Measuring Occurrence of DNSSEC Validation

Matthäus Wander

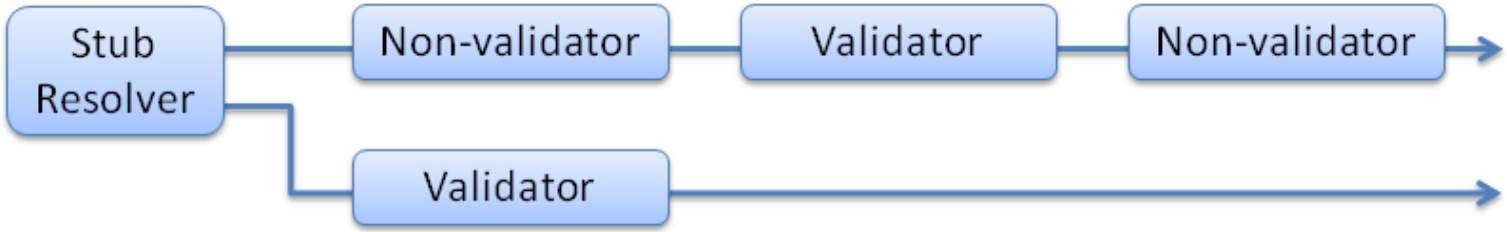
<matthaeus.wander@uni-due.de>

DNS-OARC Workshop

Toronto, October 14, 2012

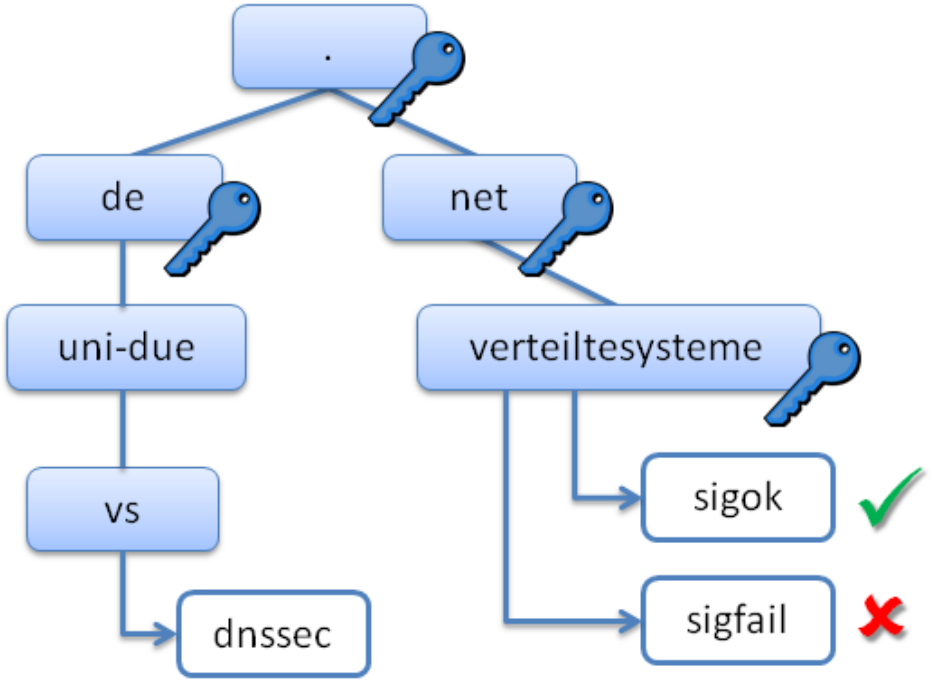
Overview

- What is the ratio of validating clients in the Web?
- Validating ⇨ rejects invalid signatures



- Outline
  - Measurement methodology
  - Result analysis
  - What's next?

