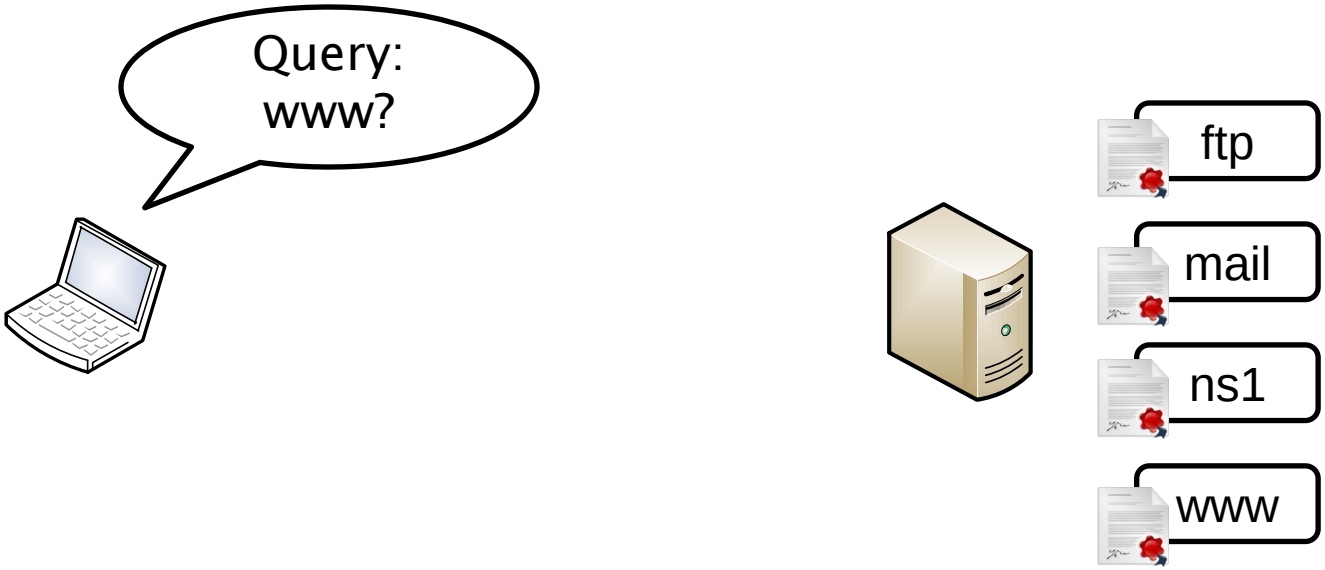
<matthaeus.wander@uni-due.de>

IEEE NCA 2014

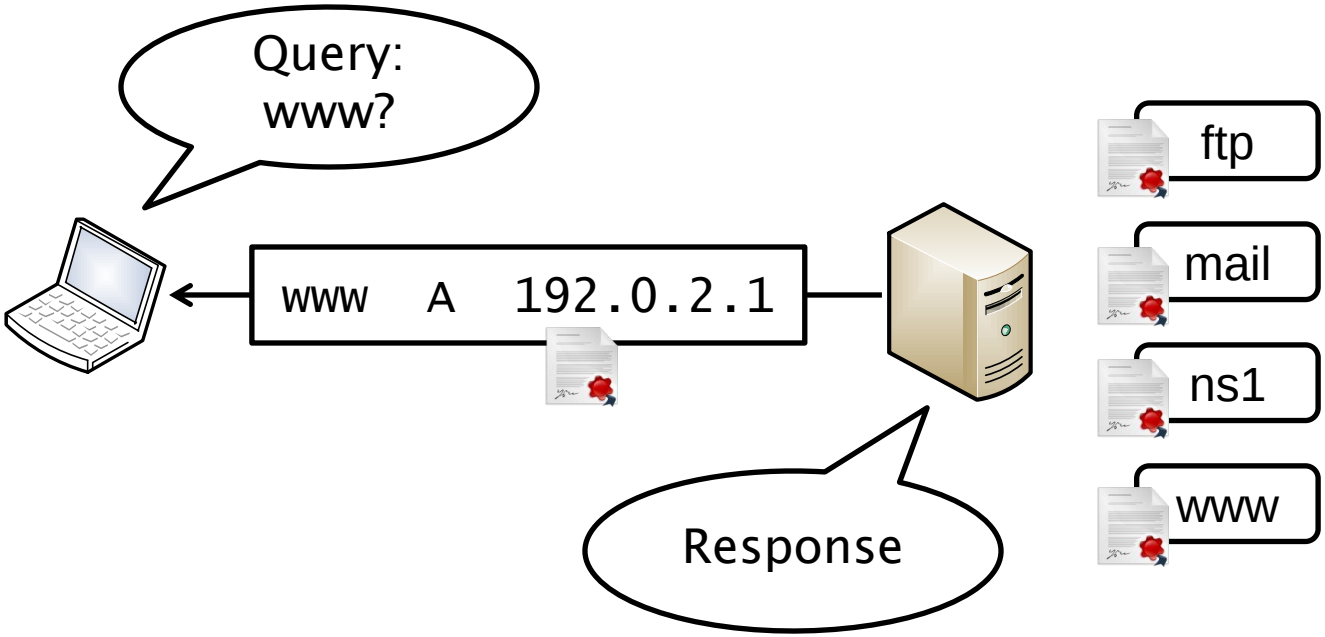
Cambridge, August 22, 2014

NSEC3 FUNDAMENTALS

Secure Denial of Existence with DNSSEC

