Who Is Answering My Queries?
Understanding and Characterizing Hidden Interception of the DNS Resolution Path

Baojun Liu, Chaoyi Lu, Haixin Duan,
Ying Liu, Zhou Li, Shuang Hao and Min Yang

Media Reports

ACM TechNews

https://technews.acm.org/archives.cfm?fo=2018-08-aug/aug-24-2018.html

How Often Are Users' DNS Queries Intercepted?
Help Net Security
Zeljka Zorz
August 21, 2018

Chinese researchers have developed approaches to det
of Domain Name System (DNS) interception, analyzing
and cellular Internet Protocol (IP) addresses worldwide

The Register

Security

How's that encryption coming, buddy? DNS requests routinely spied on, boffins claim

Uninvited middlemen may be messing with message

https://www.theregister.co.uk/2018/08/20/dns_interception/

HackRead

https://www.hackread.com/hackers-can-intercept-and-manipulate-dns-queries-researchers-warn/

Where has my query gone?

- Querying Google Public DNS
  - *whoami.akamai.net* tells you your ***real*** resolver
  - From one client machine:

```
$ dig @8.8.8.8 whoami.akamai.net
;; ANSWER SECTION:
whoami.akamai.net.      47      IN      A       173.194.171.5
```

173.194.171.5: AS15169 Google LLC

All good.

Where has my query gone?

- Querying Google Public DNS
  - *whoami.akamai.net* tells you your ***real*** resolver
  - From another client machine:

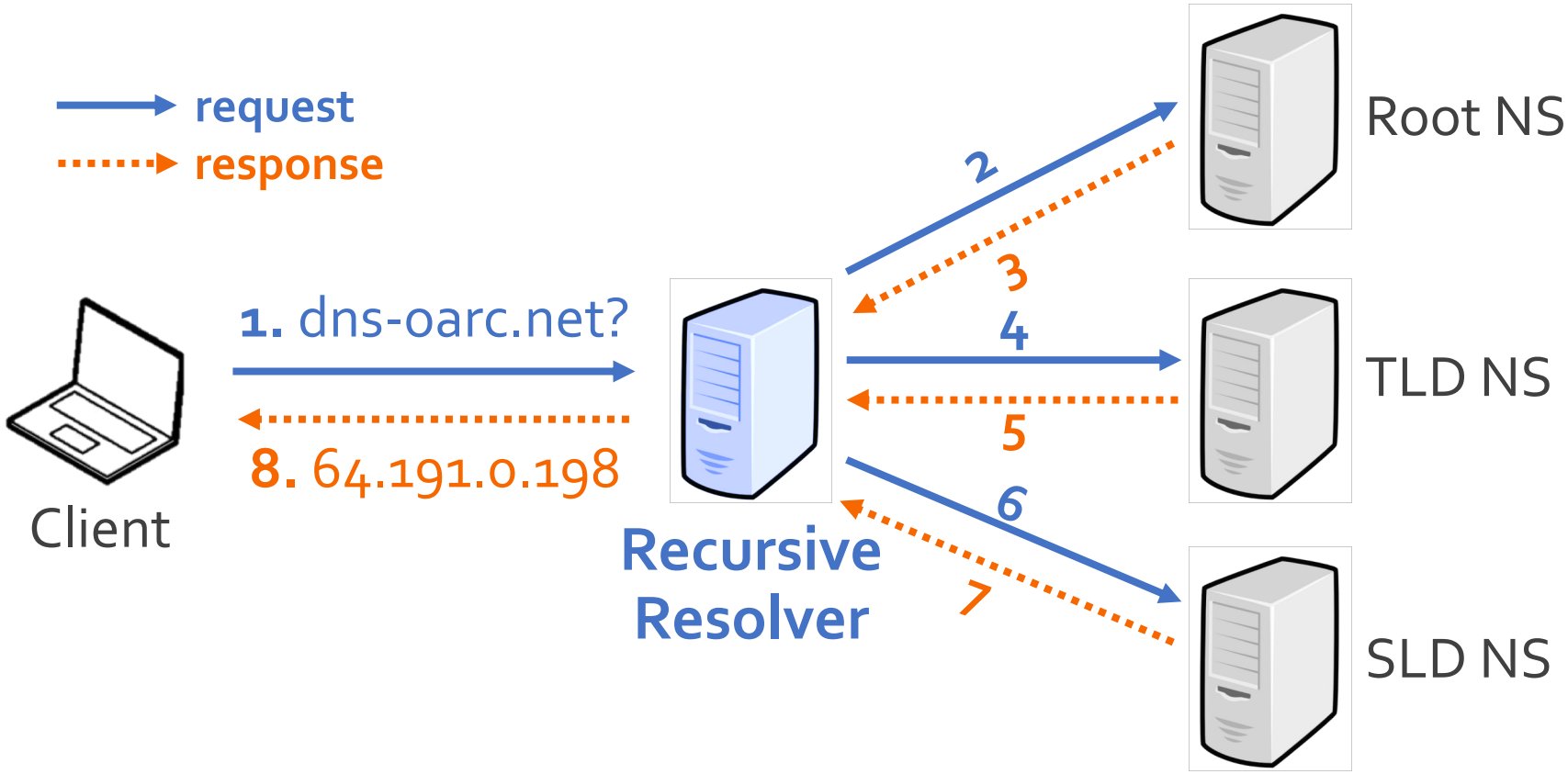
```
➜  ~ dig @8.8.8.8 whoami.akamai.net
;; ANSWER SECTION:
whoami.akamai.net.      180     IN      A       216.169.129.2
```

216.169.129.2: AS22781 Strong Technology, LLC

What happened?