Measurement Methodology

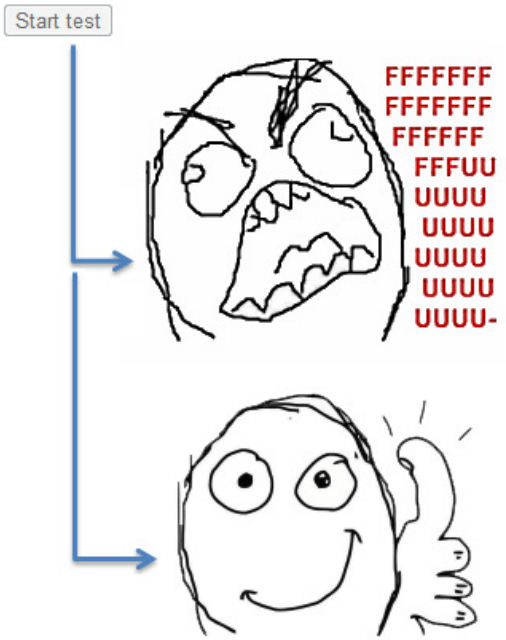


- Signed zone `verteiltesysteme.net`
  - Domain name `sigok` ✓ with valid signature
  - Domain name `sigfail` ✗ with broken signature
- Two web-based resolver tests (interactive, hidden)

Interactive Test

⇨ http://dnssec.vs.uni-due.de

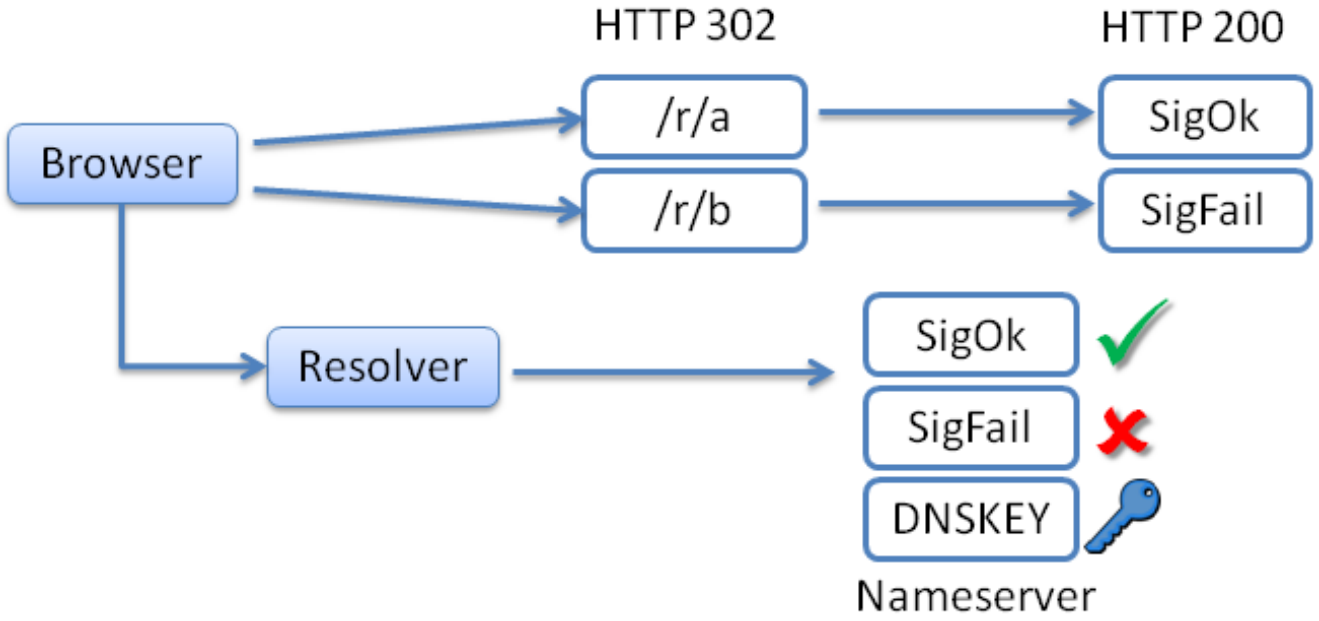
- Client-side JavaScript and images
- Load image from `sigfail` ✘ domain name
  - Success: no DNSSEC validation
  - Failure: go ahead
- Load image from `sigok` ✓ domain name
  - Success: DNSSEC validation enabled
  - Failure: inconclusive result
- Result is shown to the user and POSTed to our webserver



Hidden Test

- Load transparent 1x1 pixel images from `sigok` ✓ and `sigfail` ✗
  - Static HTML snippet (no JavaScript)

```
<img src="http://dnssec.vs.uni-due.de/r/a" alt="" height="1" width="1">
<img src="http://dnssec.vs.uni-due.de/r/b" alt="" height="1" width="1">
```