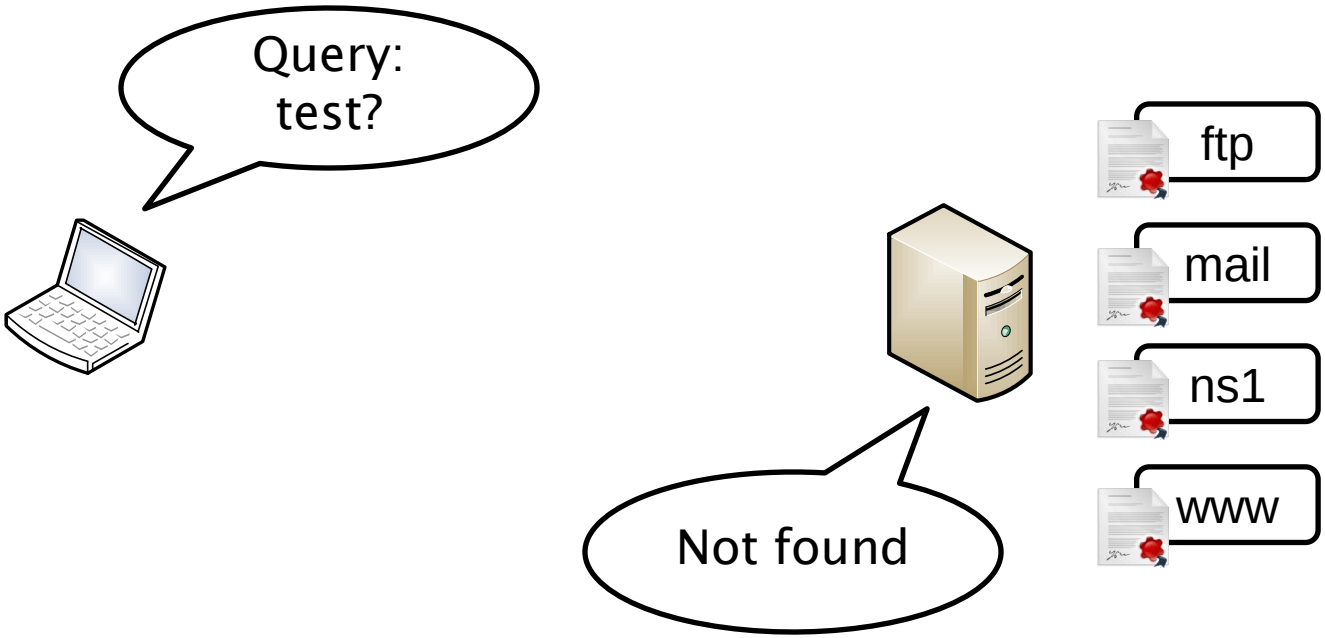


Secure Denial of Existence with DNSSEC



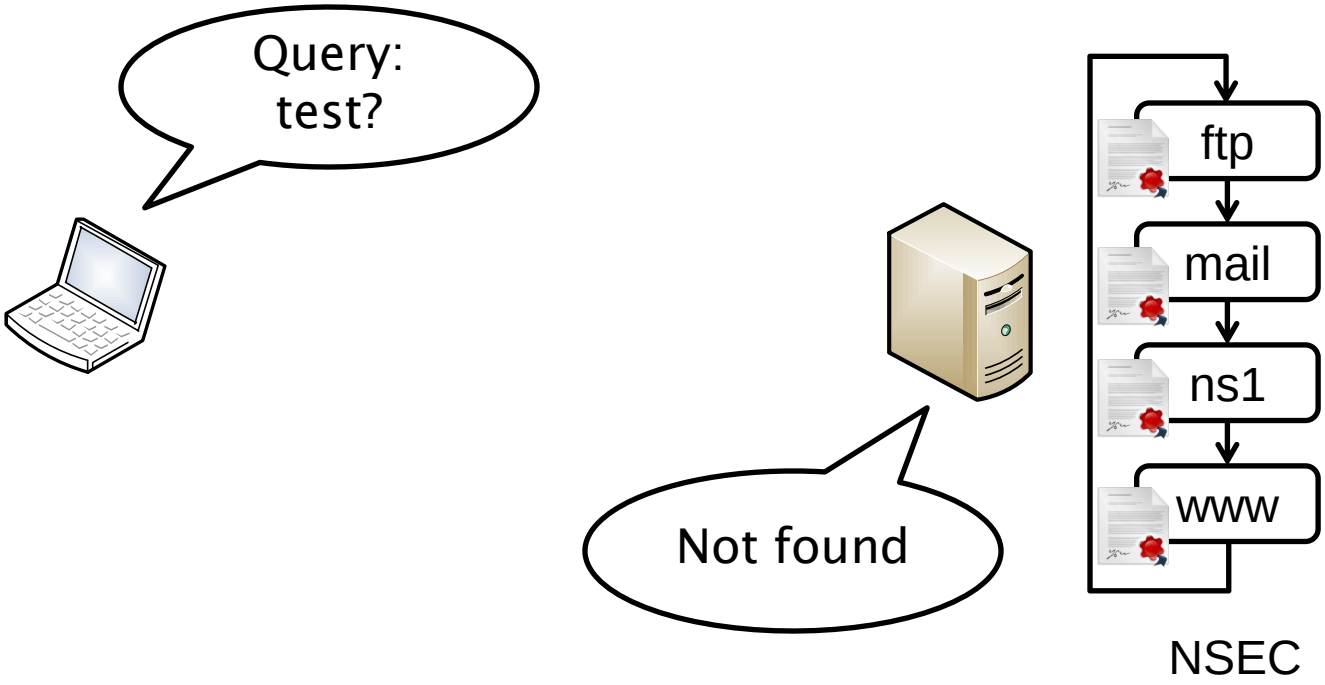
- Signed resource record
- Authenticity verified with PKI built into DNSSEC

