

The Impact of DNSSEC on the Internet Landscape

Matthäus Wander

<matthaeus.wander@uni-due.de>

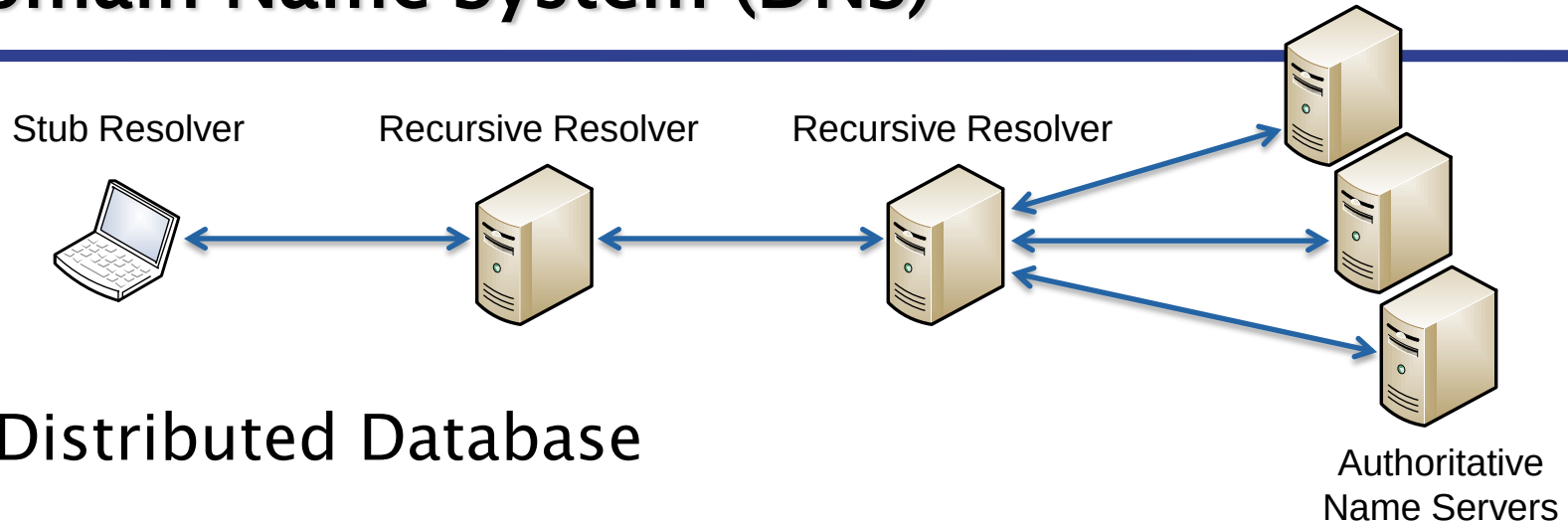
Duisburg, June 19, 2015

Outline

- Domain Name System
 - Security problems
 - Attacks in practice
- DNS Security Extensions (DNSSEC)
 - Protection and new problems
 - Adoption in practice

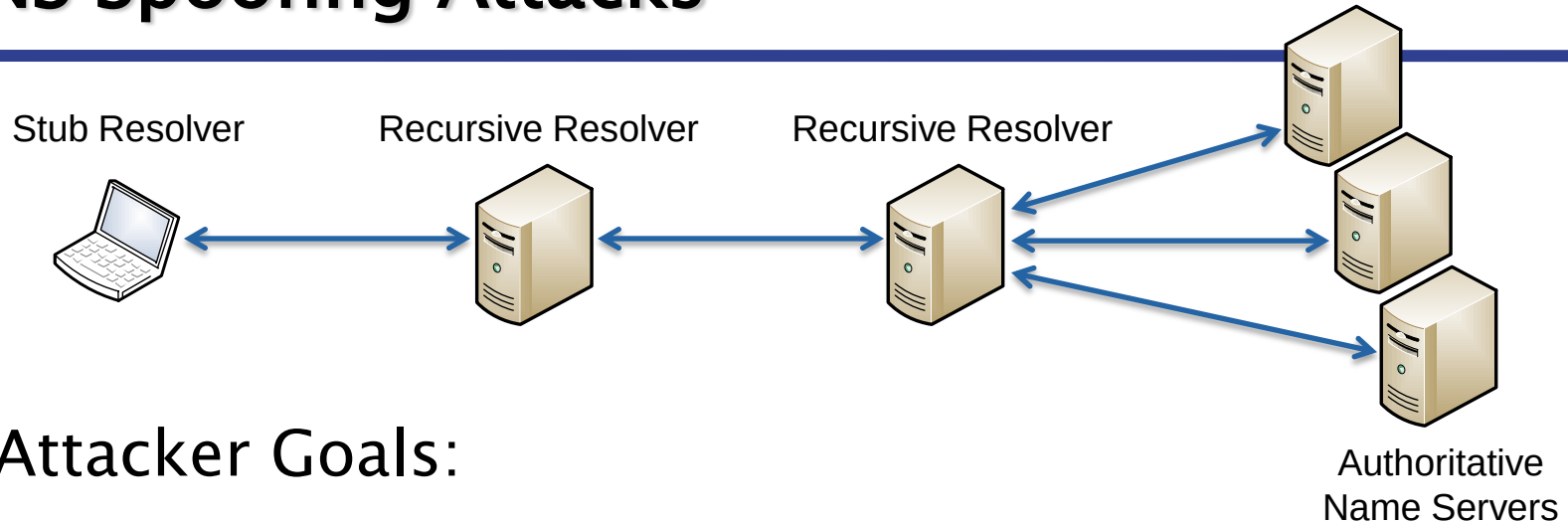
DOMAIN NAME SYSTEM

Domain Name System (DNS)



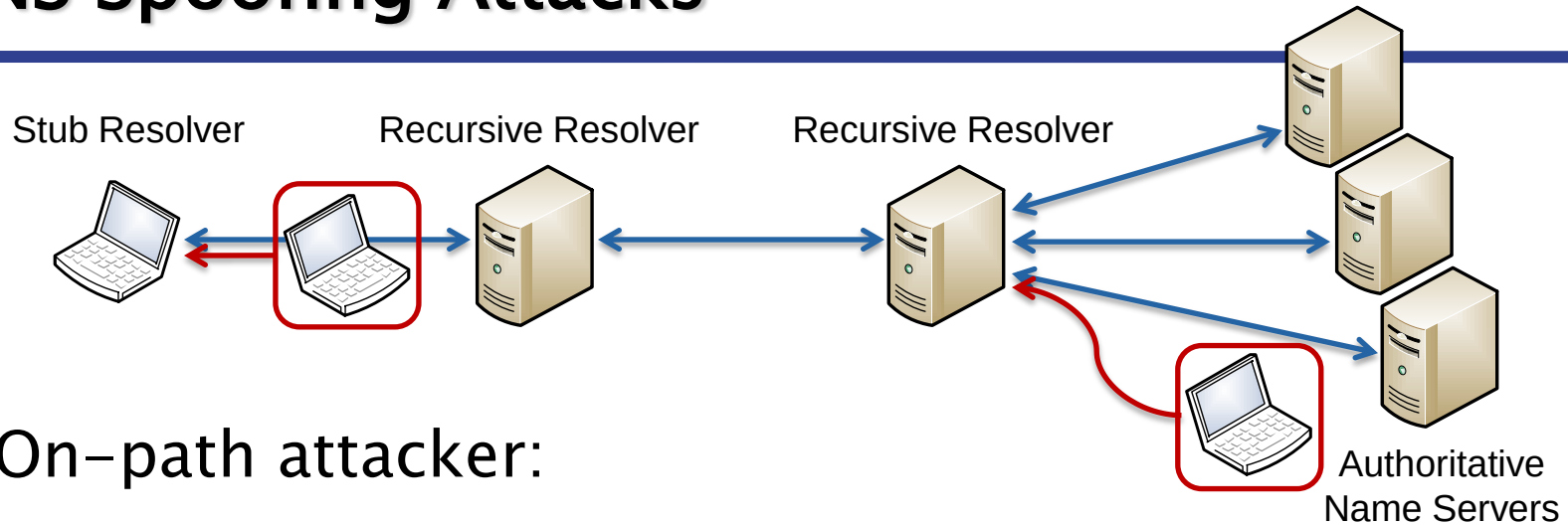
- Distributed Database
- Hierarchical Namespace
- Resolve domain names to data (e.g. IP address)
 - Data sets: resource records

DNS Spoofing Attacks



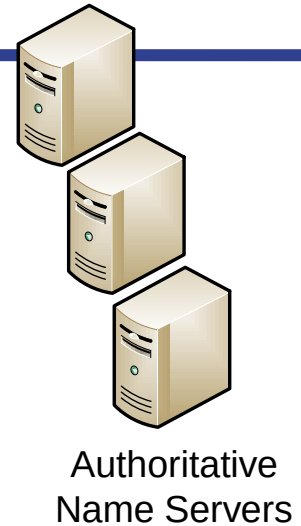
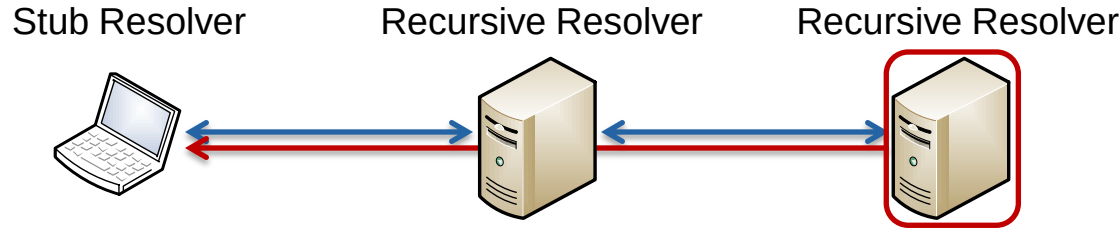
- Attacker Goals:
 - Divert application to another server
 - Deny service