DNS Resolution

- DNS: the beginning of Internet activities
  - By a **recursive resolver**

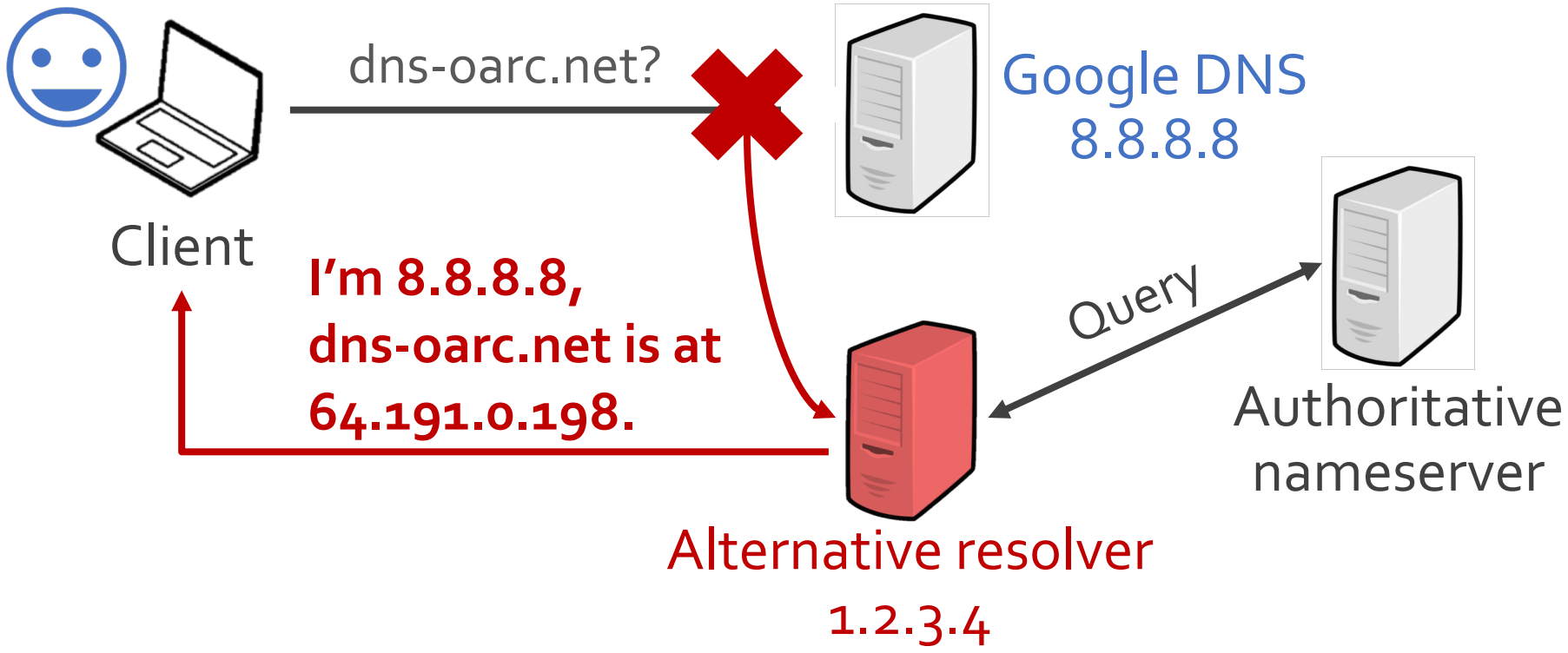


DNS Resolution

- Why public DNS?
  - Performance (e.g., load balancing)
  - Security (e.g., DNSSEC support)
  - DNS extensions (e.g., EDNS Client Subnet)

DNS Interception

- Who is answering my queries?



Spoof the IP address and **intercept** queries.

Potential Interceptors

Network Providers

Is Your ISP Hijacking Your DNS Traffic?

Babak Farrokhi — 06 Jul 2016

You might not have noticed, but there are chances that your ISP is playing nasty tricks with your DNS traffic.