Secure Denial of Existence with DNSSEC



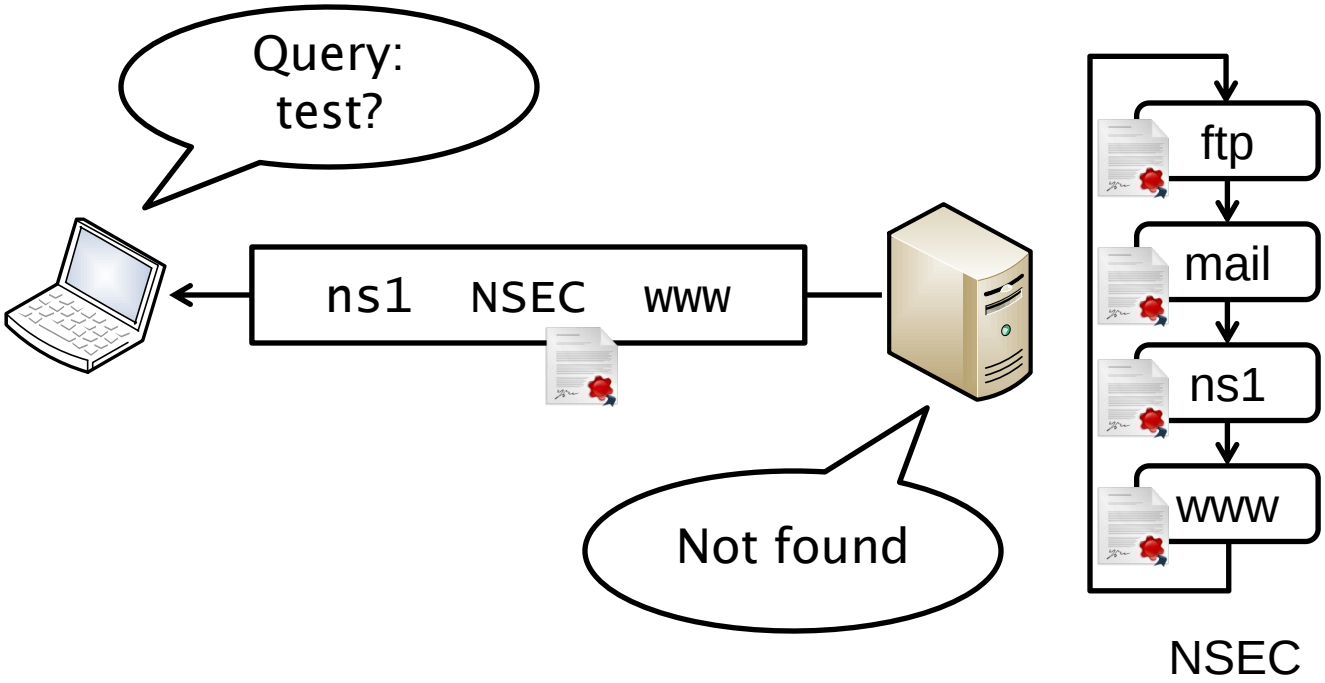
- Query name: n

Secure Denial of Existence with DNSSEC



- Query name: n

Secure Denial of Existence with DNSSEC



- Query name: n
- Response: (r_1, r_2) with $r_1 < n < r_2$

Zone Enumeration

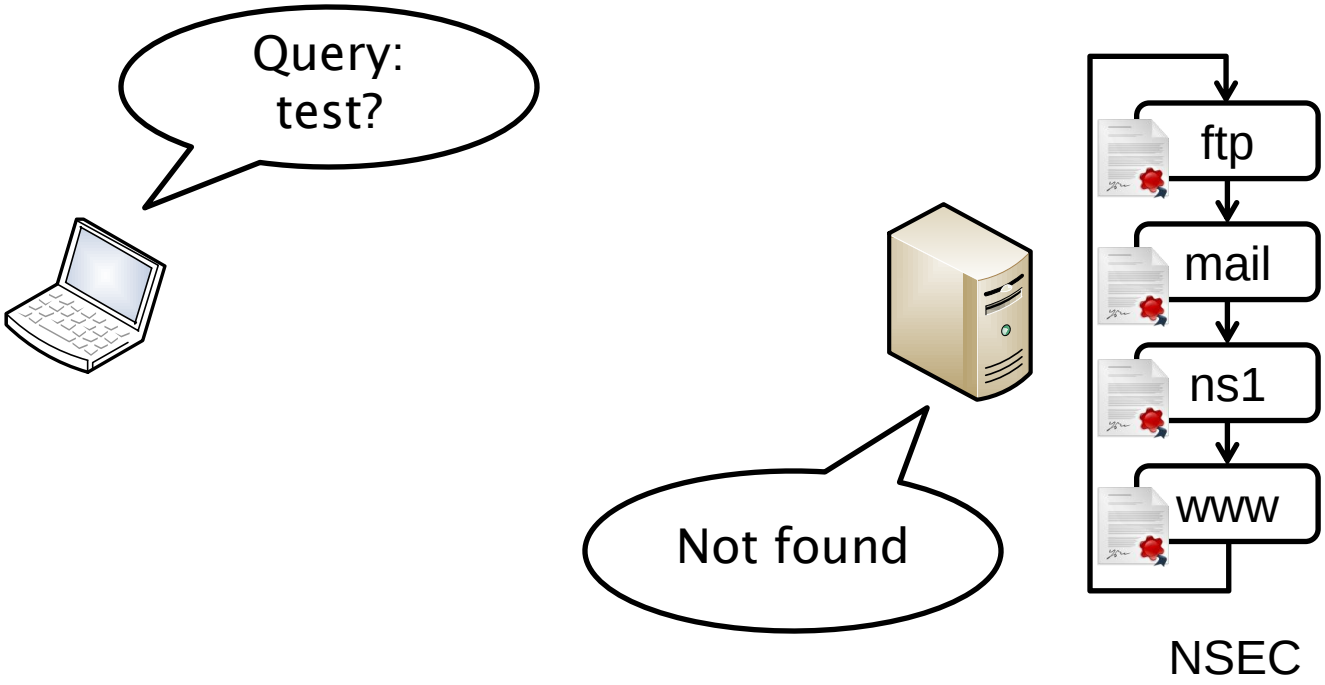
- Copy DNSSEC zone by crawling NSEC records
- Nominet (.uk) position:

> „Zone file enumeration is a show-stopper for us that will prevent us from fully implementing DNSSEC.“

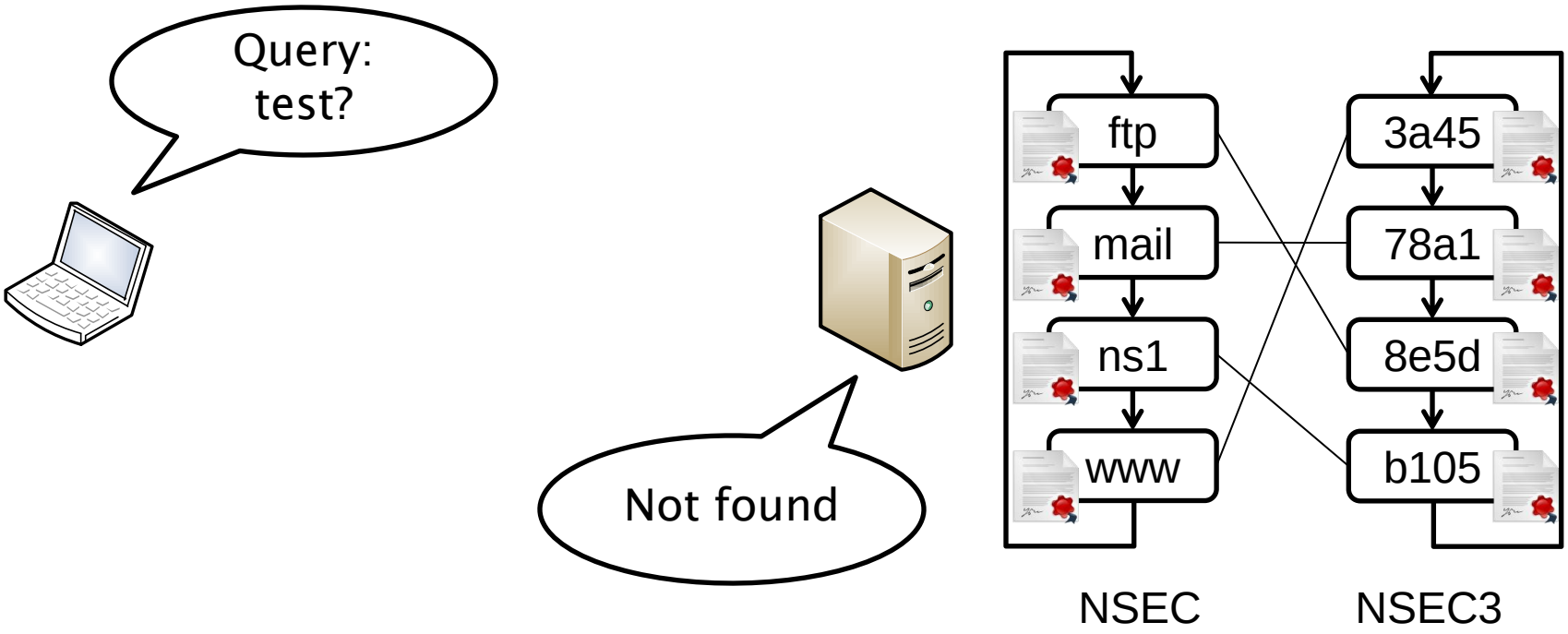
- DENIC (.de) position:

> „In conflict with Germany’s Federal Data Protection Act“

Secure Denial of Existence with DNSSEC

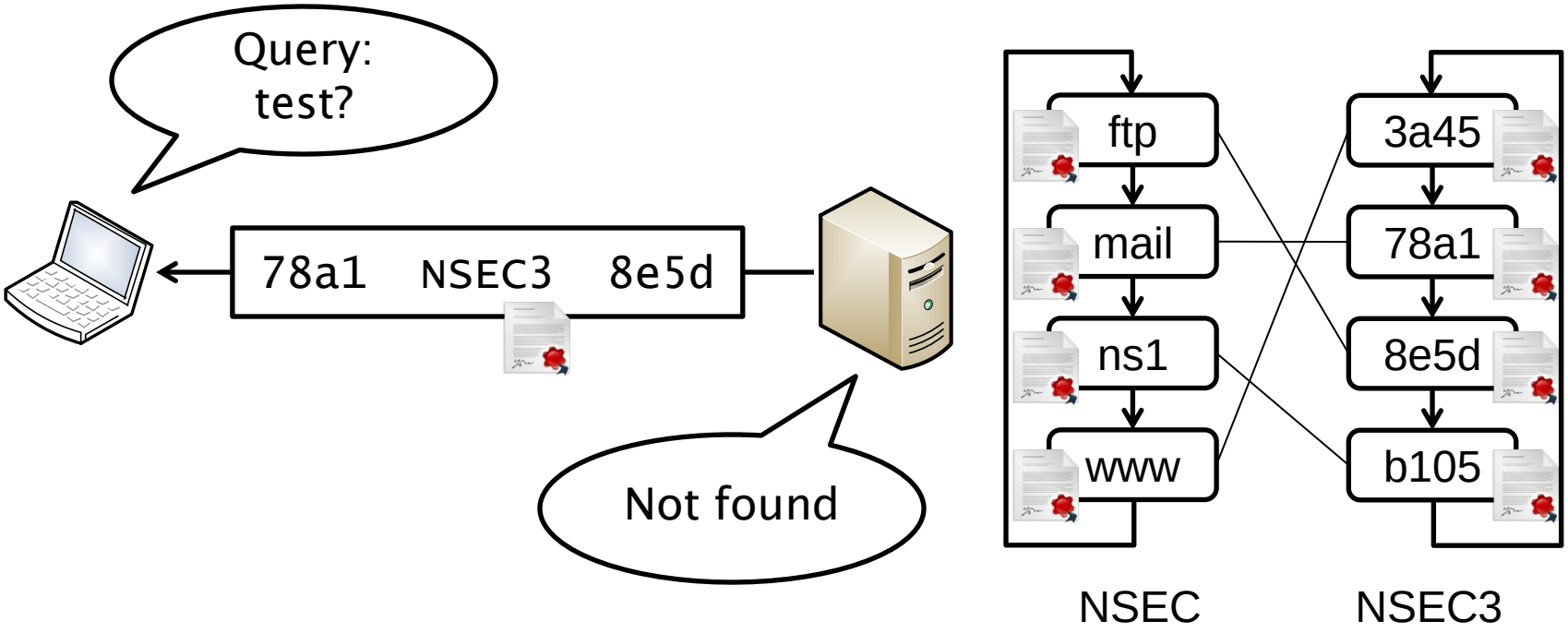


Secure Denial of Existence with DNSSEC



- Hash query name: $h(n)$

Secure Denial of Existence with DNSSEC



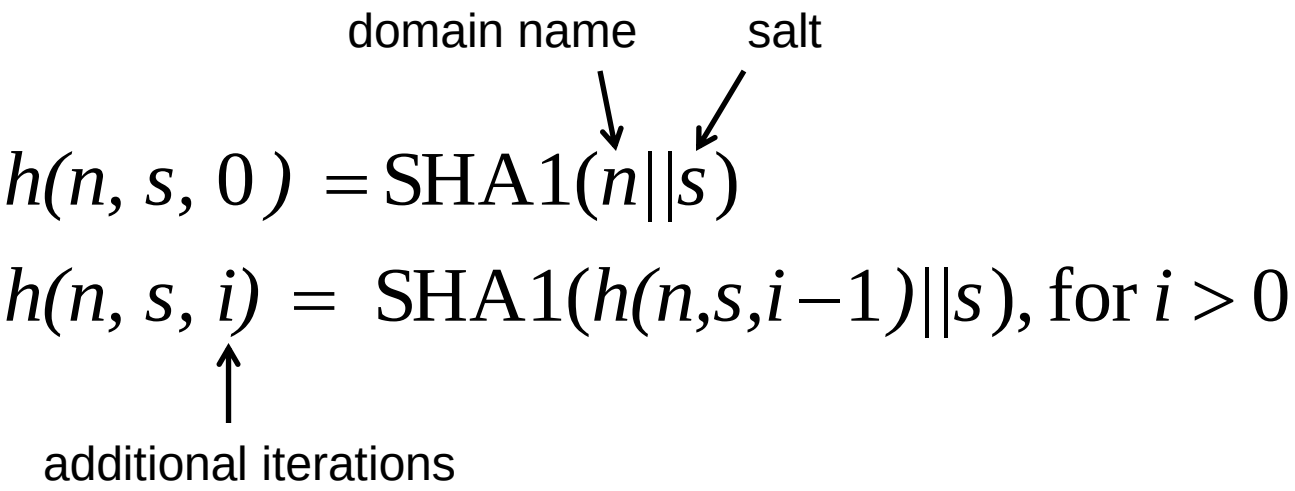
- Hash query name: $h(n)$
- Response: $(h(r_1), h(r_2))$ with $h(r_1) < h(n) < h(r_2)$

Reasons for and against NSEC3

- Privacy
- "Opt-out" feature
- CPU load
- Message size

⇨ **How well does NSEC3 prevent zone enumeration?**

NSEC3 Definition



- Repeated SHA1 computation
- Salt is identical for all names in a DNSSEC zone

Top-Level Domain Survey

TLD	i	Salt
at.	5	b4c3ee8e123154f8
ch.	2	e7bd8151
cn.	10	aef123ab
com.	0	
de.	15	ba5eba11
eu.	1	5ca1ab1e
fr.	1	41b69d30

TLD	i	Salt
info.	1	d399eaab
jp.	8	f5435b71d7
net.	0	
nl.	5	c9545f07a61d0d33
org.	1	d399eaab
ru.	3	00ff
uk.	0	

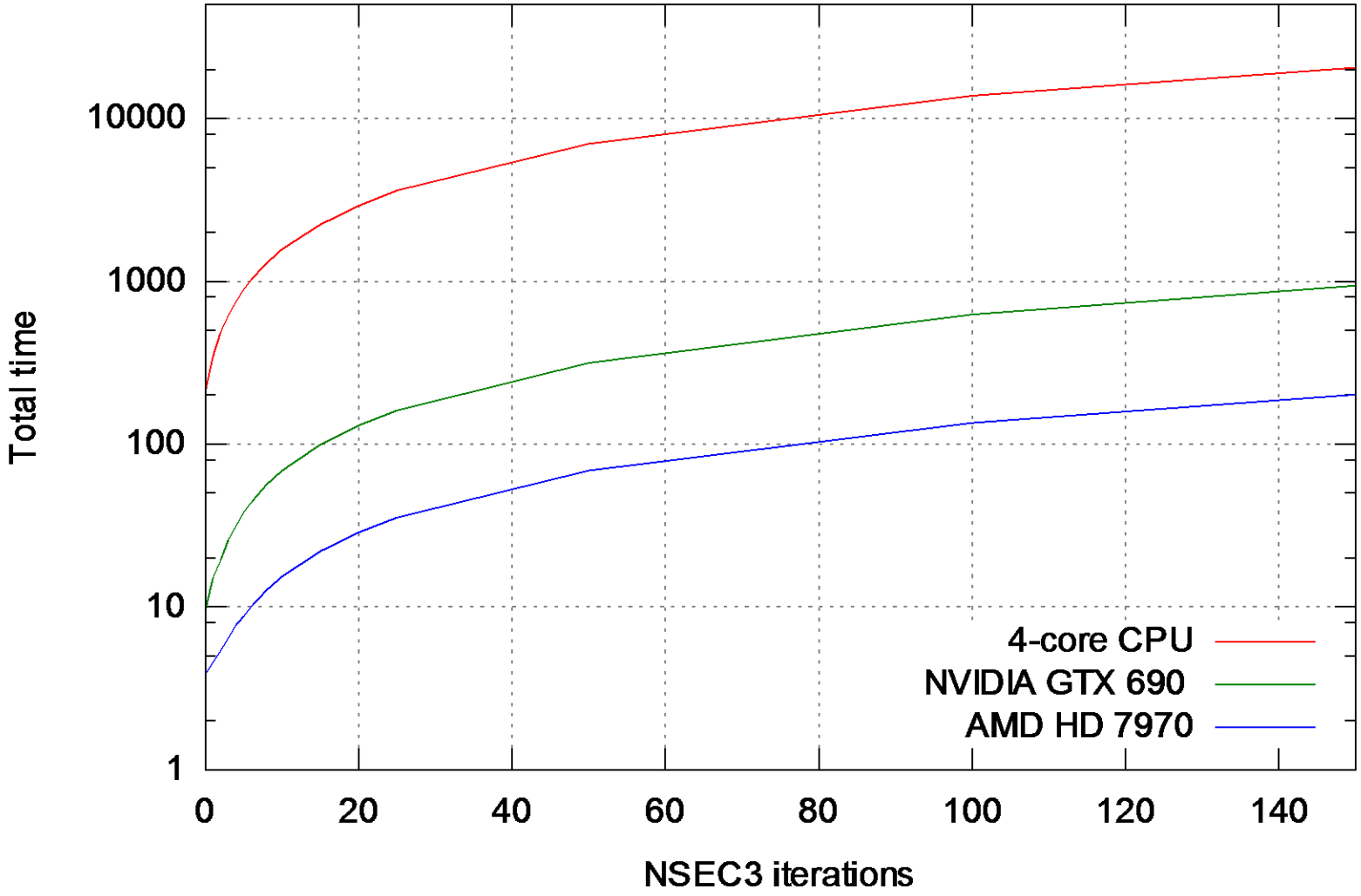
May 2014

- 335 use NSEC3, 53 use NSEC, 185 not signed
- 60% of TLDs with NSEC3 use i=1
- 42% of TLDs with NSEC3 change the salt

ATTACKING NSEC3

1. Collect hashes
2. Reverse hashes

Why AMD Graphic Cards?