DNS Spoofing Attacks



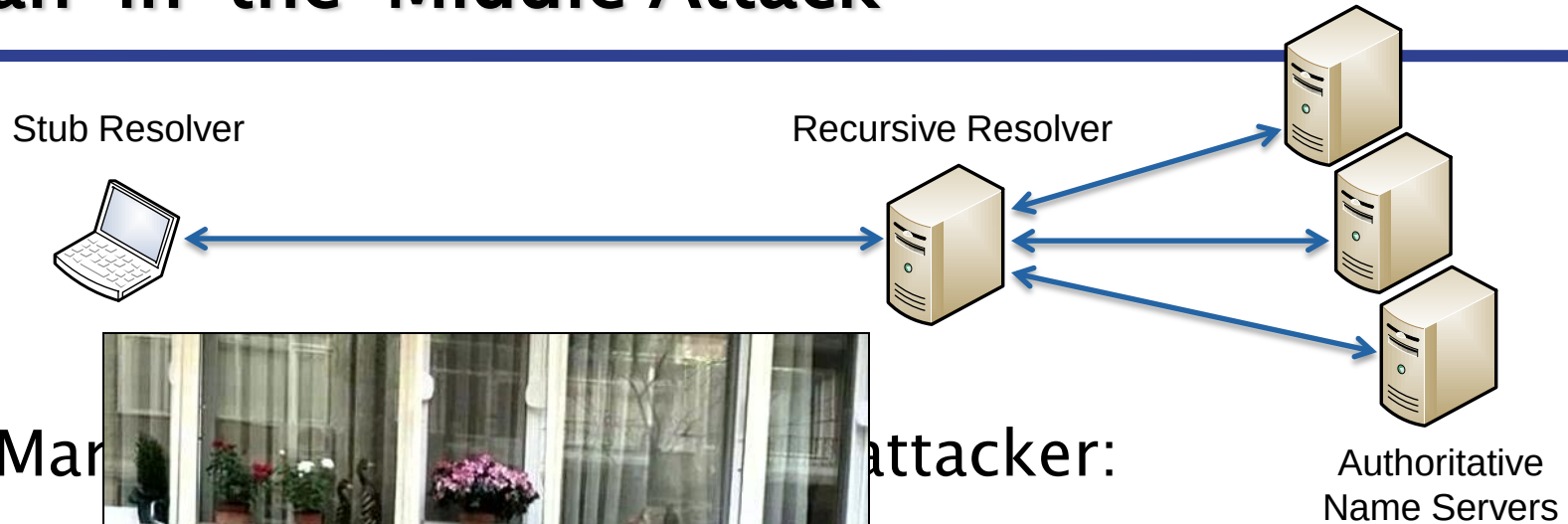
- On-path attacker:
 - Sees query, spoofs response (e.g. public WiFi)
- Off-path attacker:
 - Predicts query, spoofs response (anywhere in the Internet)

Man-in-the-Middle Attack



- Man-in-the-middle (MITM) attacker:
 - Sees query, spoofs response
- Filtering of resolver users

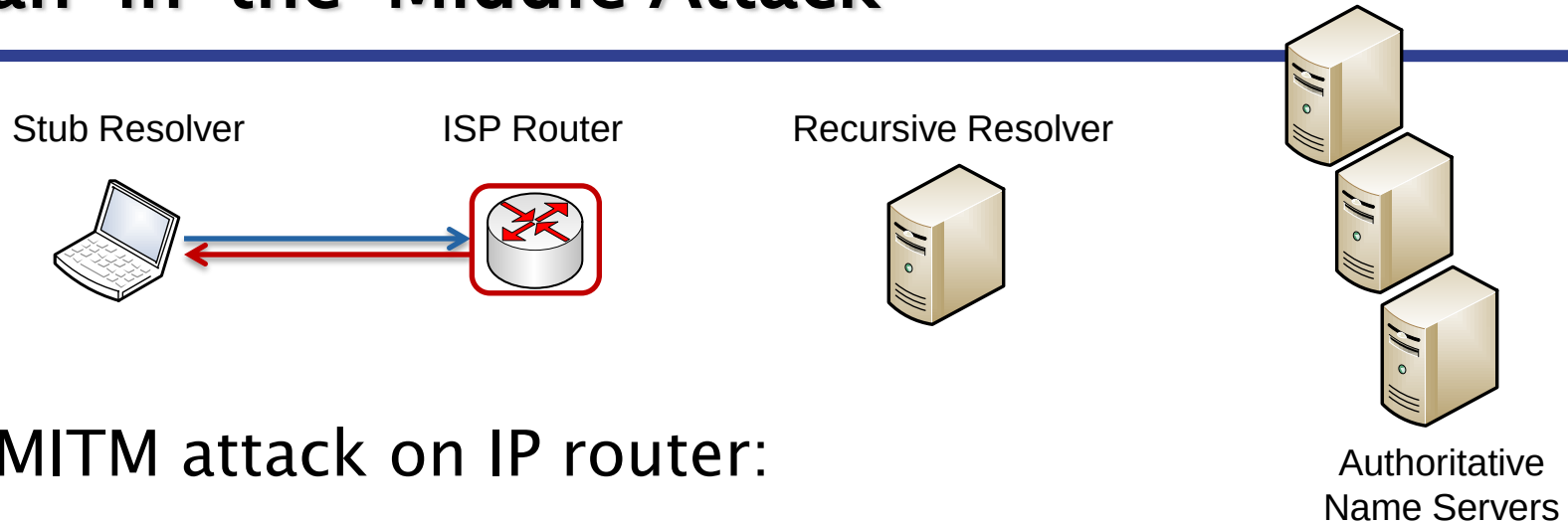
Man-in-the-Middle Attack



- Man-in-the-Middle (MITM) Attack
 - Spoofing
- Filtering

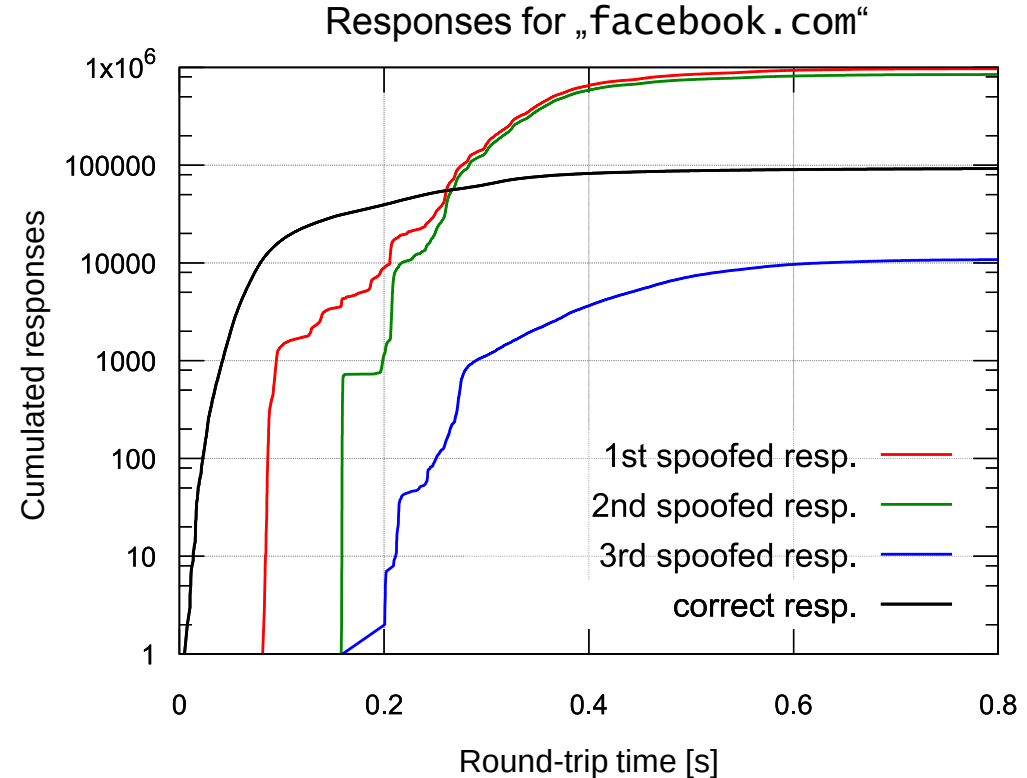
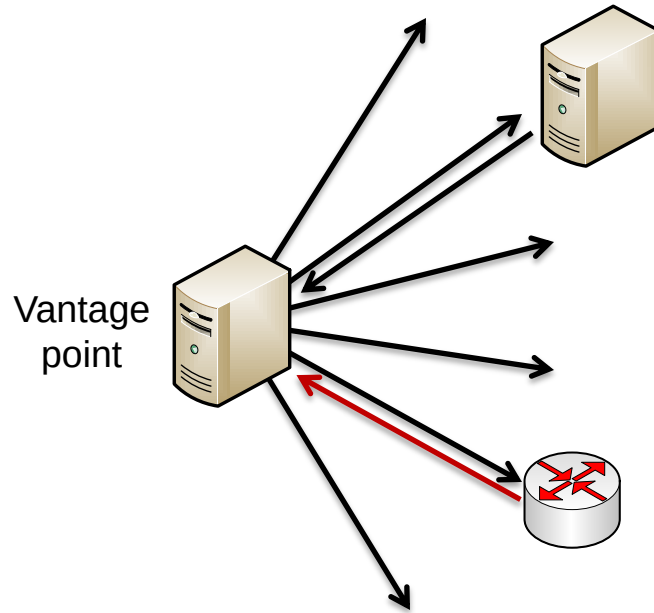


