Hijacking DNS like it's 2016

Amit Klein
Fraunhofer SIT

ABOUT THIS RESEARCH

- Sponsored by Fraunhofer SIT
  - SIT = Security in Information Technology
  - Headed by Prof. Dr. Michael Waidner
- Supervised by Dr. Haya Shulman
- Conducted by Amit Klein
  - That’s me ;-)
  - Part of M.Sc./Ph.D. thesis

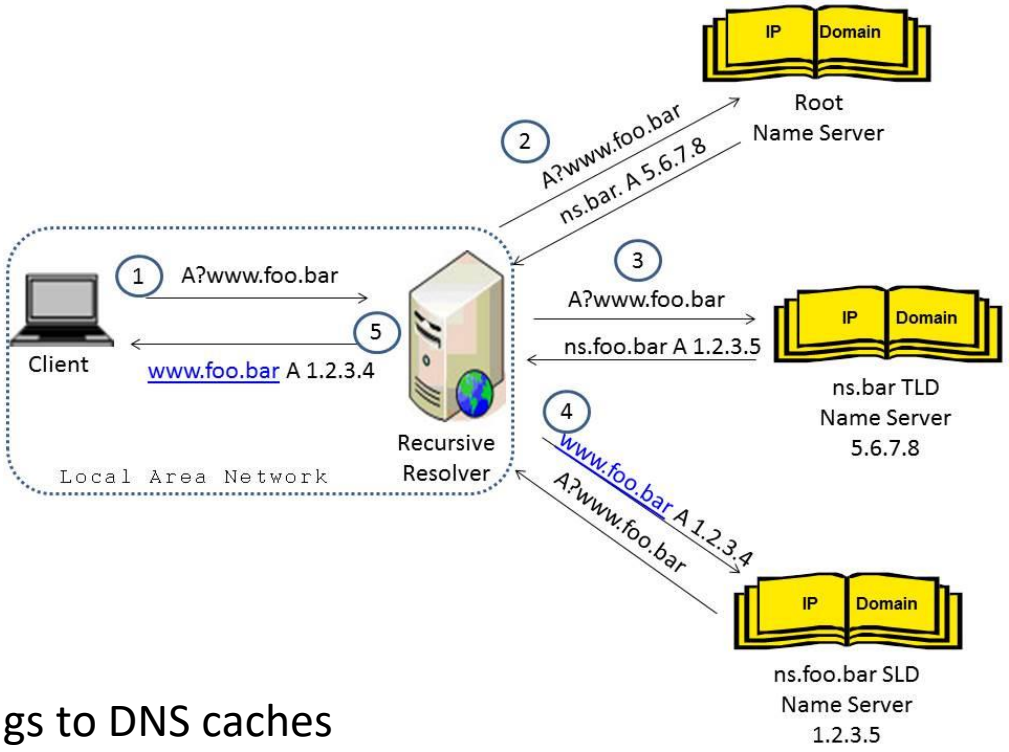
OVERVIEW

- DNS background
- DNS cache poisoning and exploits
- Ingredients in cache poisoning
- Caches study

No DNSSEC protocols were harmed in the making of this research ;-)

Domain Name System (DNS)
A critical service in the Internet

- **Lookup services**
  - Locate resources via names
  - Security mechanisms:
    black lists, policies,
    etc.
    (DANE, SPF, ROVER, …)



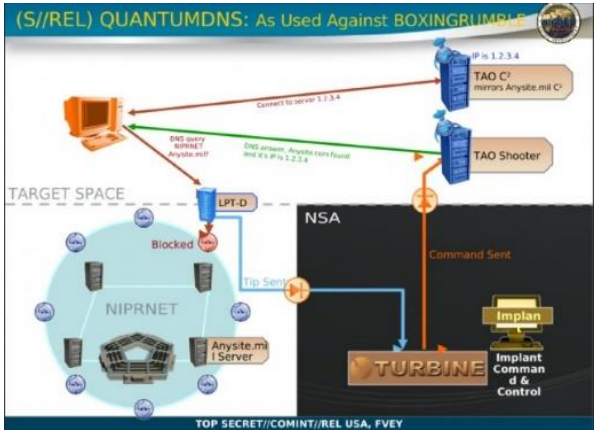
- Critical threat: **DNS cache poisoning**
  - Attacker injects incorrect mappings to DNS caches