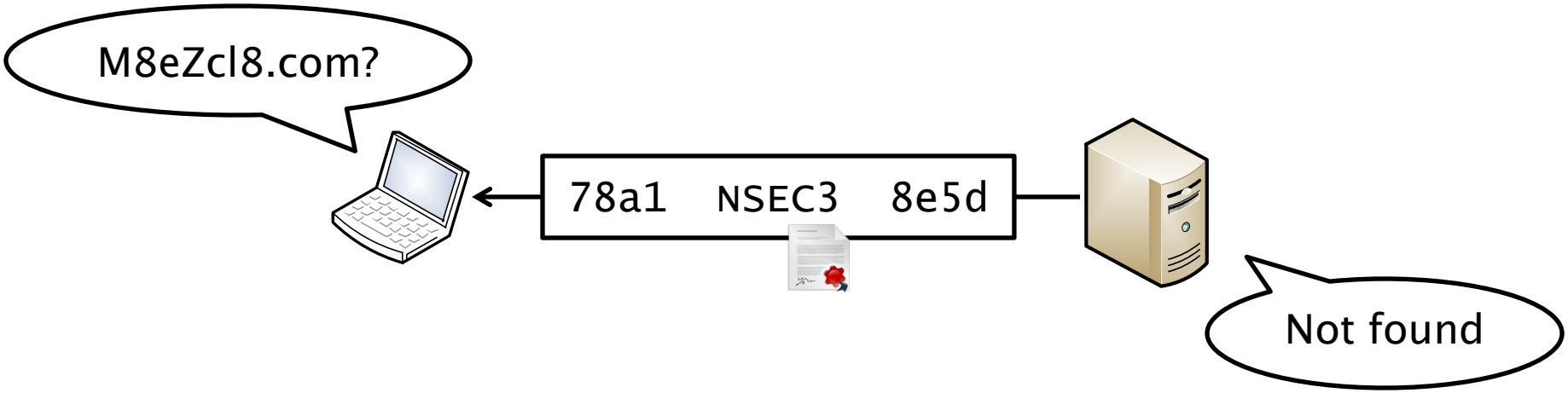


ATTACKING NSEC3

1. Collect hashes
2. Reverse hashes

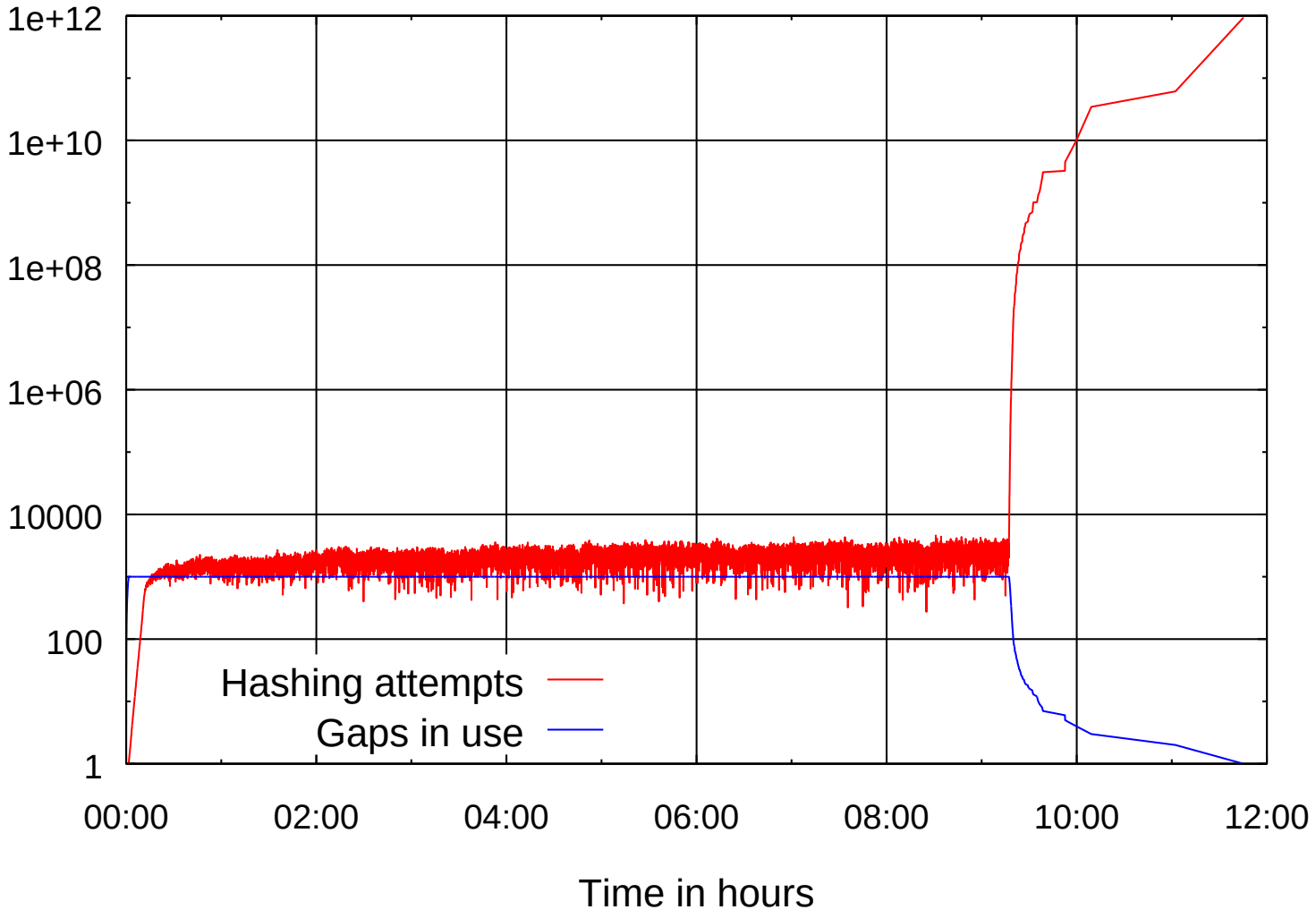
Hash Crawling

- Retrieve NSEC3 hashes from name server
  - Send queries for random non-existing names