How to Find Out if Your ISP is Doing Transparent DNS Proxy

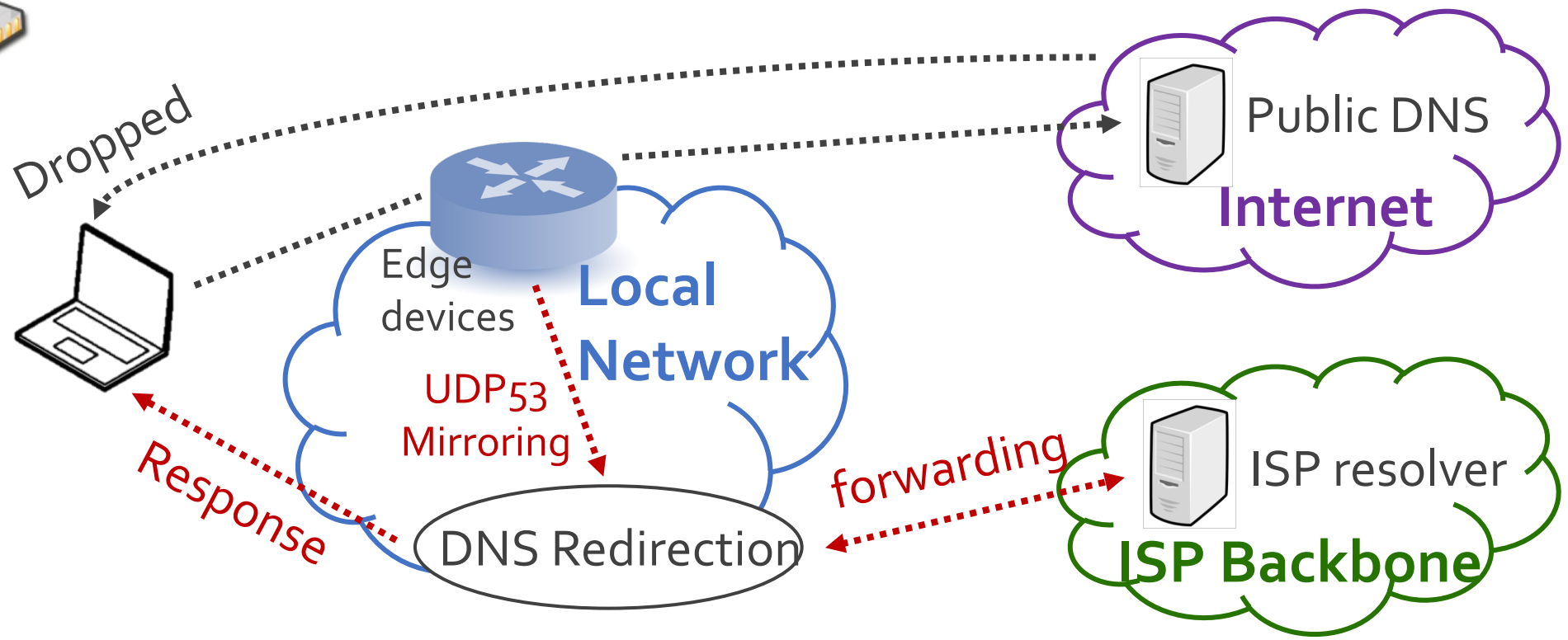
In this tutorial we will show you have to find out if your ISP (Internet Service Provider) is doing Transparent DNS Proxy.

* https://labs.ripe.net/Members/babak_farrokhi/is-your-isp-hijacking-your-dns-traffic
* https://www.cactusvpn.com/tutorials/find-out-isp-doing-transparent-dns-proxy/

Potential Interceptors

Network Providers

"Controlling external DNS with preemptive response injection"



* http://www.ttm.com.cn/article/2016/1000-1247/1000-1247-1-1-00064.shtml

Potential Interceptors

Malware / anti-virus software

Avast Real Site

Avast **Real Site** routes your connection using an IP address that is known and secure eve ght decrease in

Routes your connection

To ensure your full security, **Real Site** is enabled by default. We recommended you keep Re you need to temporarily disable it for troubleshooting purposes. To disable Real Site, go

Enabled by default

* https://support.avast.com/en-us/article/Antivirus-Real-Site-FAQ

Potential Interceptors

Network Providers

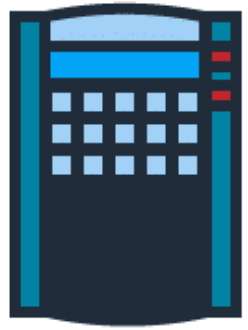
Censorship / firewall

Anti-virus software / malware

(E.g., Avast anti-virus)

Enterprise proxy

(E.g., Cisco Umbrella intelligent proxy)



Q1:

*How **prevalent** is DNS interception?*

Q2:

*What are the **characteristics** of DNS interception?*

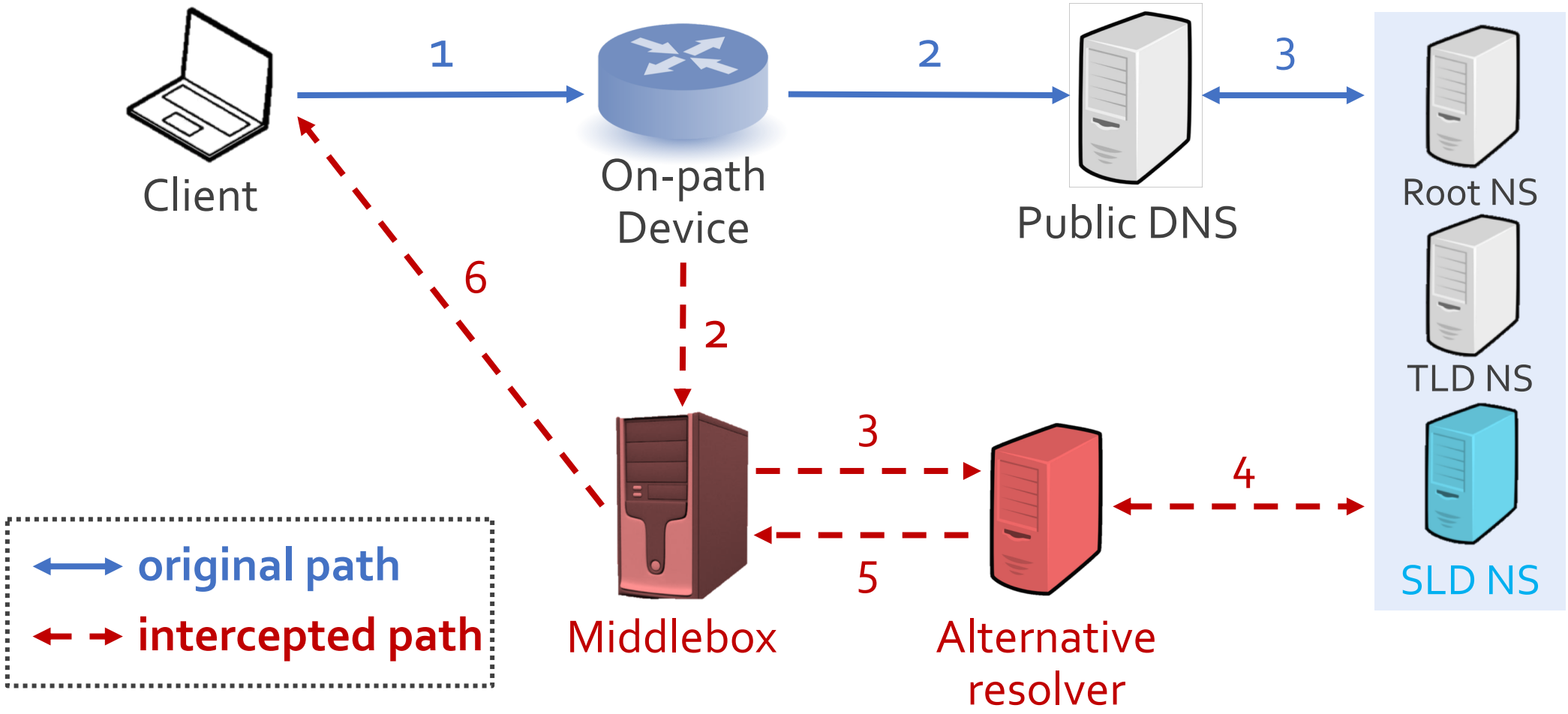
Motivation

Threat Model

Methodology

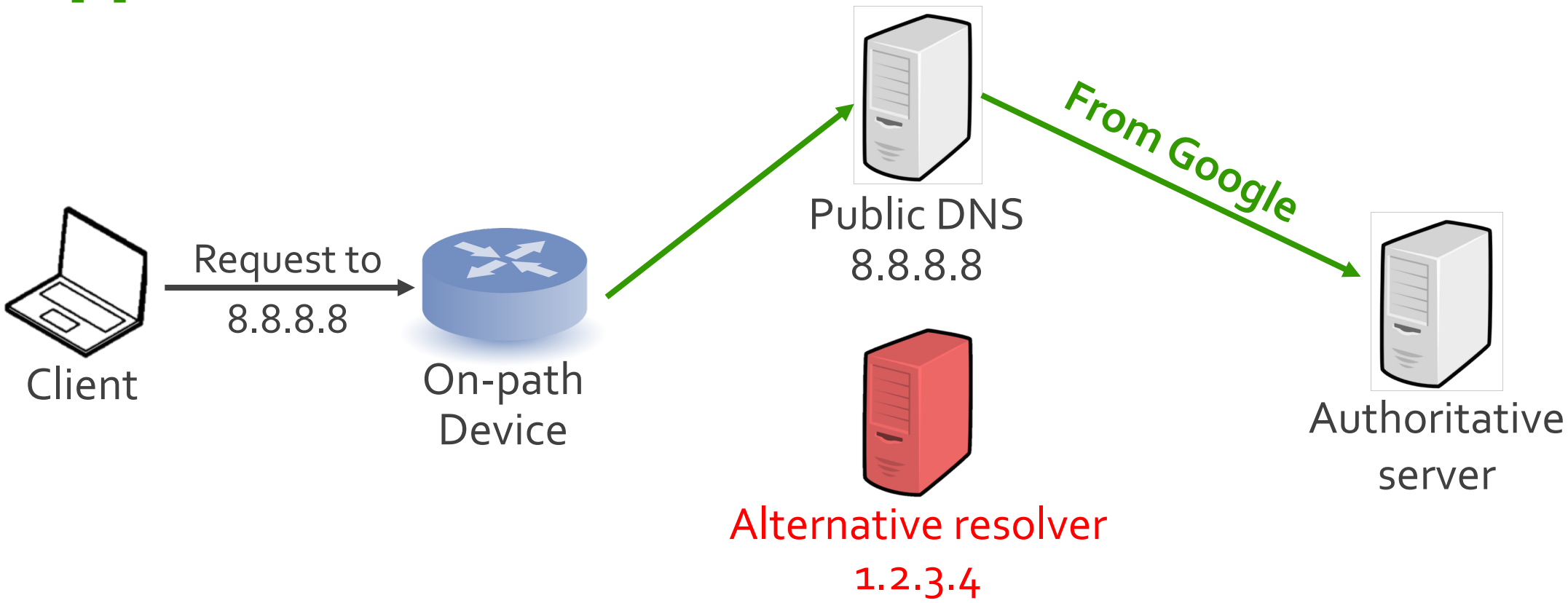
Analysis

Threat Model



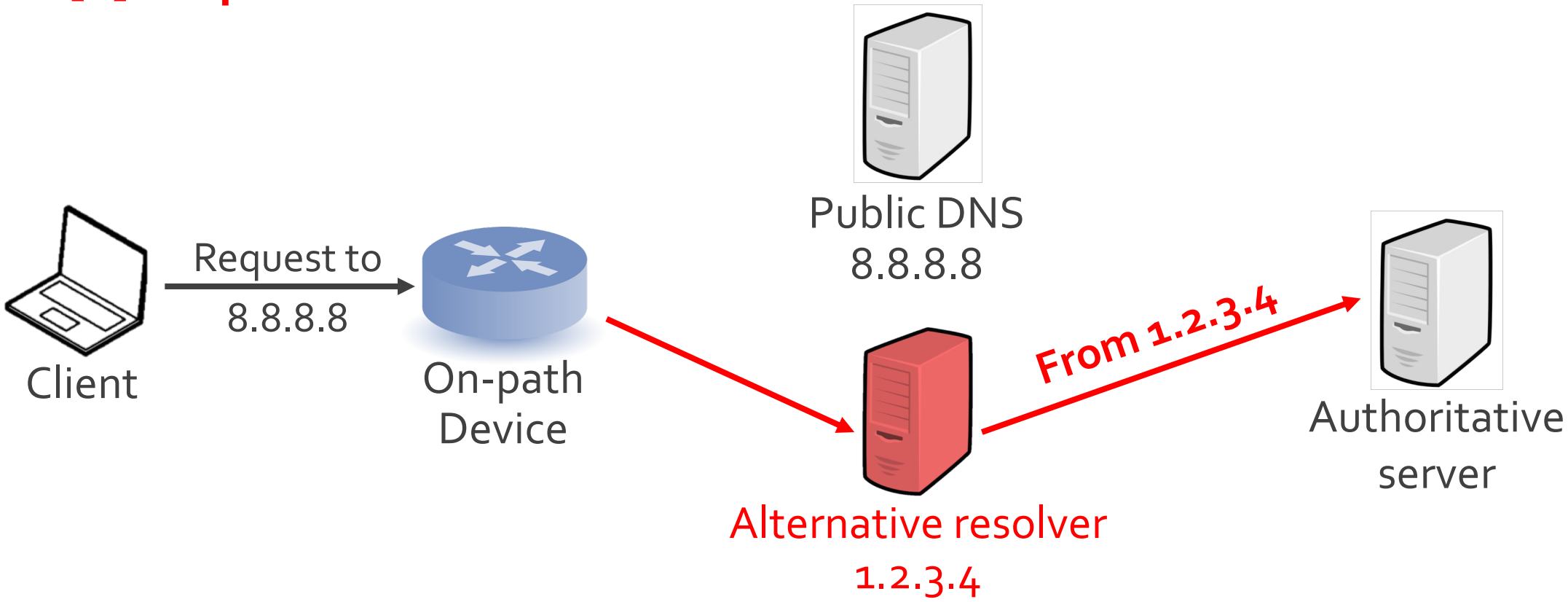
Threat Model

- Taxonomy (request)
  - **[1] Normal resolution**



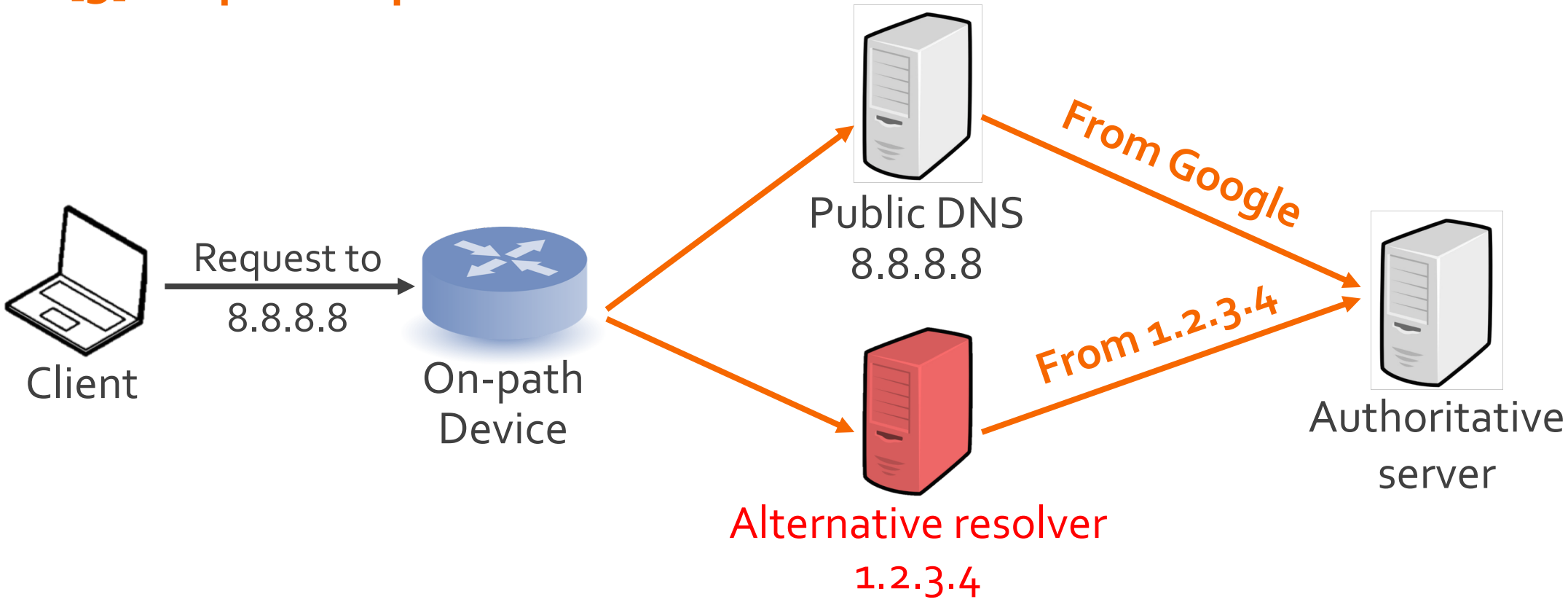
Threat Model

- Taxonomy (request)