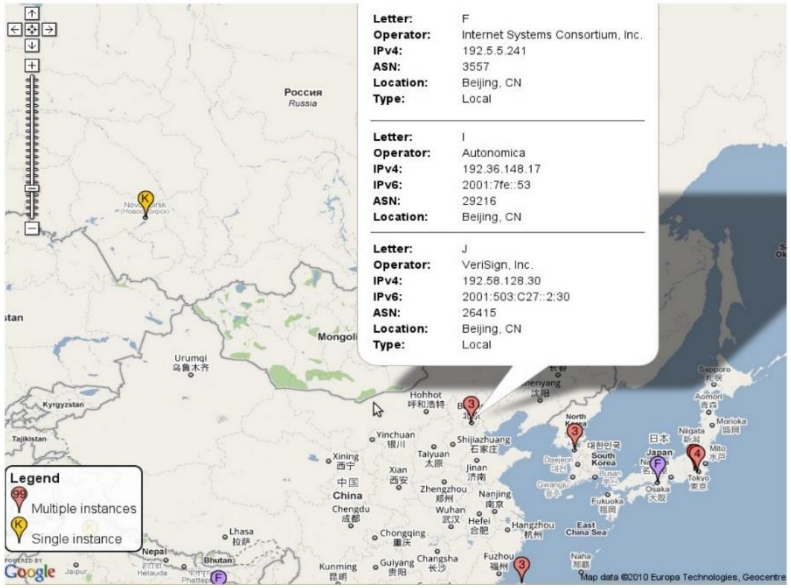
Fraunhofer SIT

DNS cache poisoning is a critical threat

And it is real!

- DNS cache poisoning attacks are a fact
  - E.g., run by NSA, GCHQ, China…
- Shulman et al. detected live hijacking (CCS14)





- `www.root-servers.org/map/`

Example: China DNS censorship

- Ask A record for facebook (or youtube,…) get IP in return

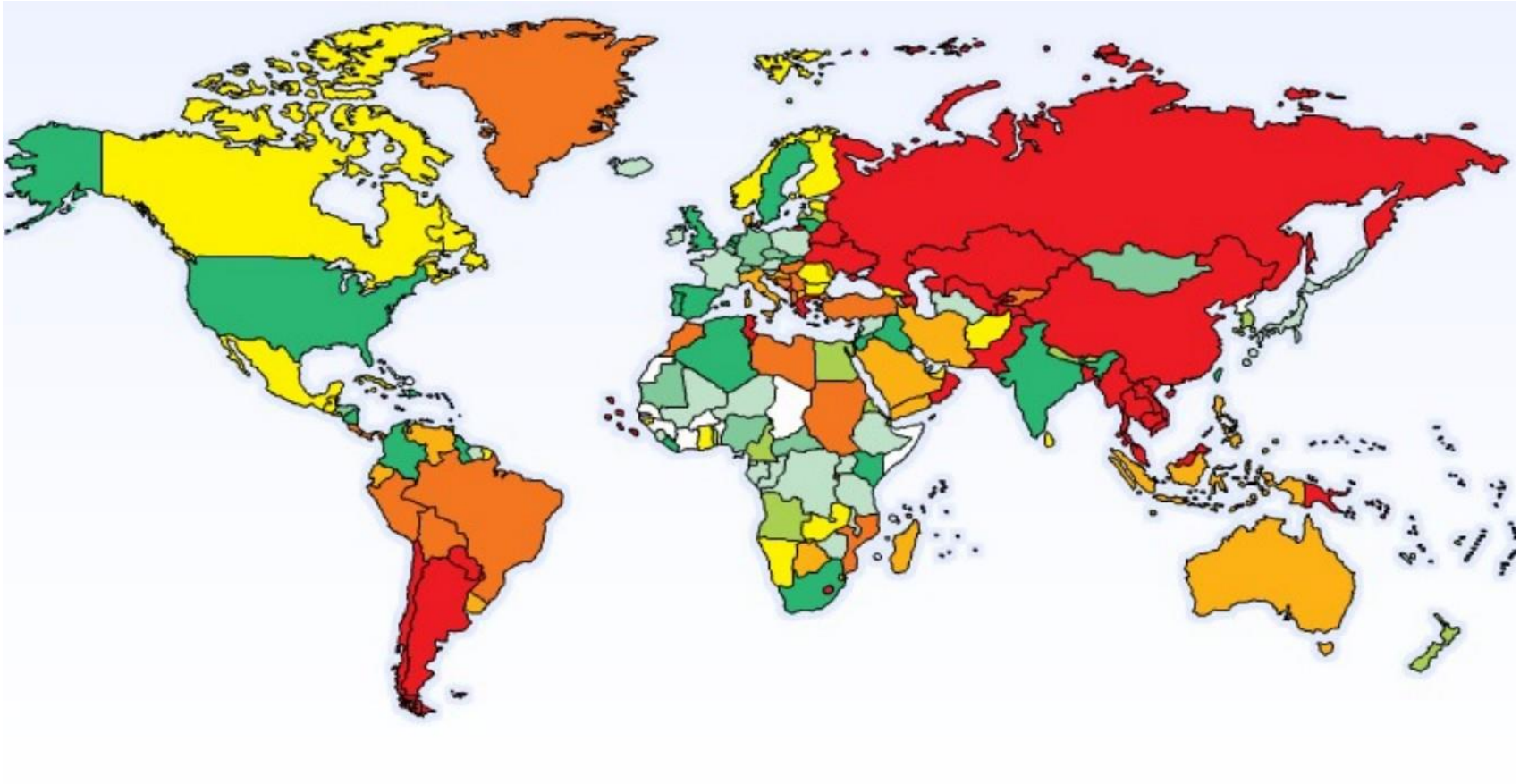
→ Query:
$dig @i.root-servers.net `www.facebook.com`