- Check hash before sending query

Crawling 345,000 Hashes from .com

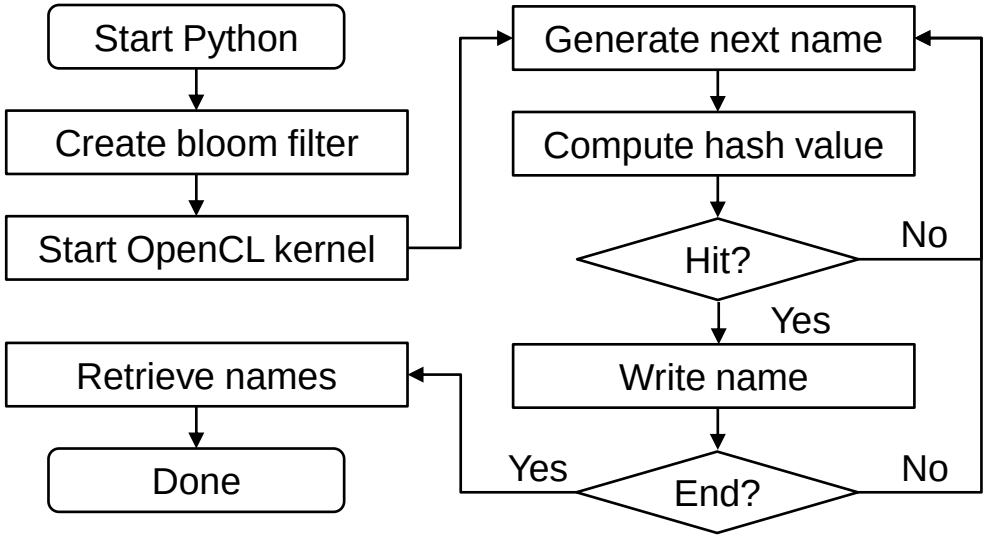


ATTACKING NSEC3

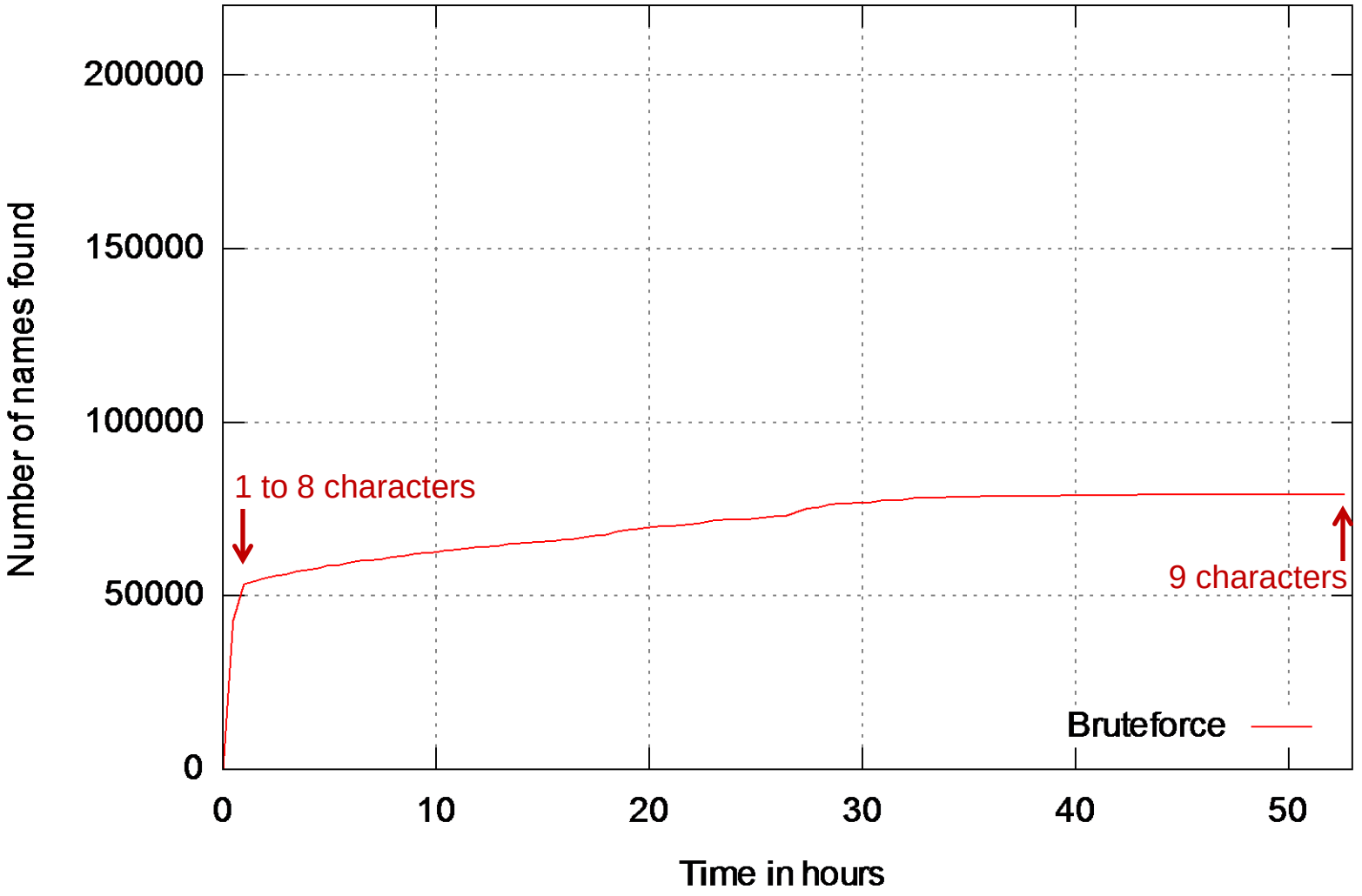
1. Collect hashes
2. Reverse hashes

GPU-based NSEC3 Hash Breaking

- Iterate through cleartext candidate names
  - Compute NSEC3 hash, compare with known hashes
- Global memory access on GPU is expensive
  - Bloom filter for 300% speedup