Man-in-the-Middle Attack



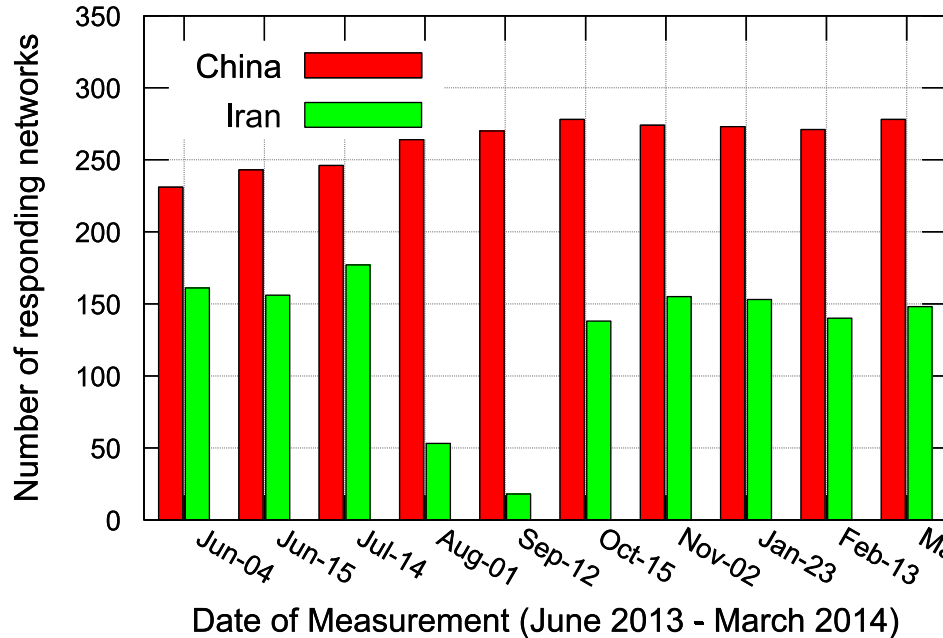
- MITM attack on IP router:
 - Deep Packet Inspection of DNS traffic
 - Router sees query, spoofs response
- Effective filtering of all DNS queries in network

Probing for DNS Injectors



DNS Injection over Time

Responses for „facebook.com“



Date of Measurement (June 2013 - March 2014)

theguardian

News Sport Comment Culture Business Money Life & style

News World news Iran

Iran's president signals softer line on web censorship and Islamic dress code

Newly elected Hassan Rouhani, an opponent of segregation by gender, says Iranians' freedoms and rights have been ignored

وزارت ارتباطات و فناوری اطلاعات
MINISTRY OF I.C.T.

صفحه نخست | نشانی و تلفن مدیران | ادارات کل ارتباطات استانها | وبپرس پس از انقلاب

یکشنبه، ۲۴ خرداد ۱۳۹۲ (۲۰۱۳/۰۳/۲۴)

صفحه نخست

- وزارت ارتباطات و فناوری اطلاعات
- پست الکترونیک
- نمونه کارهای سازمانی
- ممنوعیت اخلاقی
- آشنایی با وزارت، شرکتها و ...
- سازمان های تابعه
- ملاقات با مقام عالی وزارت
- آدمه ...

رفع فیلتر شبکه های اجتماعی در حال بررسی است

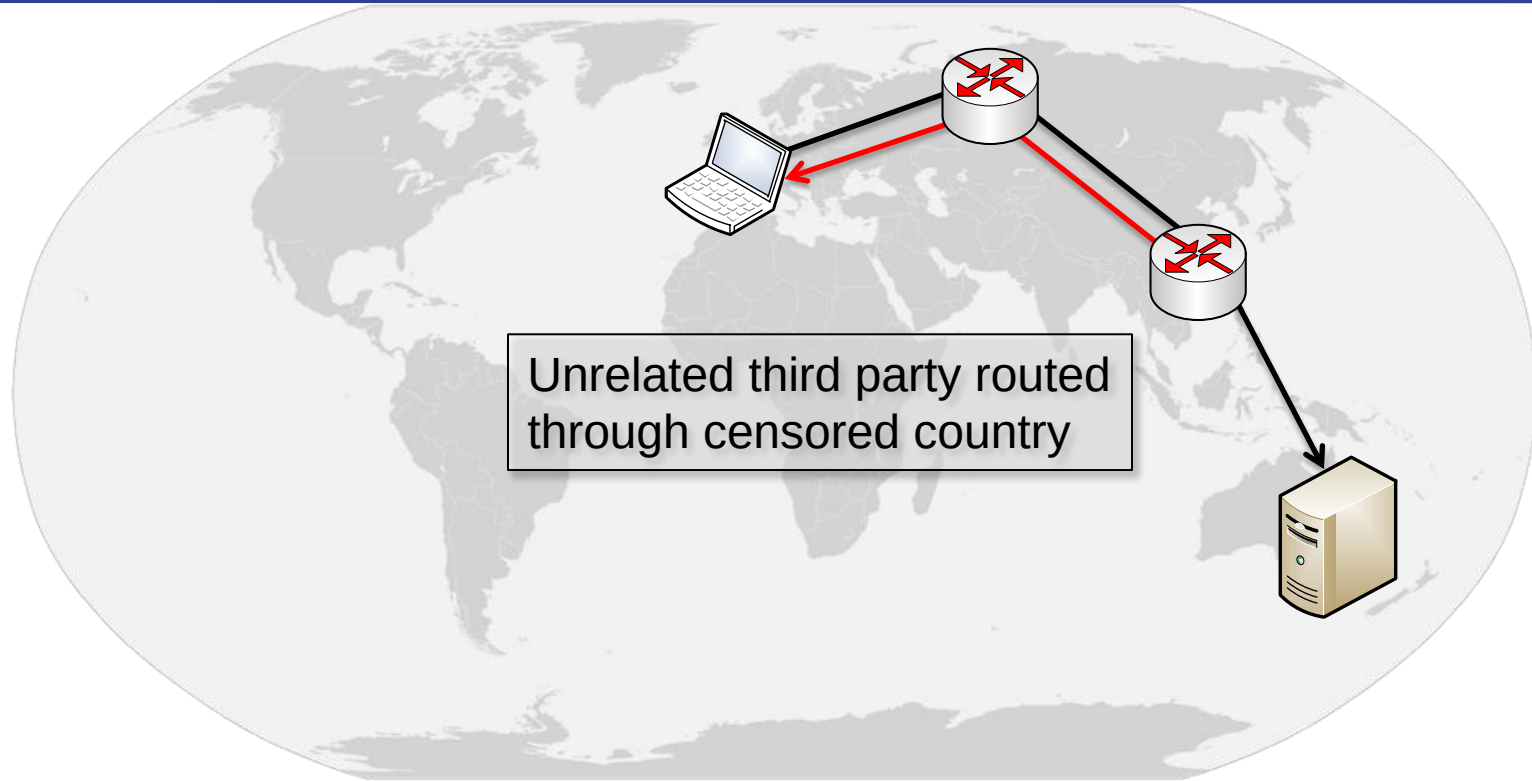
موضوع رفع فیلتر شبکه های اجتماعی، در کارگروهی خارج از وزارت ارتباطات و فناوری اطلاعات در حال بررسی است. بر اساس آخرین گزارش شده در برخی از خبرگزاریها و سایتهای خبری به نقل از دکتر واعظی وزیر محترم ارتباطات و فناوری اطلاعات، هیئت بر اینکه فیلتر وبسایت های خارجی در حال بررسی است. دکتر واعظی در جلسه مراسم ختم پدر رئیس کل بانک مرکزی در پاسخ به سوال برخی از خبرنگاران، هیئت بر اینکه فیلتر شبکه های اجتماعی در حال بررسی است. رفع فیلتر فیس بوک و واتس اپ این موضوع اتفاق افتاده است. "ایشان اظهار داشته اند من تا کنون چنین حرفی نزده ام".

به گزارش مرکز روابط عمومی و اطلاع رسانی وزارت ارتباطات و فناوری اطلاعات، اینگونه موضوعات در کارگروهی خارج از وزارت ارتباطات و فناوری اطلاعات در حال بررسی است که به محض دریافت نتایج بررسی ها و تصمیمات اتخاذ شده به طور رسمی به اطلاع عموم مردم خواهد رسید.

شایان ذکر است این موضوع نیز پیش از این توسط دکتر واعظی اعلام شده است.