→ ANSWER:
`www.facebook.com in A 8.7.198.45`

Fraunhofer SIT

Affected networks worldwide

Due to DNS cache poisoning via China censorship



Multiple exploits of DNS cache poisoning

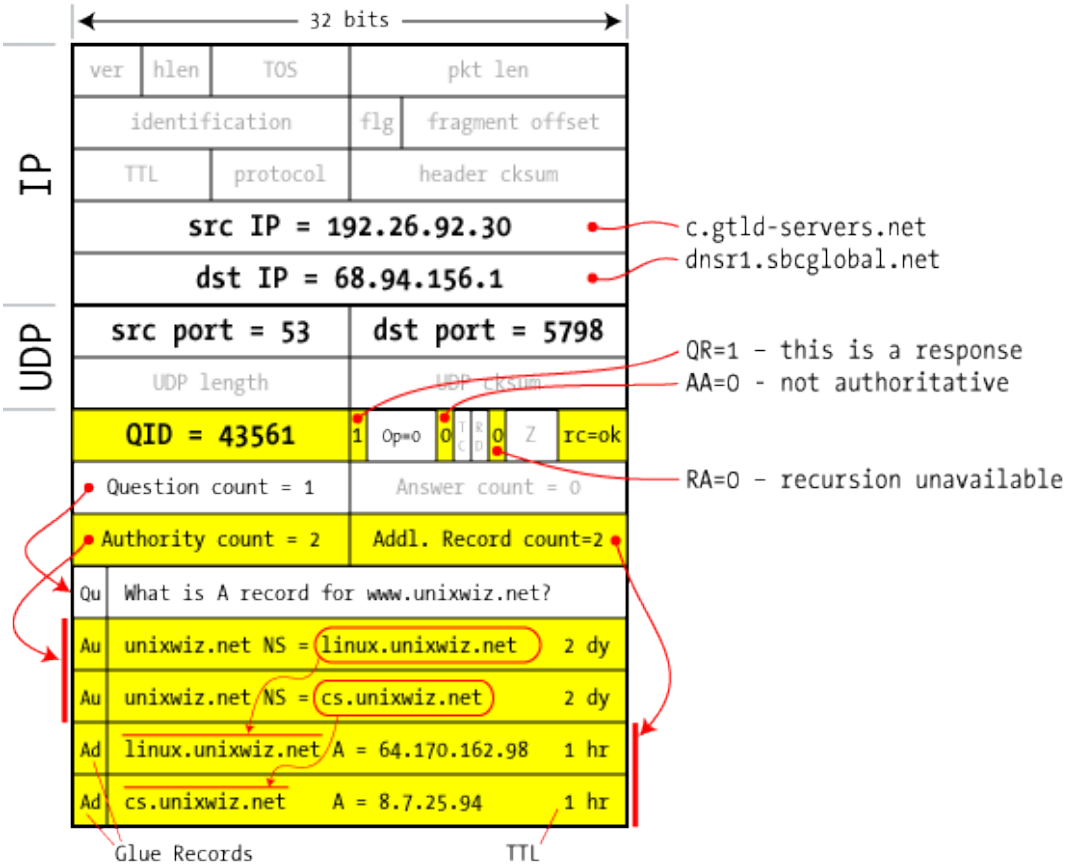
Allows to hijack emails, distribute malware, tap on traffic

- Example: password recovery procedure
- Relies on secure email

→ poison MX records for victim domain to hijack passwords

Fraunhofer SIT

A typical DNS response (structure)



(origin: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html)

Ingredients of DNS cache poisoning

Port+TXID+Caching

- Studies for port and TXID prediction
  - Old DNS resolver SW had weak TXID (Klein, 2007-2008)
  - Various scenarios for predictable port (NAT)
  - Works on forcefully reducing the port space (exhaustion)
  - (Partial) MitM attacks e.g. QuantumDNS

- No evaluation of vulnerable caching

→ our goal!