  - **[2] Request redirection**



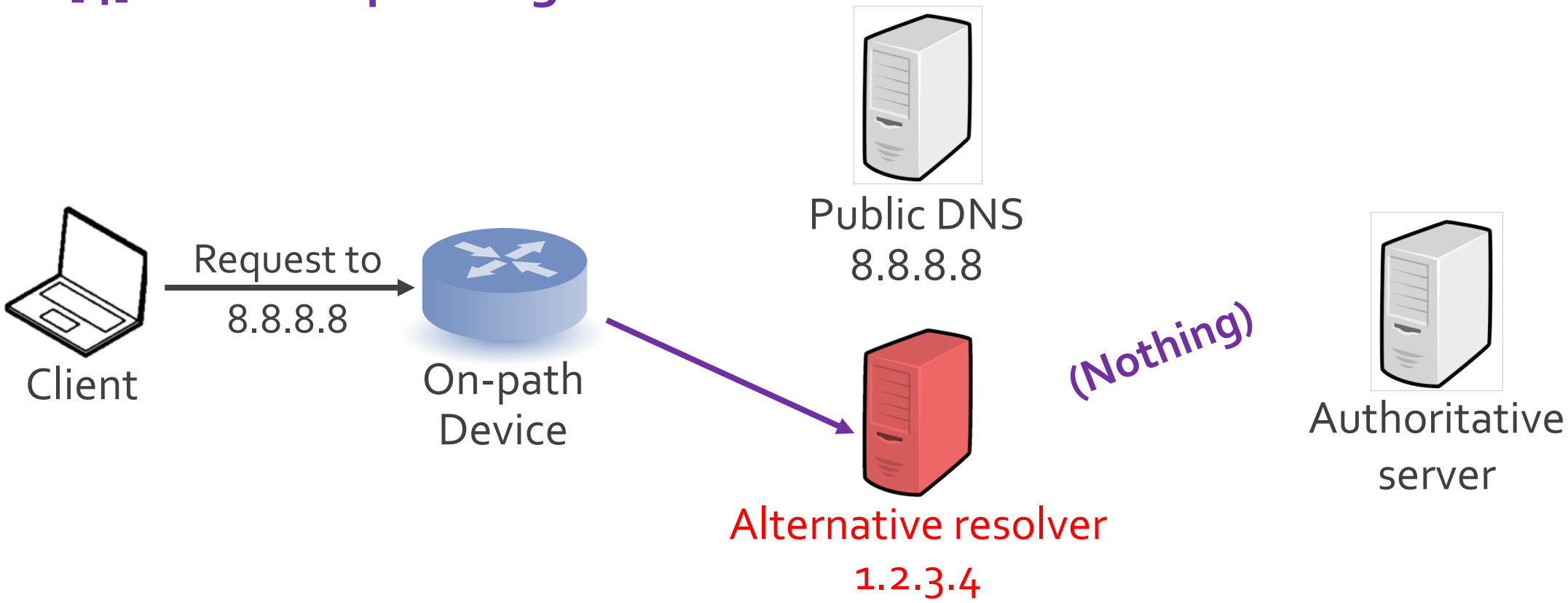
Threat Model

- Taxonomy (request)
  - **[3] Request replication**



Threat Model

- Taxonomy (request)
  - **[4] Direct responding**



Motivation

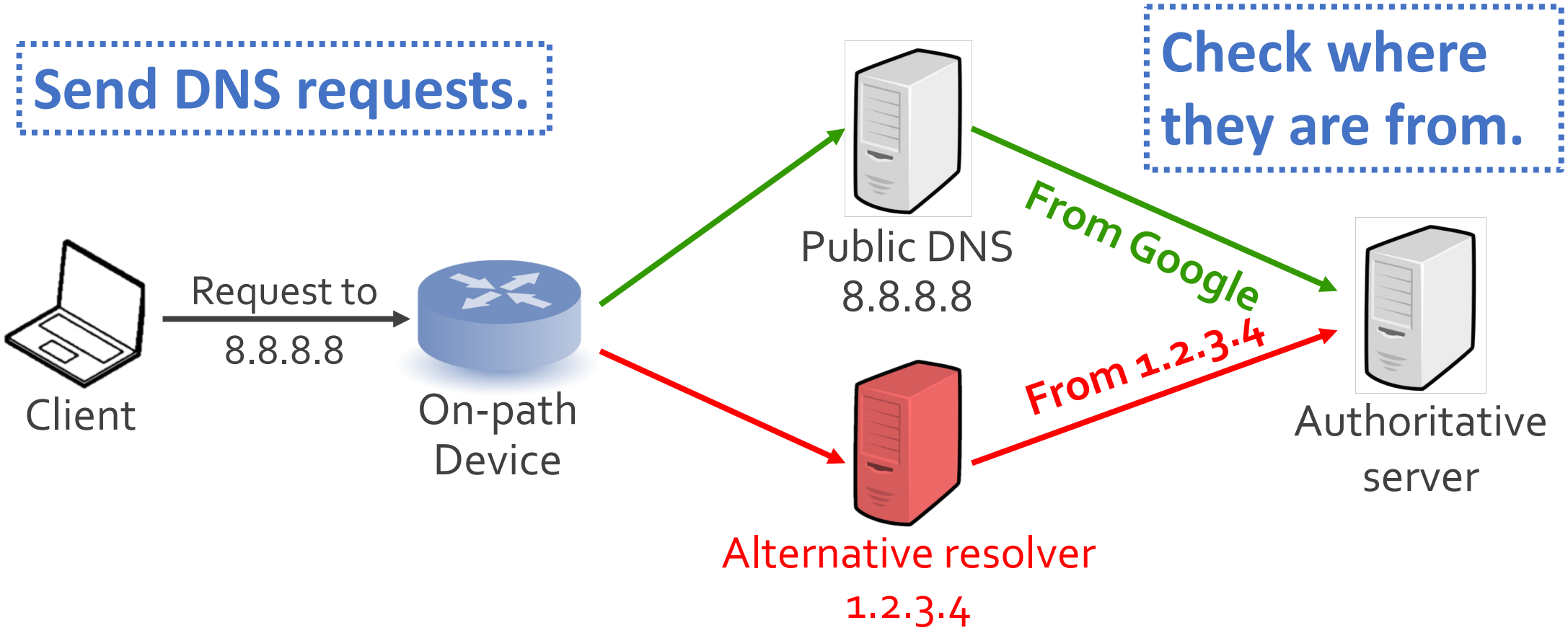
Threat Model

Methodology

Analysis

How to Detect?

- At a glance



Vantage Points

- Phase I: Global Analysis
  - ProxyRack: SOCKS5 residential proxy networks
  - Limitation: **TCP** traffic only
- Phase II: China-wide Analysis
  - A network debugger module of security software
  - Similar to ***Netalyzr*** [Kreibich, IMC' 10]
  - Capability: **TCP and UDP; Socket level**

DNS Requests

- Requirements
  - **Diverse**: triggering interception behaviors
  - **Controlled**: allowing fine-grained analysis

Public DNS	*Google, OpenDNS, Dynamic DNS, EDU DNS*
Protocol	*TCP, UDP*
QTYPE	*A, AAAA, CNAME, MX, NS*
QNAME (TLD)	*com, net, org, club*
QNAME	UUID.[Google].OurDomain. [TLD]

Collected Dataset

- DNS requests from vantage points
  - **A wide range of requests** collected

Phase	# Request	# IP	# Country	# AS
ProxyRack	1.6 M	36K	173	2,691
Debugging tool	4.6 M	112K	87	356

Motivation

Threat Model

Methodology

Analysis

How many queries are intercepted?