- HTTP and DNS requests logged and evaluated offline

Client Identification

- Correlate client with resolver IP address in different server logfiles

```
77.181.135.120 "GET /ok.png?aa53 HTTP/1.1" 200 413
```

```
62.53.190.69#22782: query: aa53.sigok.verteiltesysteme.net IN A -ED
```

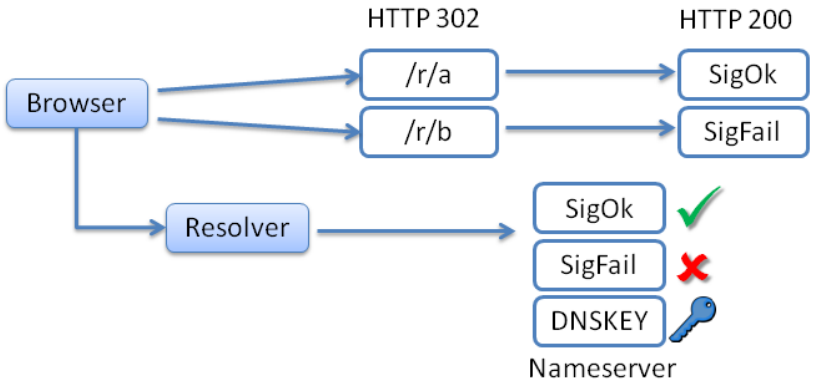
- HTTP redirect to `http://ID.sigok.verteiltesysteme.net/ok.png?ID`
  - Where `ID` := hex(SHA256(client_ip))[0:4]
  - Stateless mapping of client IP address to 16 bit ID
  - Unlikely to collide at the same time with different clients
- Pre-generated zone with 2^{19} resource record (88 MB)
  - Delivers broken signatures without nameserver adaptation
  - Vanilla zone layout

Accuracy

- `sigfail`✘ might fail to load for unrelated reasons → **false positive**
- Require loading `sigok`✓ to exclude some fault sources, e.g.:
  - failing to receive EDNS0 messages with packet size >512 bytes
  - not loading images or not following cross-domain HTTP redirects
- Some fault sources remain, e.g.:
  - network fault
  - user closes browser tab prematurely
- Another possible fault: `sigfail`✘ loads, `sigok`✓ fails
  - Harmless invalid result (false negatives are not possible)
  - Same fault pattern like a false positive (occurs with non-validators only) → estimate ratio of false positives

Result Analysis

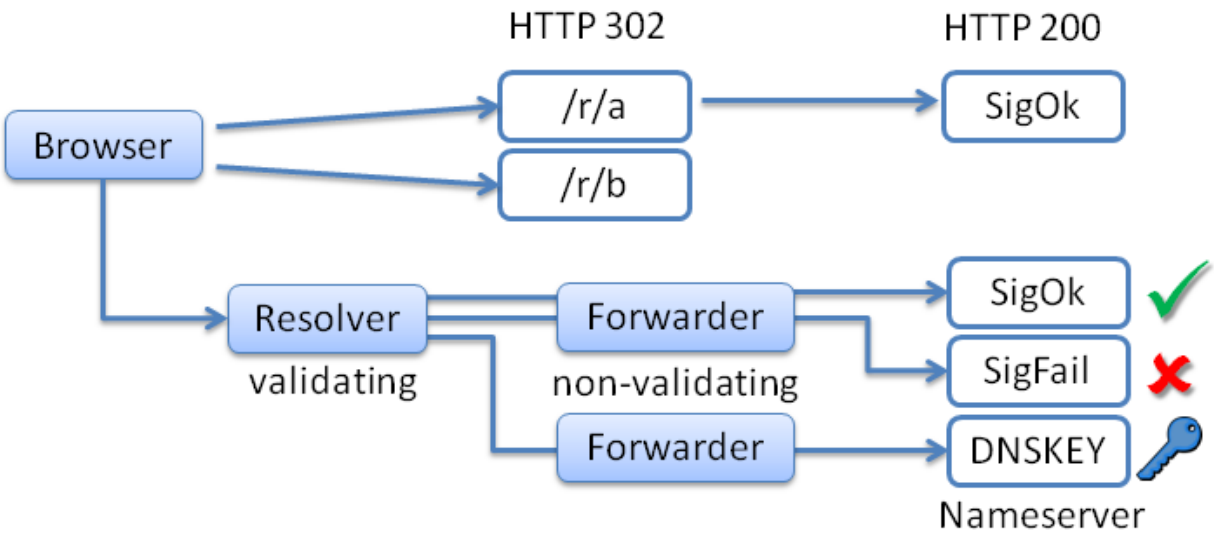
- 2.6M DNS/HTTP requests since May 2012
  - Grouped by ID into 336k Bernoulli trials
  - Δtime between requests <30s