- How effective is cache poisoning in the wild?

Naïve DNS Payload

- Send (A) query to xyz123.domain.com
- Assume the spoofed payload (DNS response) has correct TXID and port number
- Payload response:
  - Answer part: A xyz123.domain.com 5.6.7.8 (whatever, don't care)
  - Authoritative part: domain.com NS evil.domain.com
  - Additional part: evil.domain.com A 66.66.66.66 (attacker's IP)
- This is actually our "Variant #1"

Naïve DNS payload (2)

- Still works on some DNS resolvers (small minority)
  - But not on e.g. newer BINDs, Google Public DNS service
  - Some servers are immune if they've seen auth answer previously
- Poisoning DNS is harder (2016) than it used to be (2008)
  - DNS resolvers are less naïve, more strict
  - Security measures are introduced

Son&Shmatikov, Wijngaards and us

- Wijngaards 2009
  - Long list of attack variants
  - No info about the attacks
  - No info about effectiveness vs. known SW resolvers, in the wild
- Son and Shmatikov, 2010
  - Narrow attack model (missing some attacks)
  - Results for BIND, Unbound and MaraDNS (only), no in the wild survey
- Klein, Shulman and Waidner, 2016
  - Additional attacks (total 18)
  - Results for “all” known resolver SW, incl. services (Google, OpenDNS)
  - In-the-wild survey: open resolvers, enterprises (SMTP), ISPs

Advanced cache-testing as a service

No installation and easy to use

1. Send email to **`random@enterprise.com`**
2. Target SMTP needs to bounce to sender (our email address)
3. Queries our authoritative DNS server for IP of our “mail server“ (test server)
4. The query to DNS server of **`test server`** initiates a set of 18 tests
   → each test is a validation of different attack type

5. Output sent to email or presented on webpage

Remote DNS cache poisoning evaluation of popular DNS

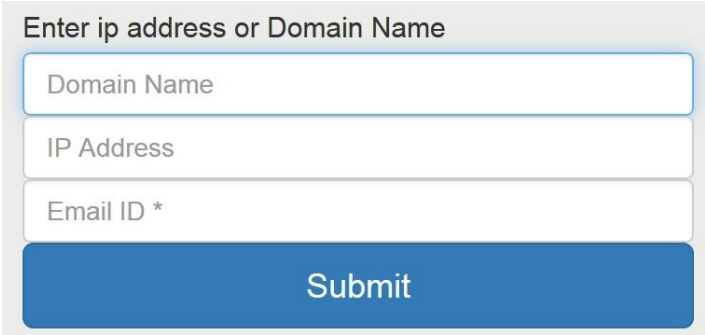
Software and appliances

yes	yes	no	no	no	no	no	yes	yes	no	no	yes	1
No	yes	yes	no	no	yes	yes	Yes	yes	no	yes	No	2
No	Yes	yes	no	no	yes	no	No	no	no	No	No	3
Yes	yes	yes	no	no	Yes	yes	Yes	yes	no	Yes	No	4
Yes	yes	yes	no	no	Yes	No	No	no	no	No	No	5
Yes	yes	yes	no	no	yes	yes	yes	yes	no	Yes	No	6
yes	yes	yes	no	no	yes	No	no	no	no	No	No	7
No	no	no	no	no	yes	Yes	yes	yes	no	Yes	No	8
No	no	yes	no	No	yes	No	no	no	no	No	No	9
No	no	yes	no	No	yes	yes	yes	yes	no	Yes	No	10
no	no	yes	no	No	yes	yes	yes	yes	no	No	No	11
yes	yes	Yes	no	No	yes	yes	yes	yes	no	yes	Yes	12
no	No	No	no	No	yes	yes	yes	yes	no	yes	no	13
yes	yes	No	no	No	yes	yes	yes	yes	no	yes	no	14
yes	yes	No	No	no	No	No	yes	yes	no	no	yes	19
yes	yes	No	No	no	yes	yes	yes	yes	yes	yes	no	20
yes	yes	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	21
yes	yes	yes	No	yes	yes	yes	yes	Yes	yes	yes	yes	22