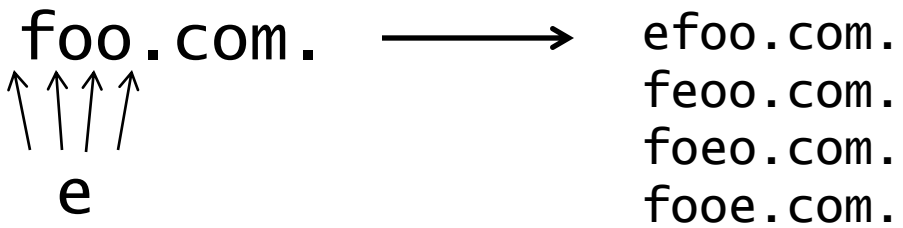


Brute-Force Attack

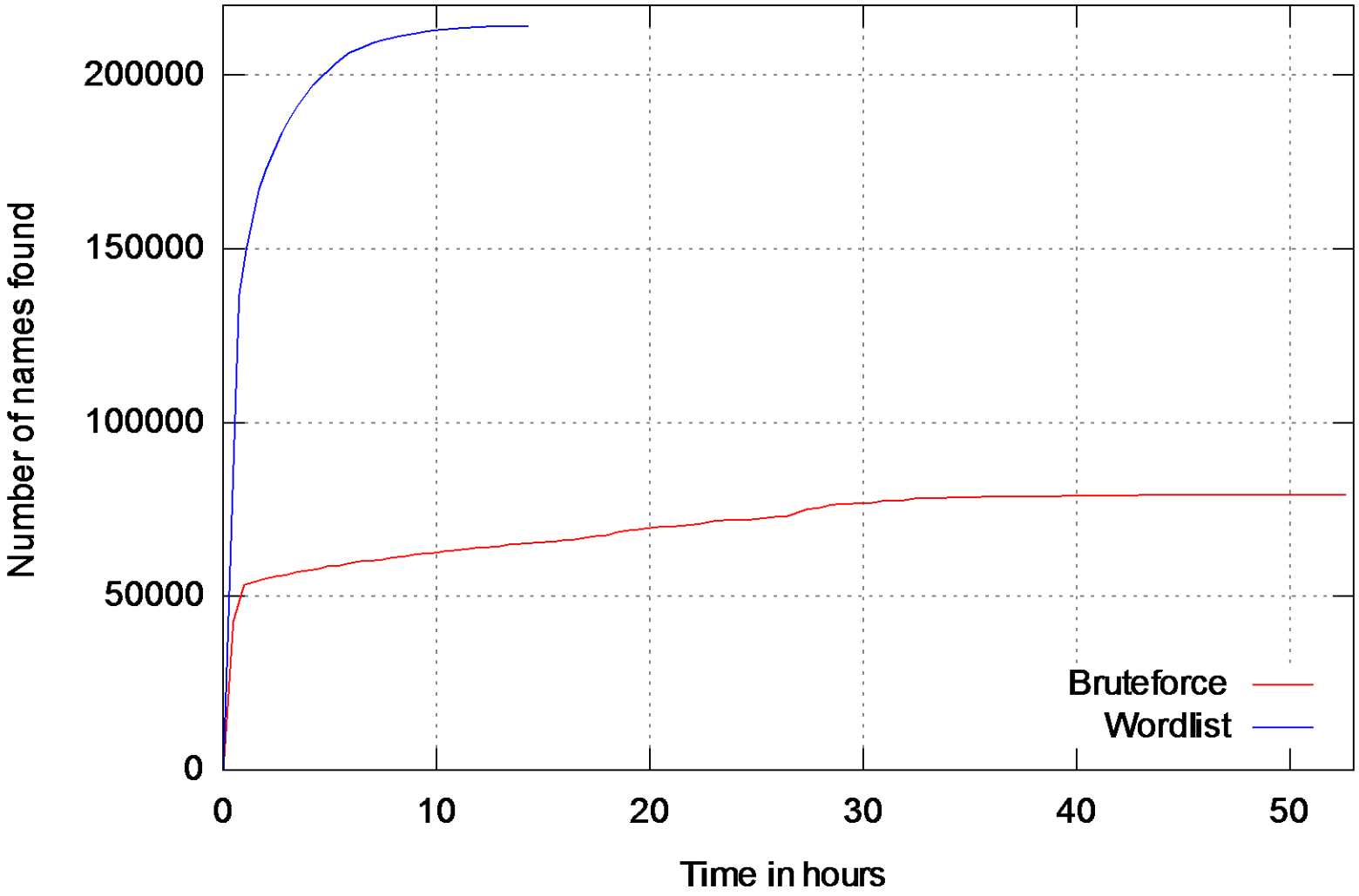


Dictionary Attack

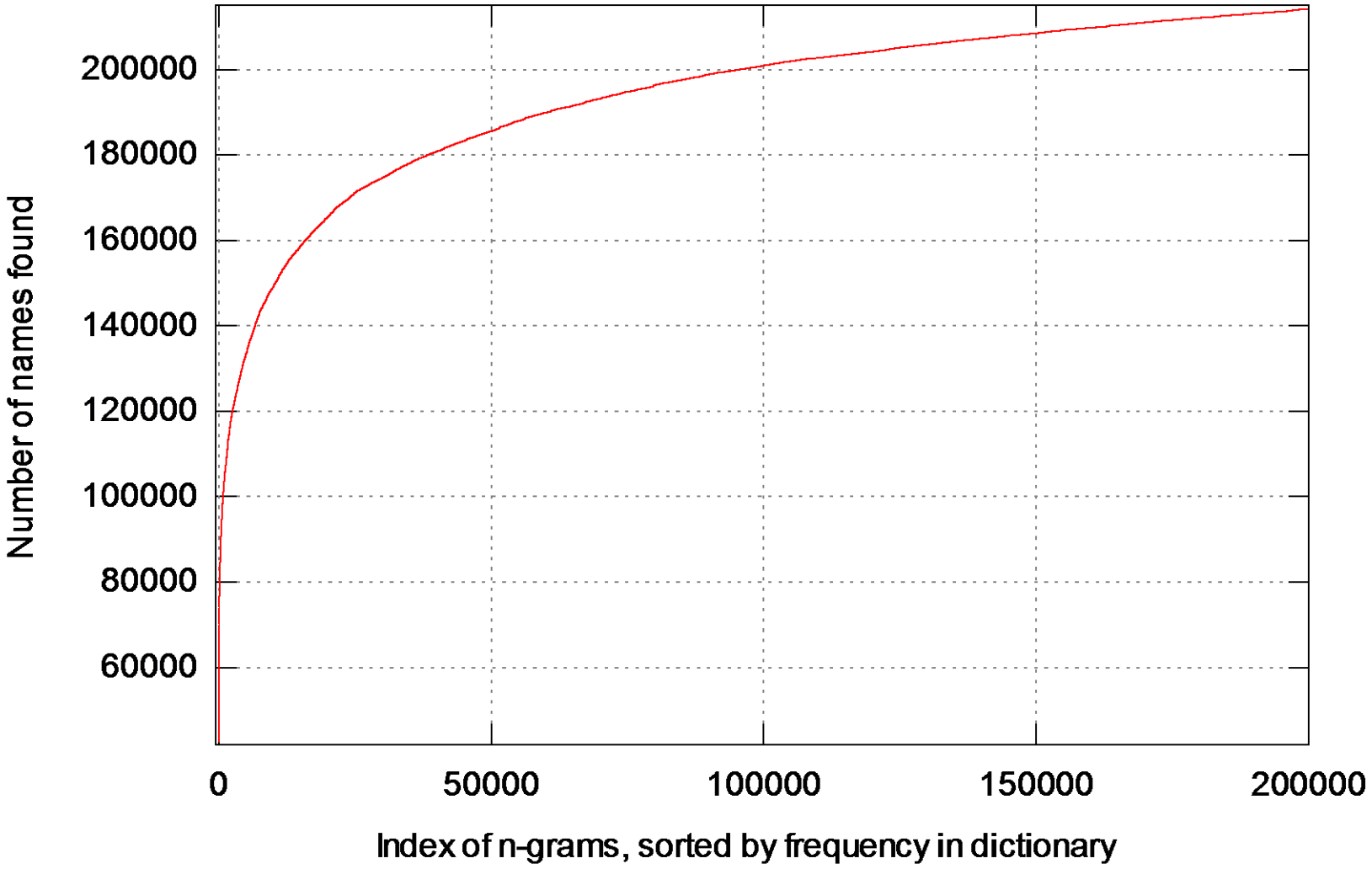
- Effectiveness depends on dictionary quality
  - Good public lists (Alexa, Quantcast)
  - List of all IPv4 reverse mappings (not exhaustive!)
- 7.1 mio candidate names
- Generate more candidates by inserting strings
  - Insert most common 200,000 n-grams (with $1 \leq n \leq 15$)