- 220k complete trials:
  - DNS request for `sigok` ✓ and `sigfail` ✗
  - Both HTTP redirects and HTTP 1x1 `sigok` ✓ image
- Validating:
  - no `sigfail` ✗ HTTP query **OR**
  - all DNS queries without `DNSSEC OK` flag
- 116k incomplete trials:
  - Mostly same client visiting several pages + browser caching
  - 326 trials missing `sigok` ✓ → estimated 0.15% false positives

DNSKEY Missing

- Seemingly positive result but DNSKEY🔑 query is missing
- Indicates **false positive**
  - Occurred in 369 trials (0.17%)
  - Comparable to estimated ratio of false positive
- Limitation: we correlate DNSKEY🔑 via IP address, not ID
  - Might be a true positive in forwarding scenario



Data Cleaning

- Positive result but DNSKEY🔑 missing (0.17%)
- Duplicate results per IP address within 24h (59%)
- ID hash collision (<0.01%)
  - Different client IP addresses with same ID
- Inconsistent user agent (1.2%)
  - Mostly harmless e.g. same user accessing website with two browsers
  - But also: 2 clients behind NAT with **different** resolvers

⇨ one or more filter conditions applied to 130k (59%) trials

Not filtered: inconsistent IP addresses (1.5%)

- HTTP images queried from different IP addresses than redirects
- Occurred with enterprise and carrier-grade NAT