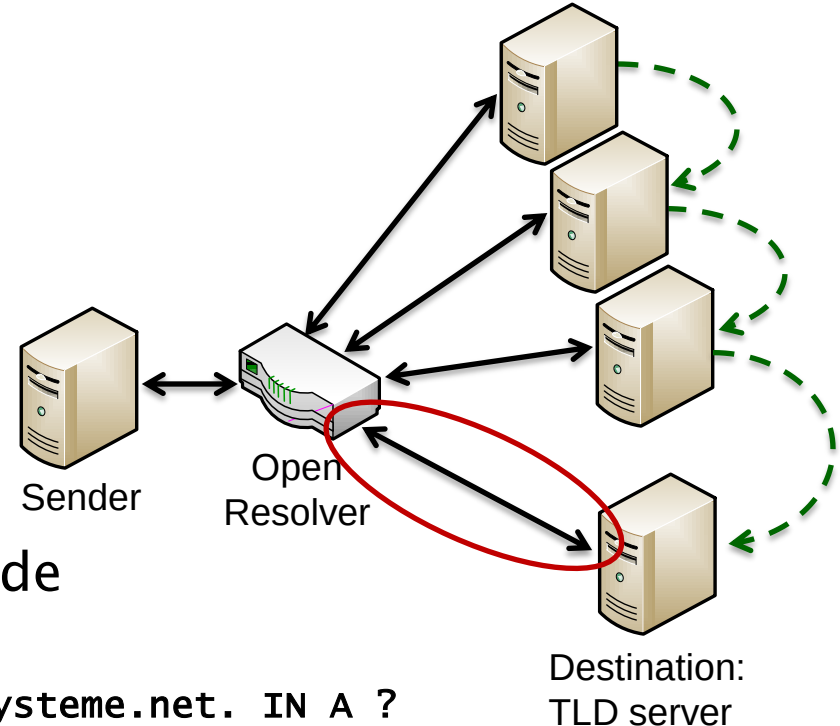
۱۵ مهر ۱۳۹۲
تعداد کلیک: ۸,۲۵۱

Impact Assessment on Third Parties



Open Resolver Measurement

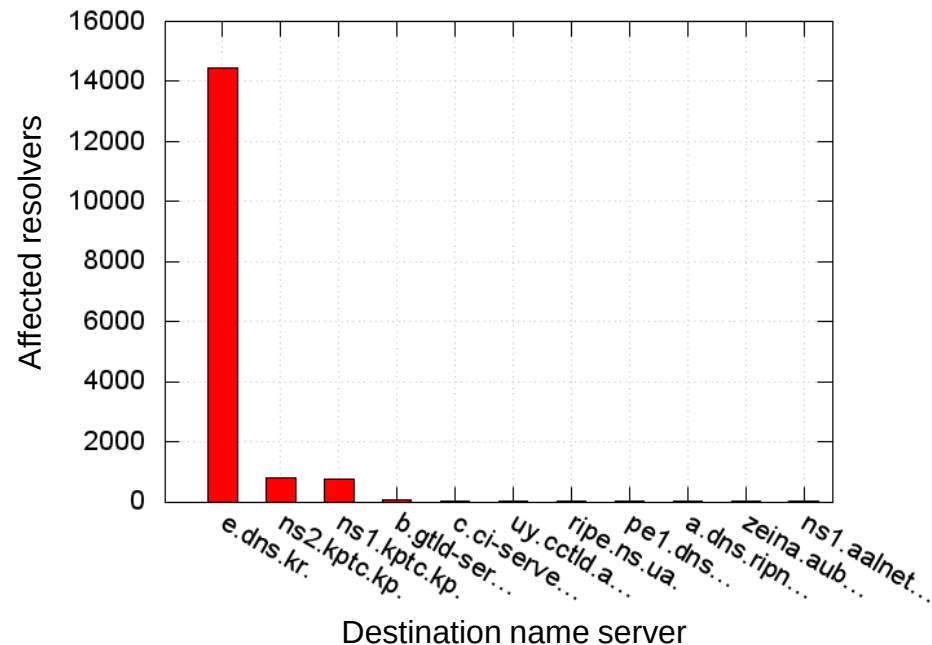
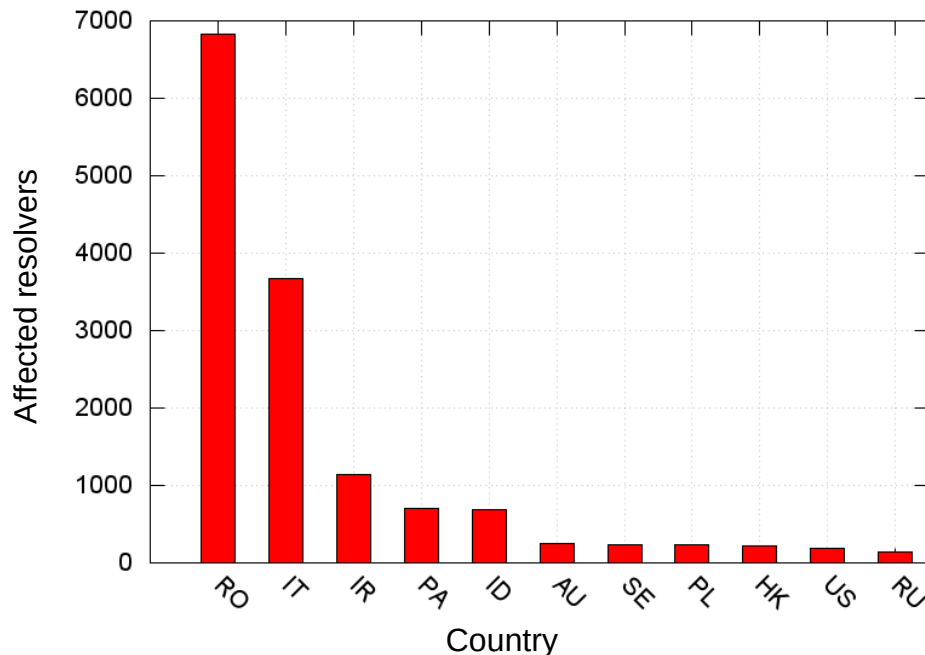
- Worldwide impact of Chinese DNS injection
- Top-level domains
 - 1144 name servers
- Multiple vantage points
 - 255k open resolvers worldwide



`www.minghui.org.s1.verteiltesysteme.net. IN A ?`

Open Resolver Results

- 15k resolvers (6%) affected by Chinese DNS injection
- 14k affected when contacting „e.dns.kr“