Advanced cache-testing as a service

Majority of networks vulnerable

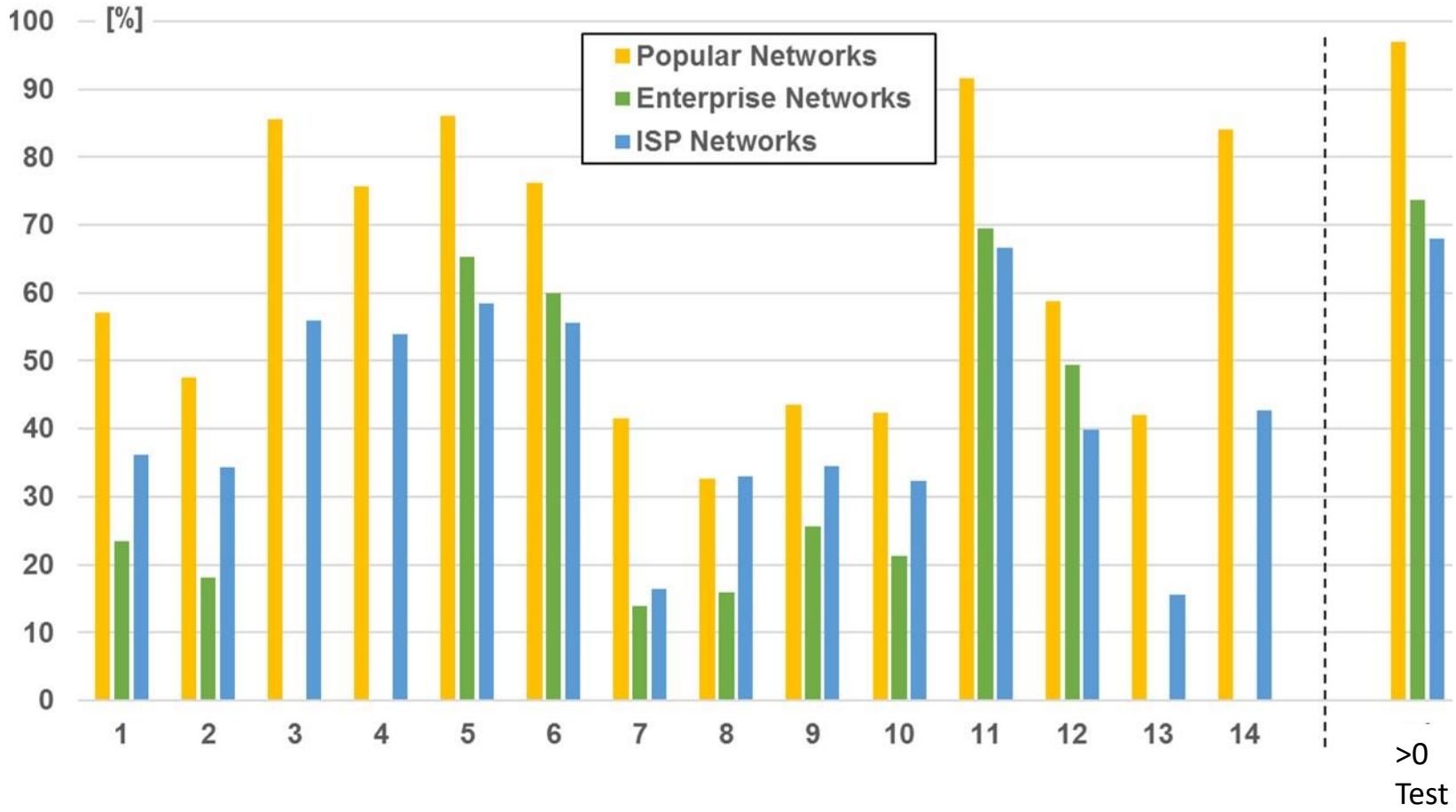
- Provide remote evaluation as a webservice
- Our evaluation of caches vulnerabilities in networks shows:
  - **97% of SMTPs vulnerable(!)**
  - Distribution of DNS SW in the wild (SMTP):
    - `BIND distributions – 47%`
    - `Unbound – 7%`
    - `Google public DNS – 35%`
    - `MS DNS – 11%`
  - Distribution of source ports
    - `1% static source ports`
    - `3% predictable source ports`