⇨ 89k results from 70k distinct IP addresses

DNSSEC Validation Ratio

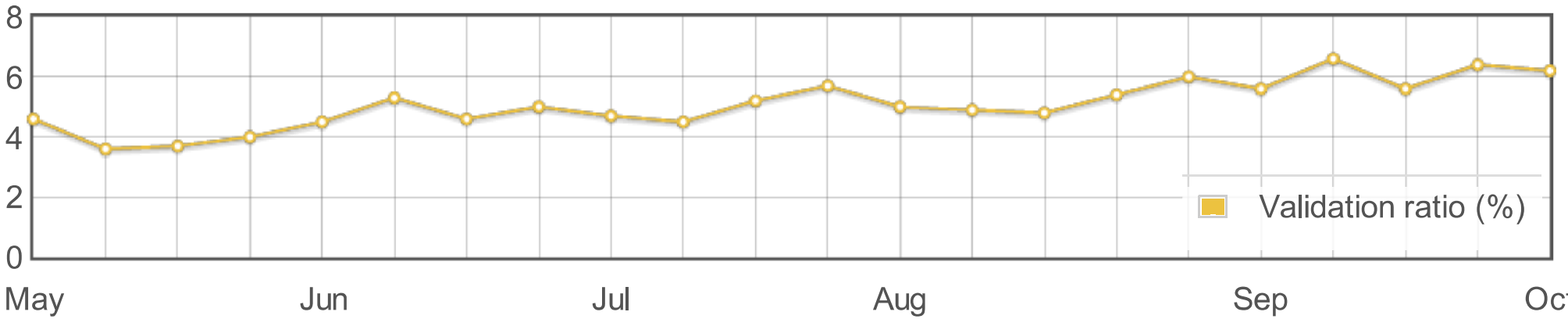


Chart 1: Validation ratio per calendar week, overall 4.7%

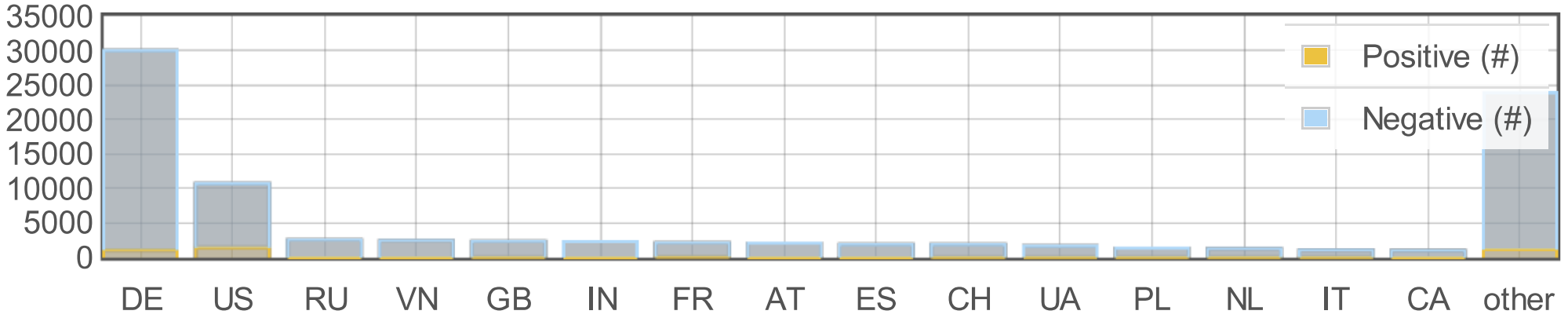


Chart 2: Absolute numbers per country

DNSSEC per Country

Results from 179 countries, 31 with >500 trials

No.	Country	Trials	Validation	σ
1.	Sweden	738	55.6%	±1.8%
2.	Czech Republic	626	35.8%	±1.9%
3.	United States	10739	13.7%	±0.3%
4.	Netherlands	1332	4.7%	±0.6%
5.	Brazil	911	4.3%	±0.7%
6.	France	2159	4.3%	±0.4%
7.	Switzerland	1894	4.2%	±0.5%
8.	Poland	1372	3.9%	±0.5%
9.	Germany	29975	3.7%	±0.1%
10.	Italy	1095	3.5%	±0.6%
11.	Indonesia	1015	2.4%	±0.5%
12.	Ukraine	1708	1.9%	±0.3%
13.	Greece	1014	1.7%	±0.4%
14.	United Kingdom	2373	1.6%	±0.3%
15.	Serbia	615	1.5%	±0.5%
16.	Philippines	752	1.2%	±0.4%

No.	Country	Trials	Validation	σ
17.	Belgium	606	1.0%	±0.4%
18.	Austria	2100	0.9%	±0.2%
19.	Australia	711	0.8%	±0.3%
20.	Russia	2606	0.7%	±0.2%
21.	Mexico	627	0.5%	±0.3%
22.	China	627	0.5%	±0.3%
23.	Canada	1066	0.5%	±0.2%
24.	Spain	1932	0.5%	±0.2%
25.	Malaysia	529	0.4%	±0.3%
26.	Romania	1039	0.3%	±0.2%
27.	India	2325	0.1%	±0.1%
28.	Vietnam	2517	0%	±0%
29.	Egypt	727	0%	±0%
30.	Turkey	651	0%	±0%
31.	Israel	591	0%	±0%

Further Results

- 36k trials (40.7%) comprise ≥2 resolvers
- 3k trials (3.5%) comprise ≥2 resolvers from different ASes
- 1.3k (1.5%) were negative but contained DNSKEY🔑 query
  - Trials with one and with multiple resolvers
  - DNSKEY🔑 query is a weak validation indicator
- Some clients use mixed validating and non-validating resolvers
  - Get SERVFAIL from validator, fall back to non-validator
  - Our test yields negative result in case of mixed validation
  - **Except** when application aborts waiting for name resolution

⇨ Effect of mixed validation needs to be investigated further

AS	Organization	Count
3320	Deutsche Telekom	10,675
15169	Google	8,045
3209	Vodafone D2	3,675
13184	Telefonica Germ.	1,983
36692	OpenDNS	1,739
4.2k others		66,297

What's next?

- Raw data (anonymized) will be available in a few days
  - http://dnssec.vs.uni-due.de
- Paper with details currently under peer-review
- Want to contribute? Add HTML snippet to your website
  - Privacy note: discloses to us client address, referer, user-agent
- Pending enhancements
  - Minimize traffic of duplicate tests
  - Generate online statistics
- Related project: VeriSign prefetch test
  - Less privacy invasive
  - http://validator-search.verisignlabs.com/