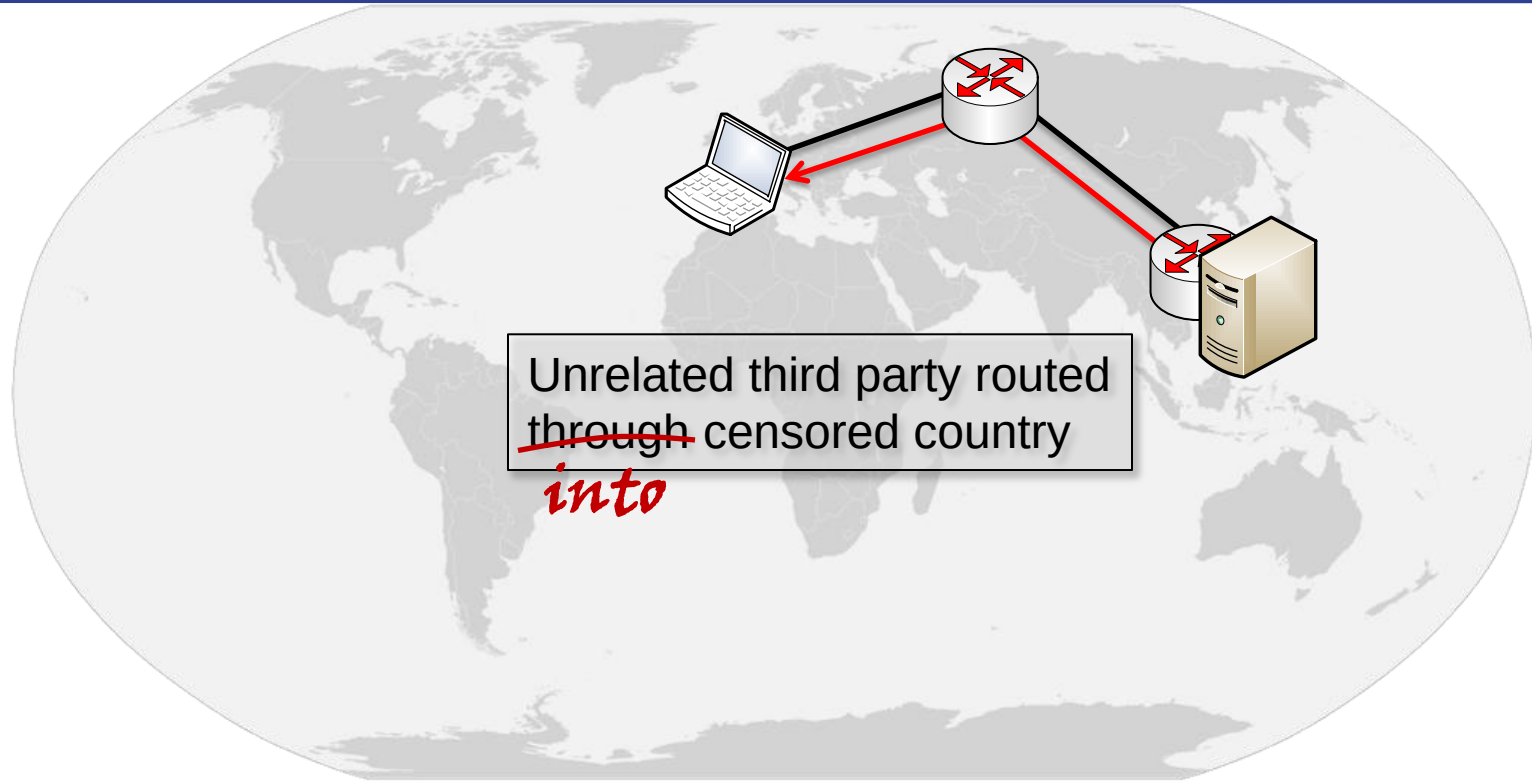


.kr Top-Level Domain Servers

Published in:
IEEE Access, 2014

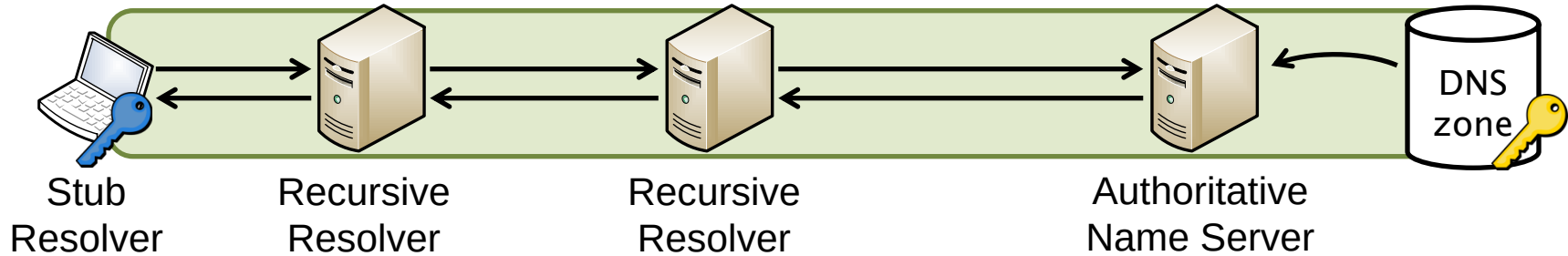


Impact Assessment on Third Parties



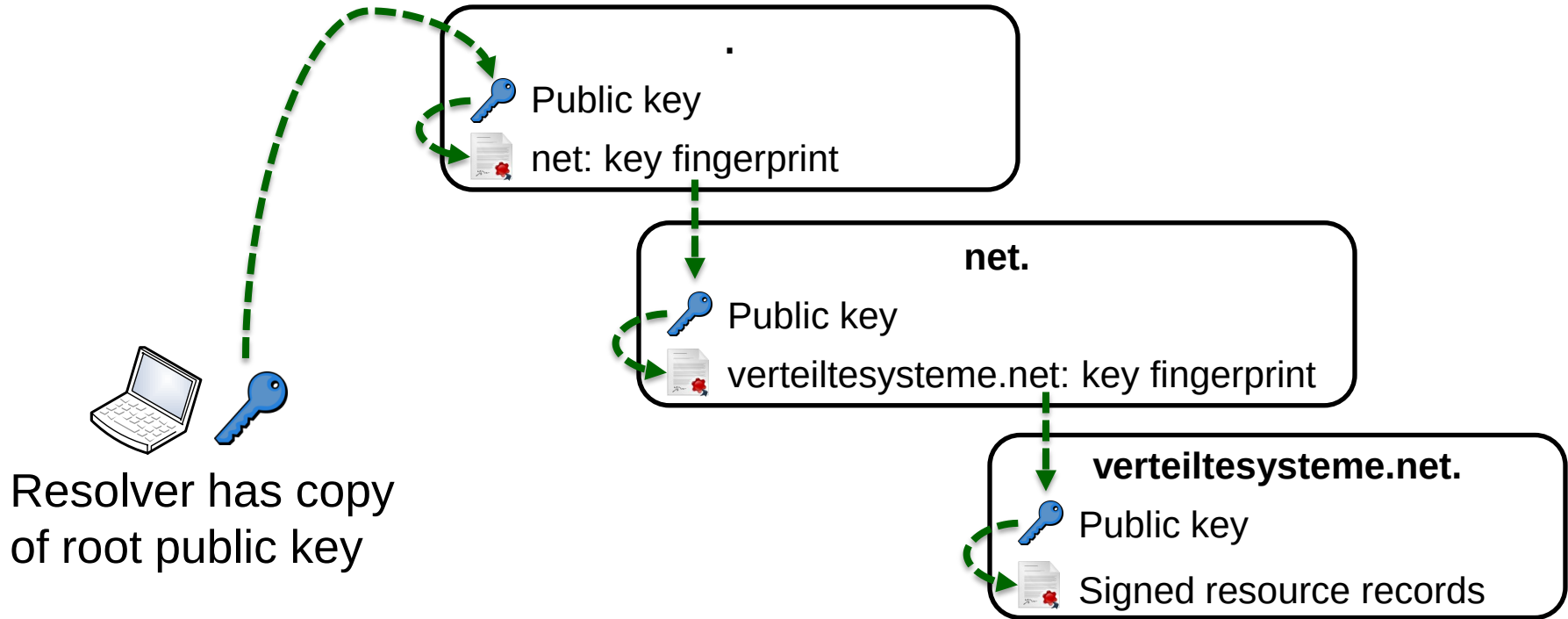
DNSSEC

Concept

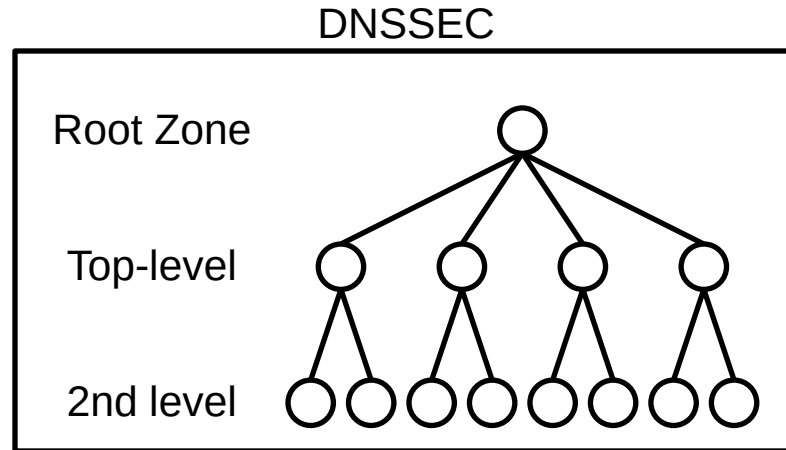


- Security goals: data integrity and authenticity
- Signatures  pre-generated over DNS data sets
- End-to-end security between **validator** and **signer**

Public Key Distribution

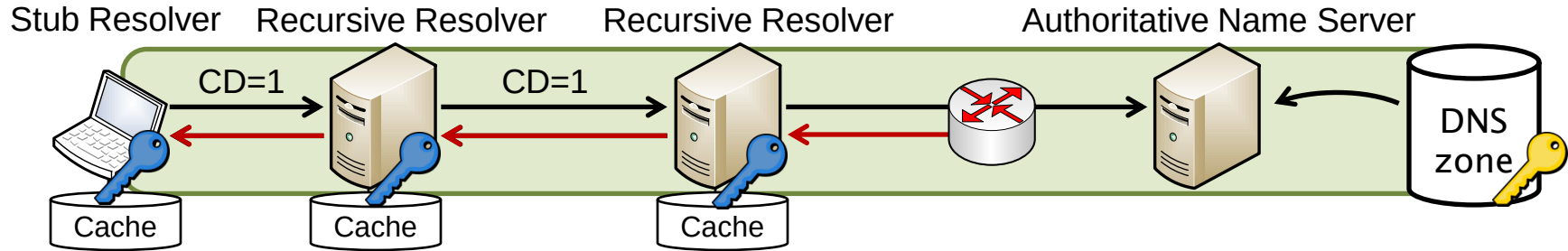


Trust Model



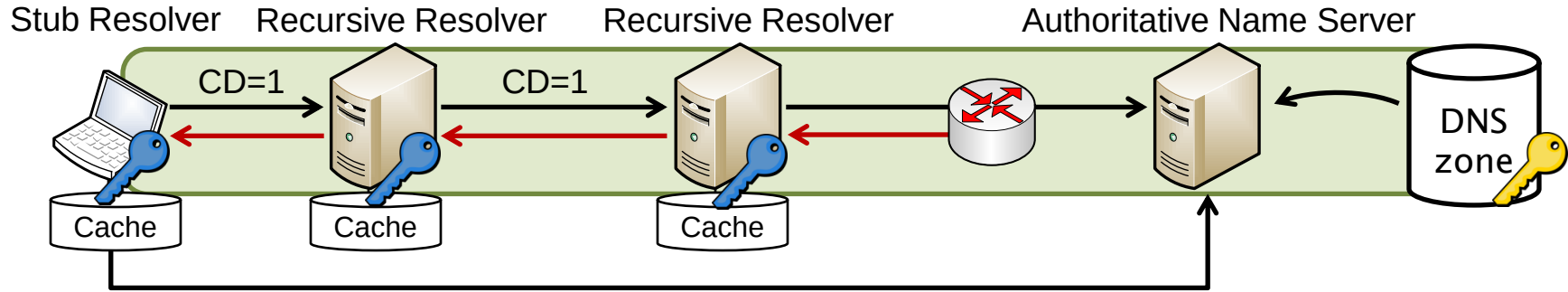
- Authority limited to subnamespace
- Powerful root authority

Cache Lock-in



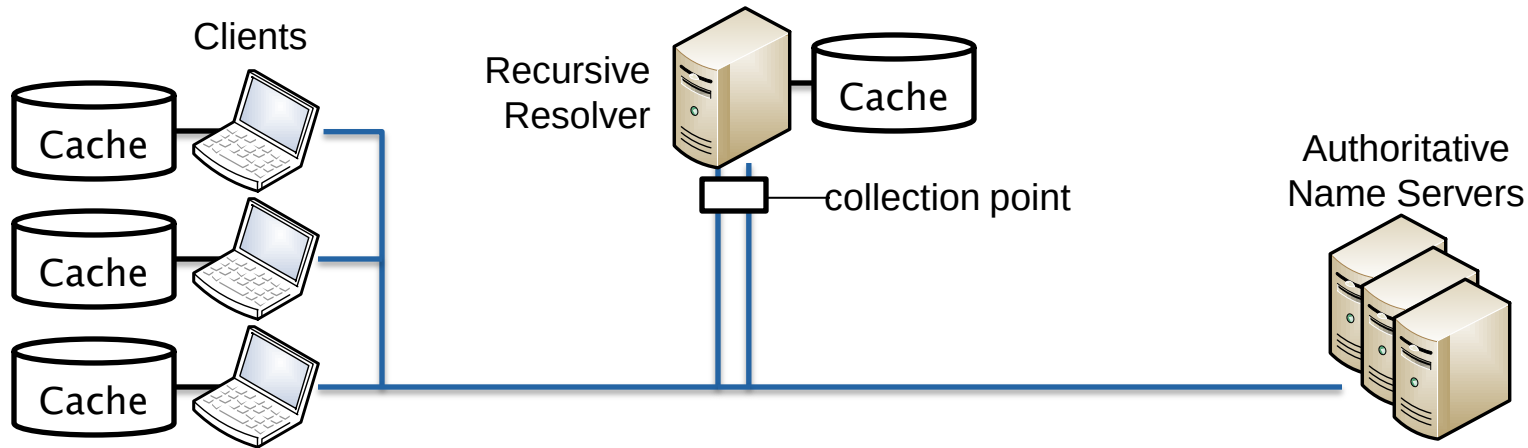
- End-to-end security: validation on end host
 - Independent of validation failures on intermediate resolvers
- Request response without DNSSEC validation
 - Problem: cache lock-in