Dictionary Attack



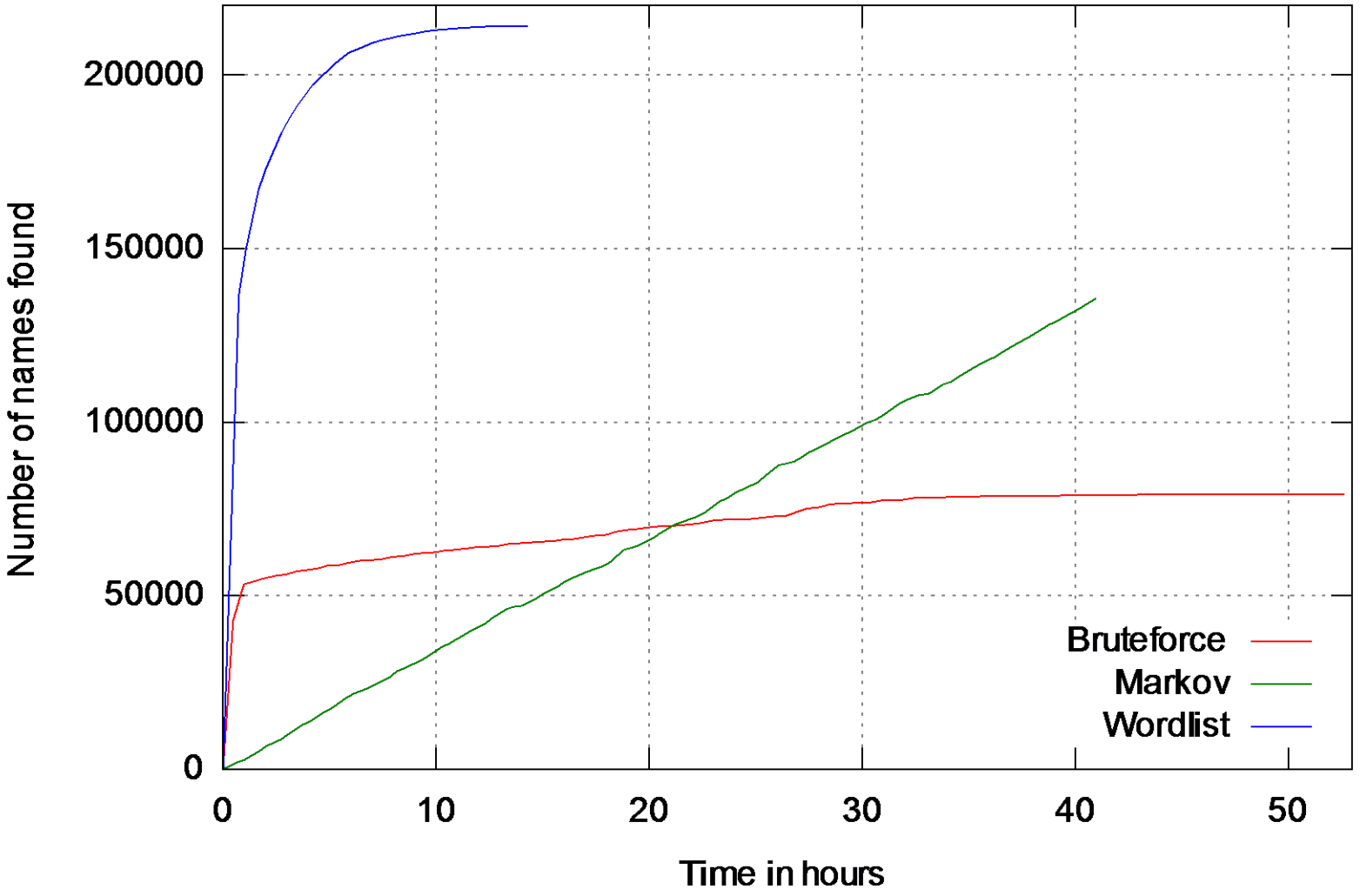
Effectiveness of Insertion Wordlist



Markov Attack

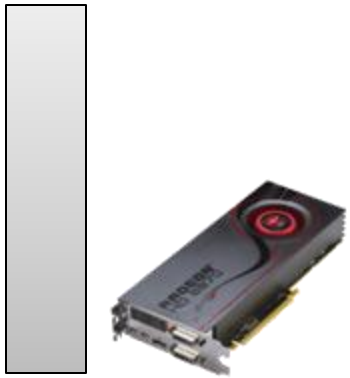
- Some strings are more probable than others
  - ‚th‘ more common in English than ‚tx‘
  - Model language with 1st order Markov chains
- Markov attack requires training
  - Use hits from brute-force and dictionary attacks
  - Markov model derived from names found
- Enumerate most probable names
  - Omit others (with given time frame)

Markov Attack

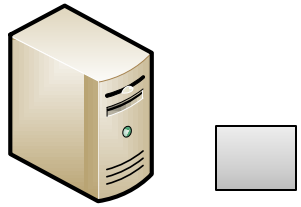


Discussion

- Reversed 65% `.com` domains after 5 days
- Server operator pays for NSEC3 with CPU load
- Adjust iterations to increase CPU workload



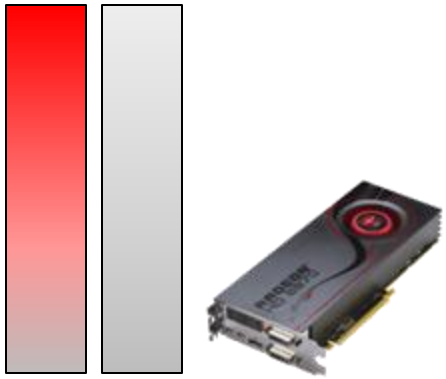
Attacker



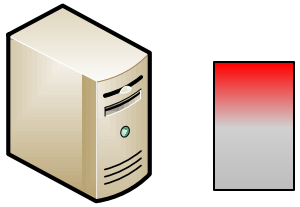
Server operator

Discussion

- Reversed 65% `.com` domains after 5 days
- Server operator pays for NSEC3 with CPU load
- Adjust iterations to increase CPU workload



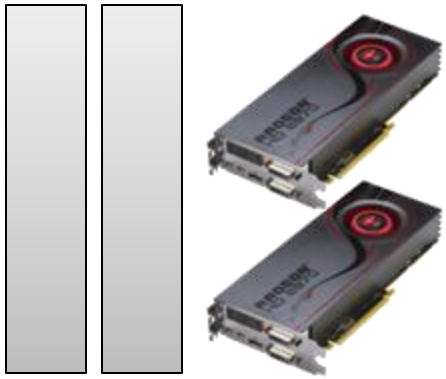
Attacker



Server operator

Discussion

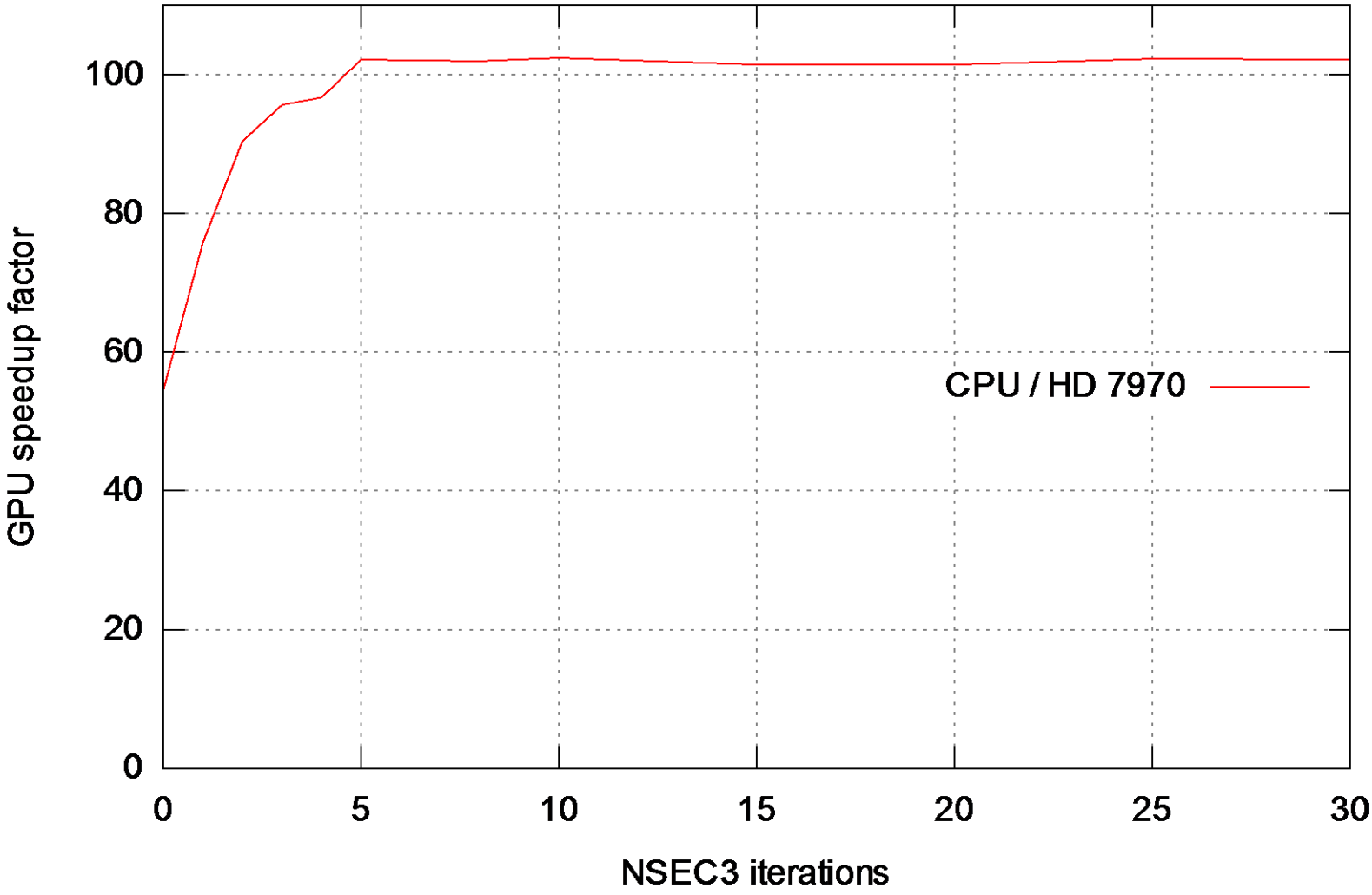
- Reversed 65% `.com` domains after 5 days
- Server operator pays for NSEC3 with CPU load
- Adjust iterations to increase CPU workload



Attacker

Server operator

Efficiency of CPU vs. GPU



Conclusions

- NSEC3 returns negative DNSSEC responses without disclosing existing domain names
- GPUs very efficient for breaking NSEC3 hashes
- Reversed 65% `.com` domains after 5 days
- Assess whether weak privacy justifies the costs
- Future work:
  - GPU-based NSEC3 accelerators for DNSSEC servers