Ports	OS
[1024-5000]	Windows distributions incl XP Linux up until 2.2 FreeBSD up until 4.11
[49152-65535]	Vista FreeBSD until 8.0
[32768-61000]	Linux
[10000-65535]	FreeBSD

DNS Security

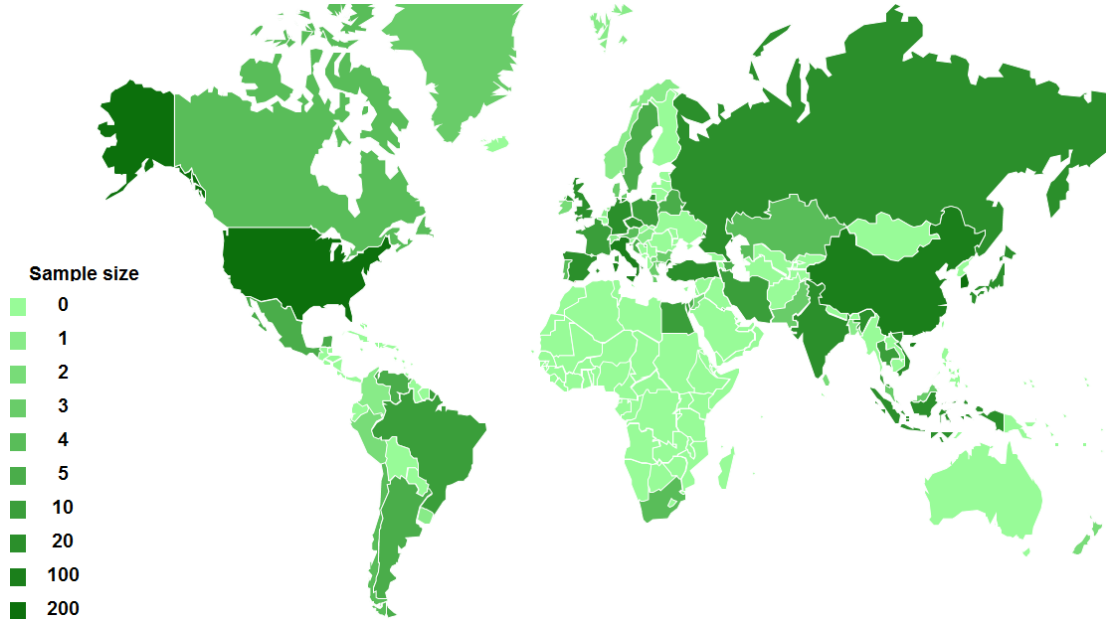
Cache poisoning vulnerabilities



Fraunhofer SIT

DNS Security

Tested networks



Open Resolvers		Email Servers		Ad-Network	
Network Operators	**%**	**Network Operators**	**%**	**Network Operators**	**%**
Aruba S.p.A.	9.597	Google Inc.	24.211	Comcast Cable Communications, Inc.	15.02
Google Inc.	6.59	Yandex LLC	10.526	Time Warner Cable Internet LLC	6.103
Korea Telecom	4.095	Amazon.com, Inc.	4.2105	Orange S.A.	5.634
INTERNET CZ, a.s.	3.199	Hangzhou Alibaba Advertising Co.,Ltd.	4.2105	Google Inc.	4.695
tw telecom holdings, inc.	3.135	Internet Initiative Japan Inc.	4.2105	BT Public Internet Service	4.225
LG DACOM Corporation	2.687	Websense Hosted Security Network	4.2105	MCI Communications Services, Inc. Verizon	3.286
Data Communication Business Group	2.175	SAKURA Internet Inc.	3.1579	AT&T Services, Inc.	2.817
Getty Images	1.727	ADVANCEDHOSTERS LIMITED	2.1053	OVH SAS	2.817
CNCGROUP IP network China169 Beijing	1.536	Dadeh Gostar Asr Novin P.J.S. Co.	2.1053	Free SAS	2.347
Level 3 Communications, Inc.	1.536	Limited liability company Mail.Ru	2.1053	Qwest Communications Company, LLC	2.347
OTHER	63.72	OTHER	38.947	OTHER	50.7

Fraunhofer SIT

Directions and by-products

- Cache counting techniques (spin-off paper)
- Resolver software fingerprinting (spin-off paper)
- Attack life-span analysis and extension (possible spin-off paper)
- Real-life attack considerations:
  - Cache counting
  - Packet loss
  - Imbalanced load balancing

Q&A

Thank you!