Cache Lock-in



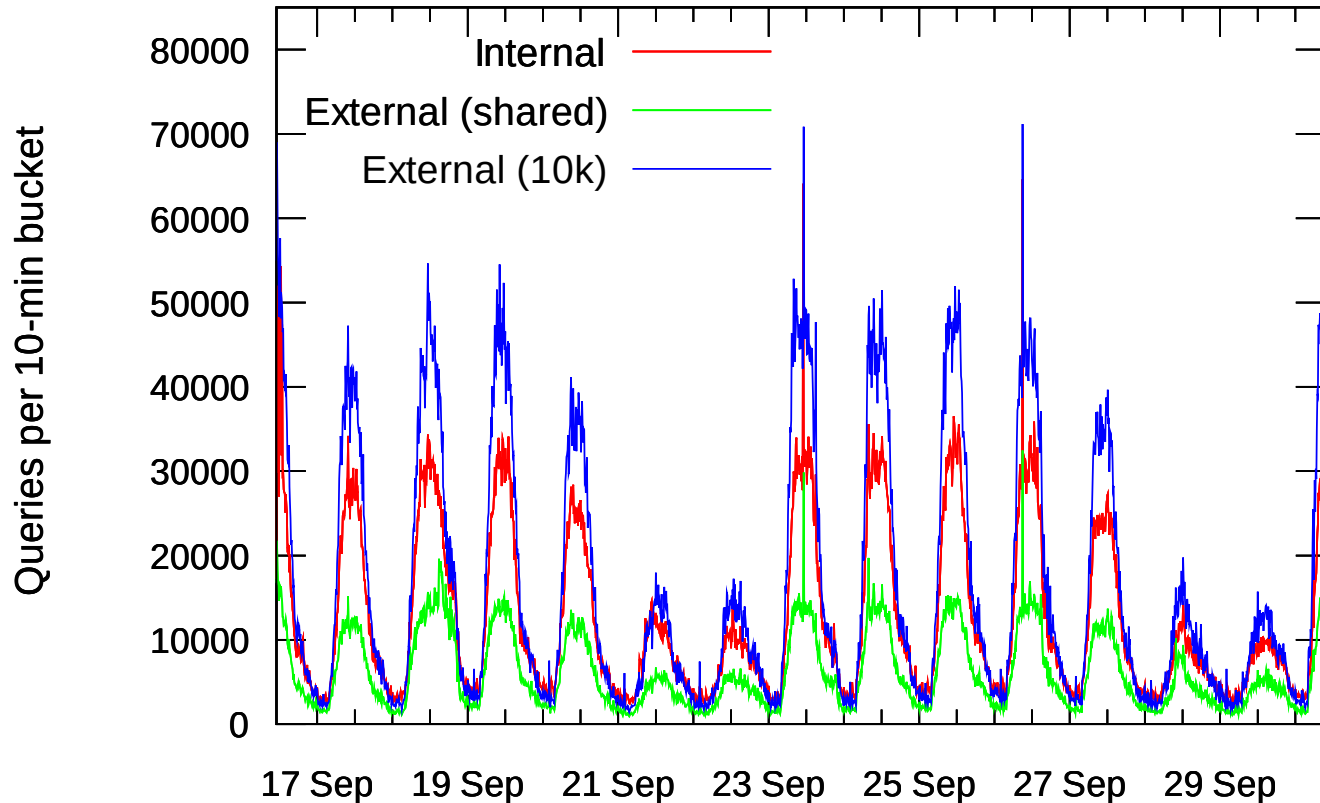
- Omit intermediate resolvers
- Effectiveness of intermediate caching?

Trace-driven Simulation of Cache Effectiveness



- Cache models:
 - Shared cache in front of 10k clients
 - 10k independent caches

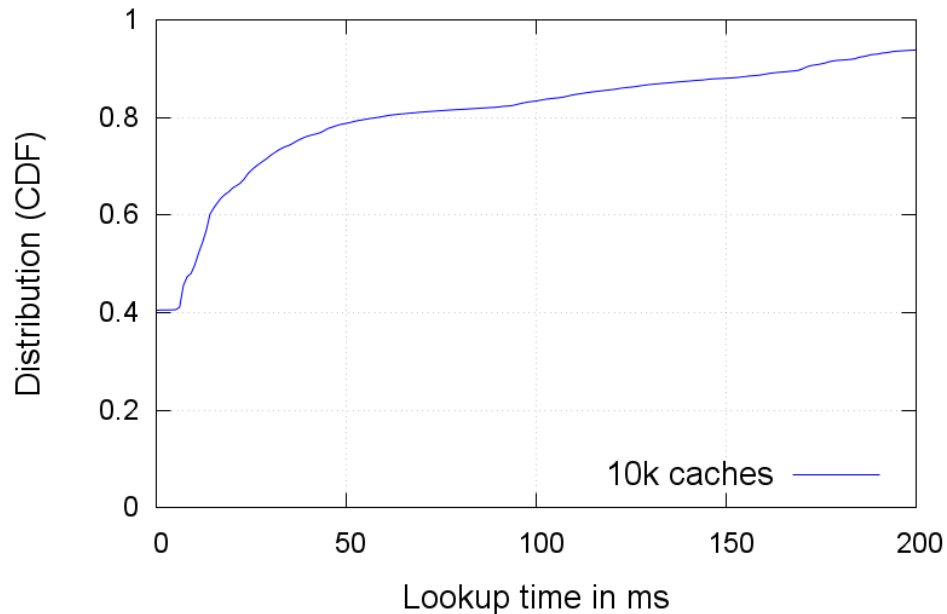
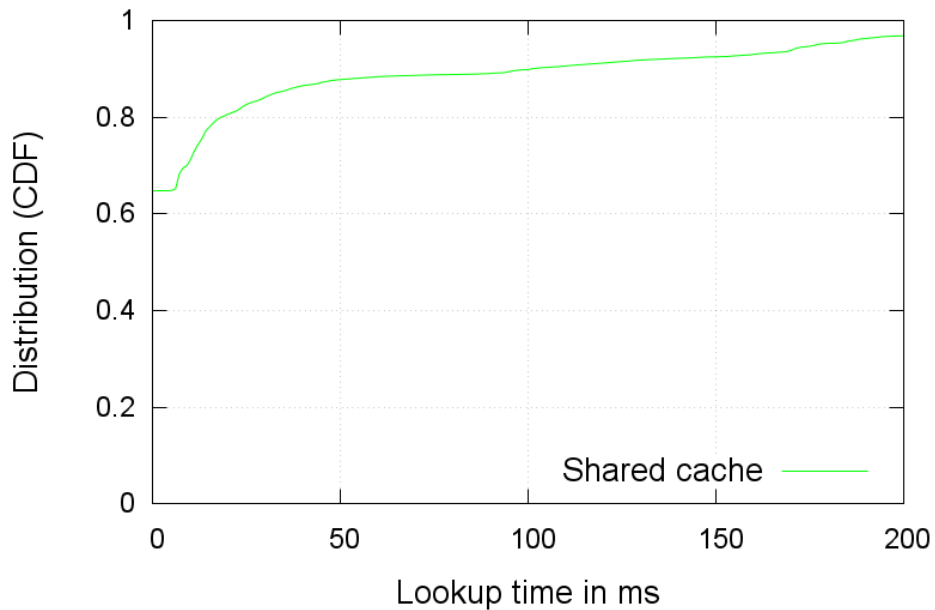
Bandwidth Overhead



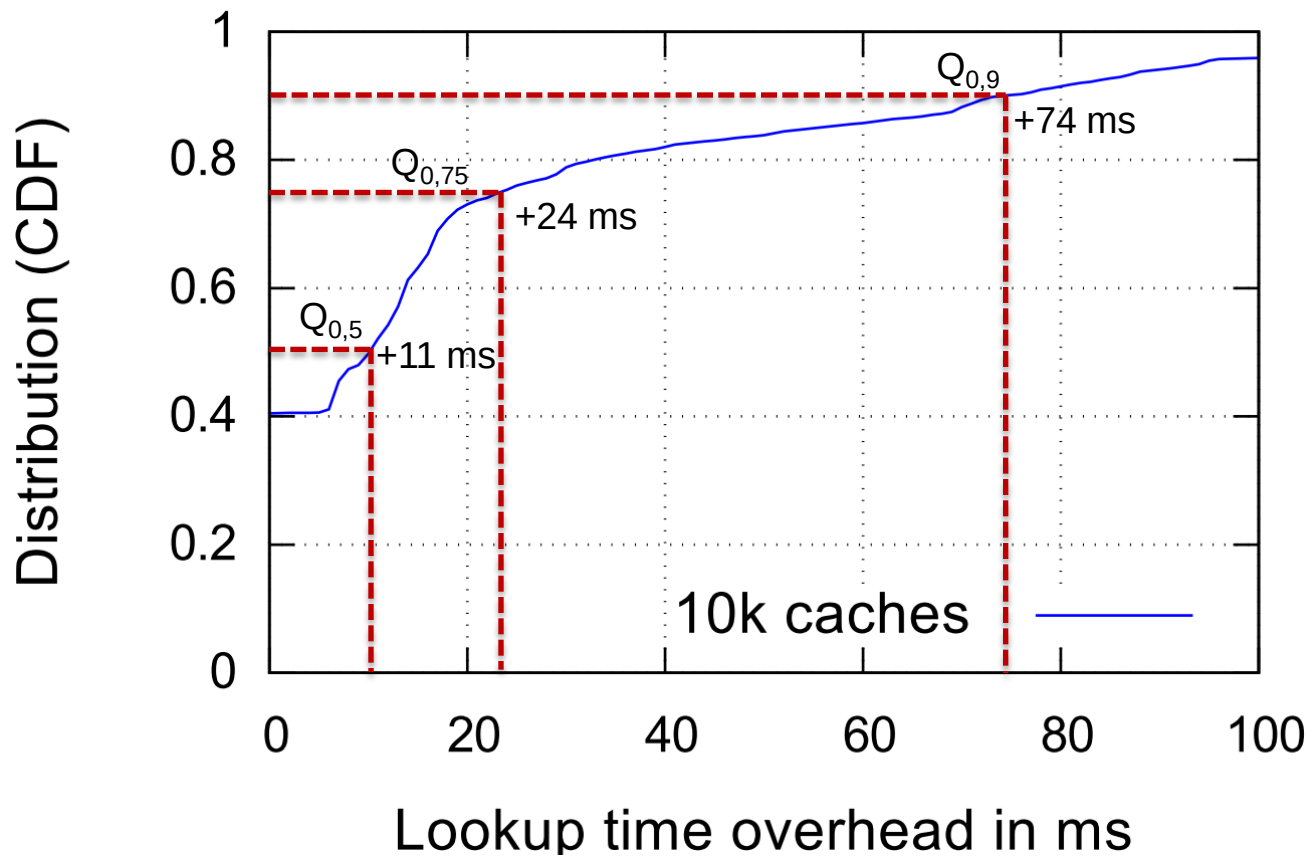
External traffic:

- Shared cache: 2.44 GBytes
- 10k caches: 7.55 GBytes

Latency Overhead



Latency Overhead

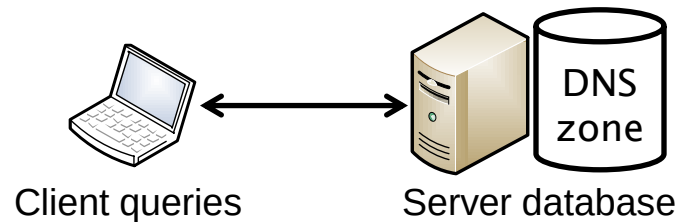


⇒ Utilize intermediate DNS caches

⇒ Fall back to autonomous resolution on failure

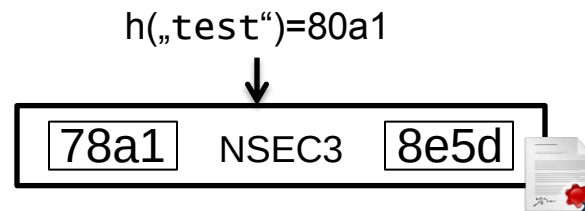
Privacy and Confidentiality

- Client: no privacy improvement
 - Cleartext DNSSEC messages



- Server: discloses hash values of zone contents

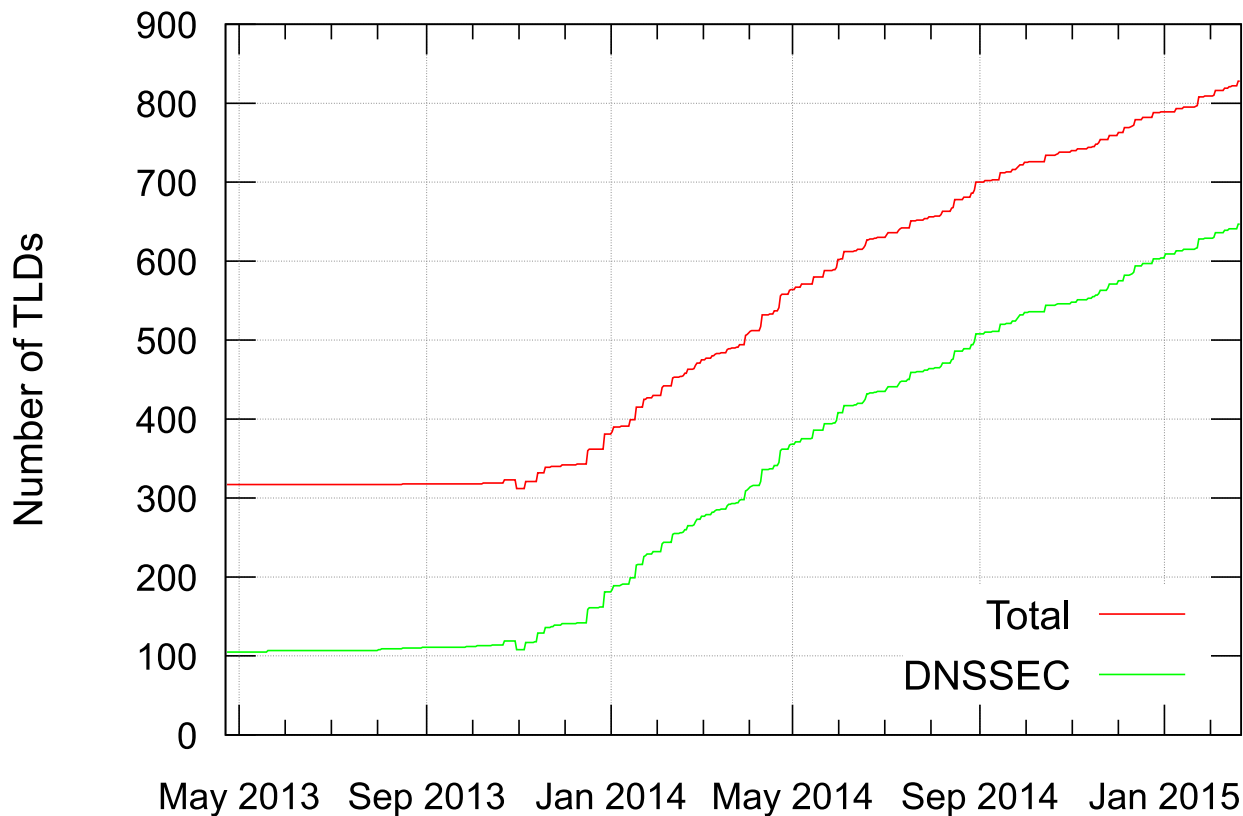
- Server proves non-existence
- Hashing supposed to hide names



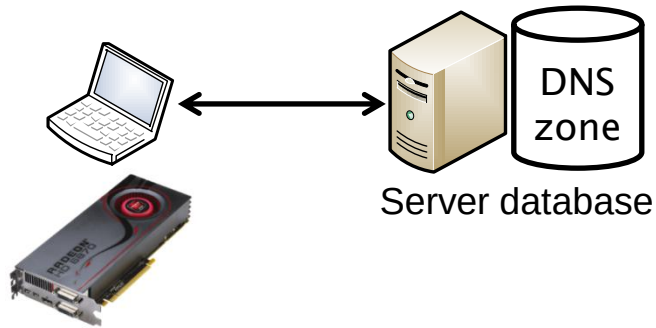
- Break NSEC3 hash values with GPU-based attacks
 - One GPU reveals 65% .com hash values in 5 days

ADOPTION OF DNSSEC

Signed Top-Level Domains



Signed Second-Level Domains



TLD	Domains
1. nl	2,279,702
2. br	566,694
3. cz	448,984
4. com	426,182
5. se	349,514
6. eu	320,311
7. fr	205,662

8. no	119,759
9. be	92,385
10. net	81,391
11. org	46,382
12. ovh	29,372
13. nu	21,126
14. de	20,004

Total: 5,146,705 signed domains

Algorithms and Key Sizes

Survey of
3.4M domains

Algorithm	Domains
RSA/MD5	0
DSA/SHA-1	2,176
RSA/SHA-1	1,547,782
RSA/SHA-256	1,869,157
RSA/SHA-512	1,100
GOST R 34.10-2001	30
ECDSA P-256/SHA-256	29
ECDSA P-384/SHA-384	19

>99% use RSA

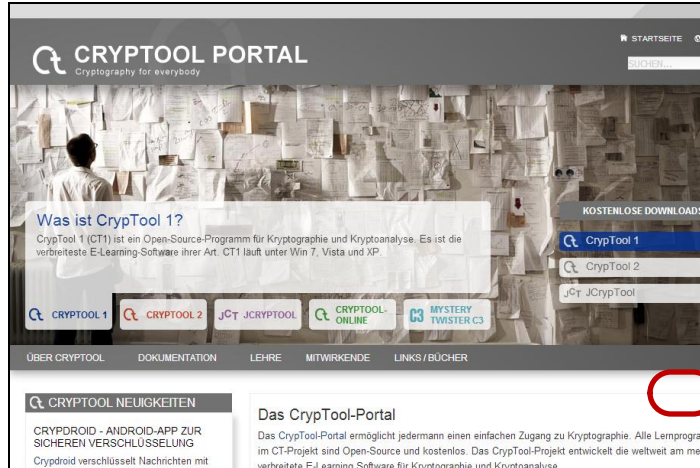
RSA Key Size	Domains
512	13,674
768	25
1024	3,152,420
1032	535
1152	108
1280	185,825
1304	105
1536	106
2048	59,907
2560	1
3072	3
4096	5,135

Shortest RSA key per domain

Result	Domains
No DNSKEY (dangling DS)	17,751
No trusted DNSKEY (dangling DS)	1,066
No RRSIG for trusted DNSKEY	238
Signature expired	2,138
Signature verify failure	5
Validation failure	21,198
Validation success	3,416,700

0,6% domains fail validation

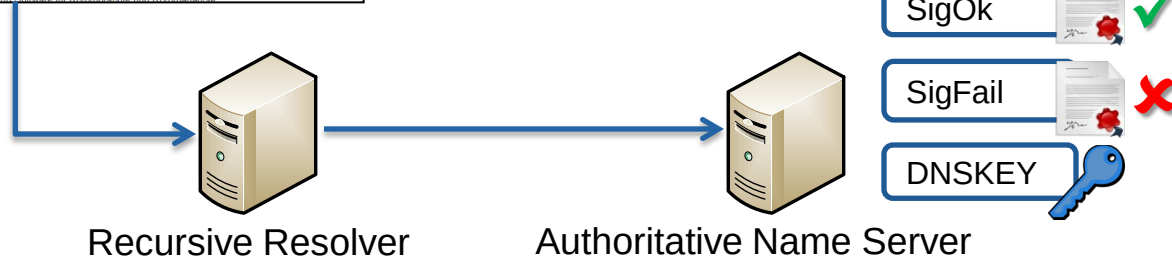
Measuring Validating Clients



→ <https://SigOk.verteiltssysteme.net/a.png>

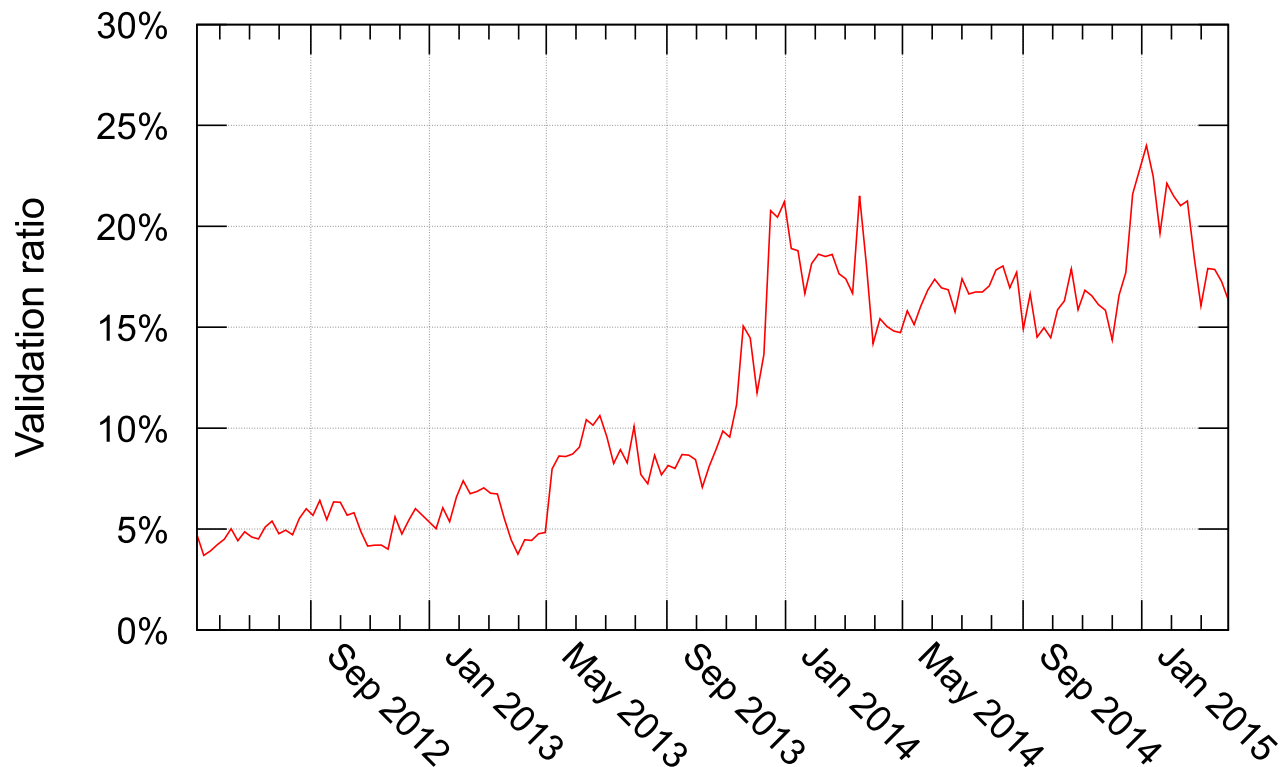
→ <https://SigFail.verteiltssysteme.net/b.png>

○ Invisible 1px images



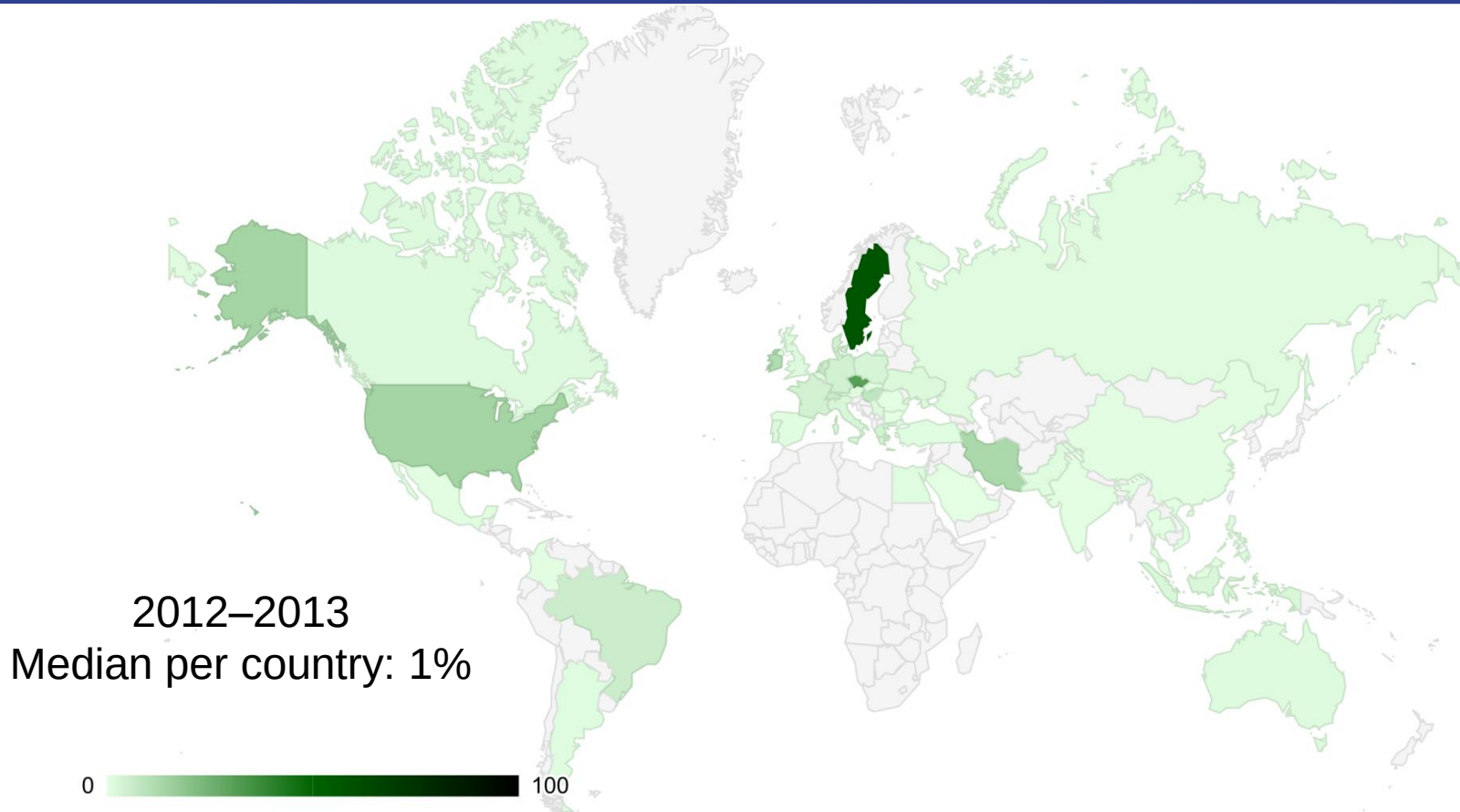
DNSSEC Validation

- 841k test results from 557k distinct IP addresses

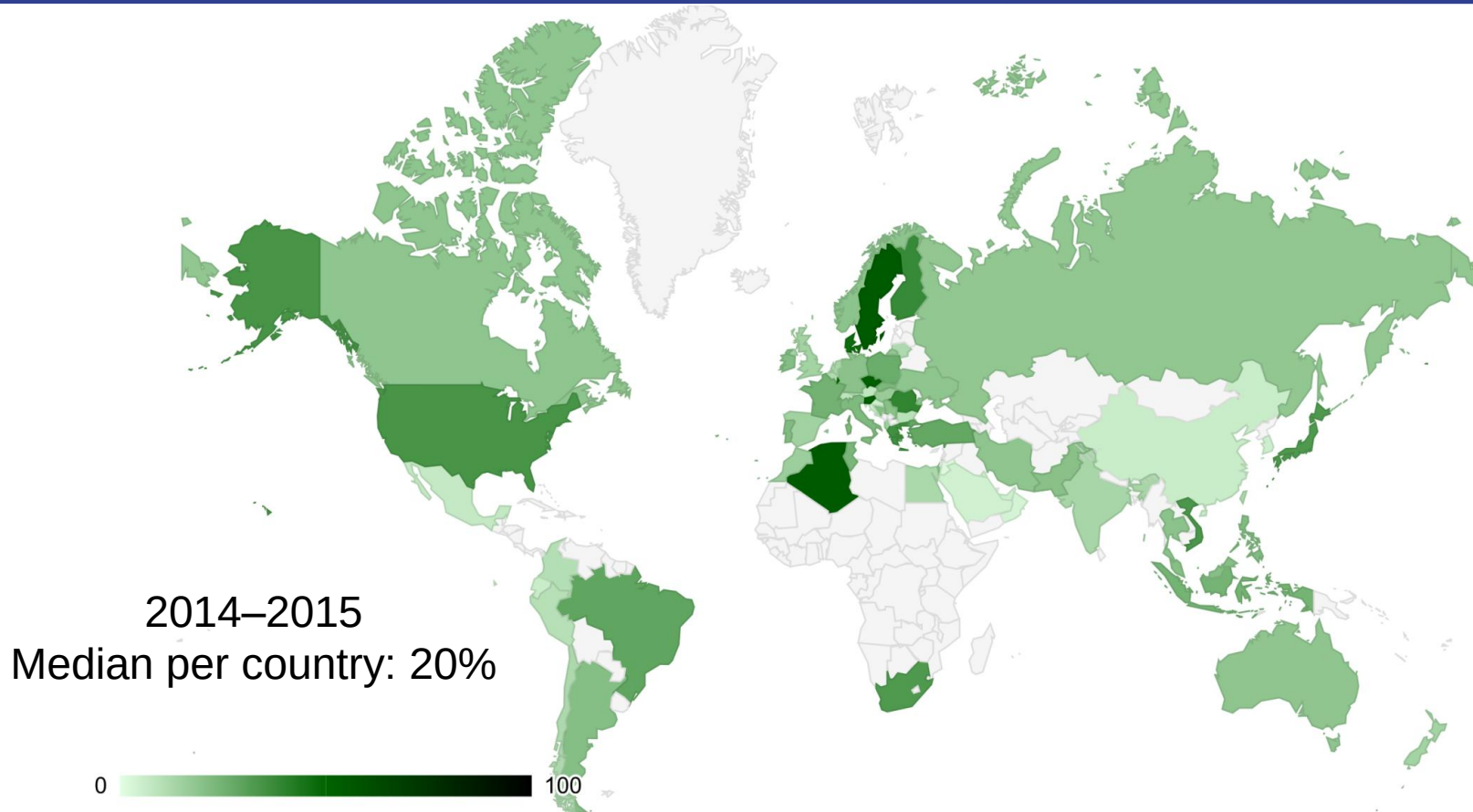


DNSSEC Validation per Country

Published in:
LNCS PAM, 2013



DNSSEC Validation per Country



Conclusions (1 / 2)

- DNS spoofing used for Internet filtering
 - 6% resolvers worldwide affected by Chinese DNS injection
 - Evidence of router-based DNS injection in Iran
 - Political changes in DNS filtering observable from outside
- DNS caching causes lock-in on bogus data
 - Trace-driven simulation shows moderate benefit of caching
 - Suggestion: omit DNS caches on DNSSEC validation failure

Conclusions (2/2)

- DNSSEC secures data integrity and authenticity
 - Hashing is ineffective for protecting the DNS database
- First-time survey of all DNSSEC signed domains
 - 5M signed domains: >99% use RSA, 0.6% are broken
- 3-year measurement of validating clients
 - Worldwide increase of DNSSEC adoption
 - Varies by country (median 20%)

Referenced Publications

- M. Wander, T. Weis:
Measuring Occurrence of DNSSEC Validation,
Passive and Active Measurement (PAM), LNCS Springer, 2013.
- M. Wander, C. Boelmann, L. Schwittmann, T. Weis:
Measurement of Globally Visible DNS Injection,
IEEE Access, 2014.
- M. Wander, L. Schwittmann, C. Boelmann, T. Weis:
GPU-based NSEC3 Hash Breaking,
IEEE NCA, 2014. Awarded **best student paper**.