Magnitude

- Investigated ASes

198 ASes
have intercepted traffic
(of 2,691, 7.36%, TCP)

61 ASes
have intercepted traffic
(of 356, 17.13%)

Magnitude

- Interception ratio
  - China-wide analysis, UDP & TCP

Google Public DNS **27.9%** 7.3%

OpenDNS **12.6%** 0.9%

ORACLE + Dyn **16.1%** 2.3%

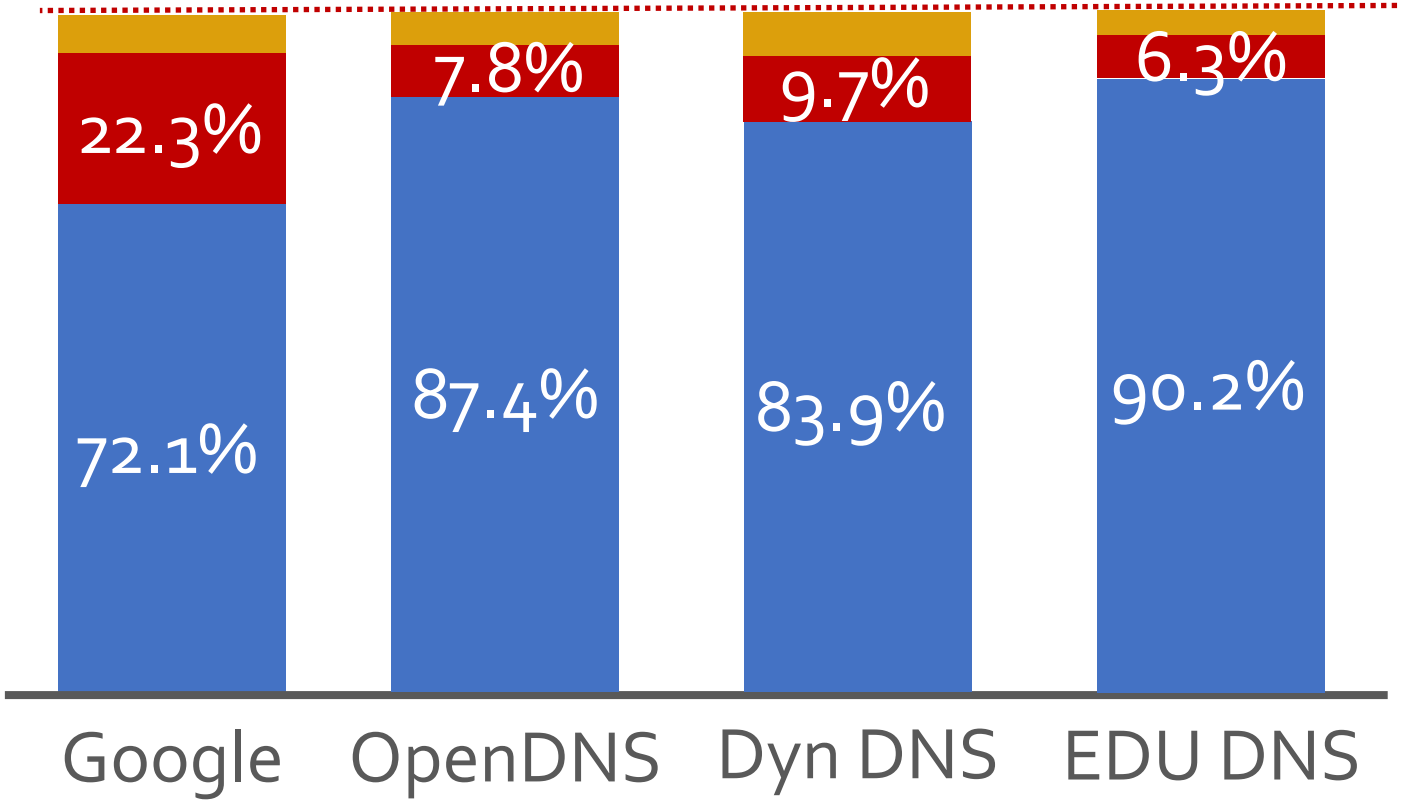
EDU DNS **9.8%** 1.1%

Popular services are preferred.

How are my queries intercepted?

Interception Characteristics

- Magnitude (% of total requests)
  - **Normal resolution** **Request redirection** **Request replication**



Direct responding is rare.

Request redirection > Request replication

Interception Characteristics

- AS-level analysis
  - Sorted by # of total requests

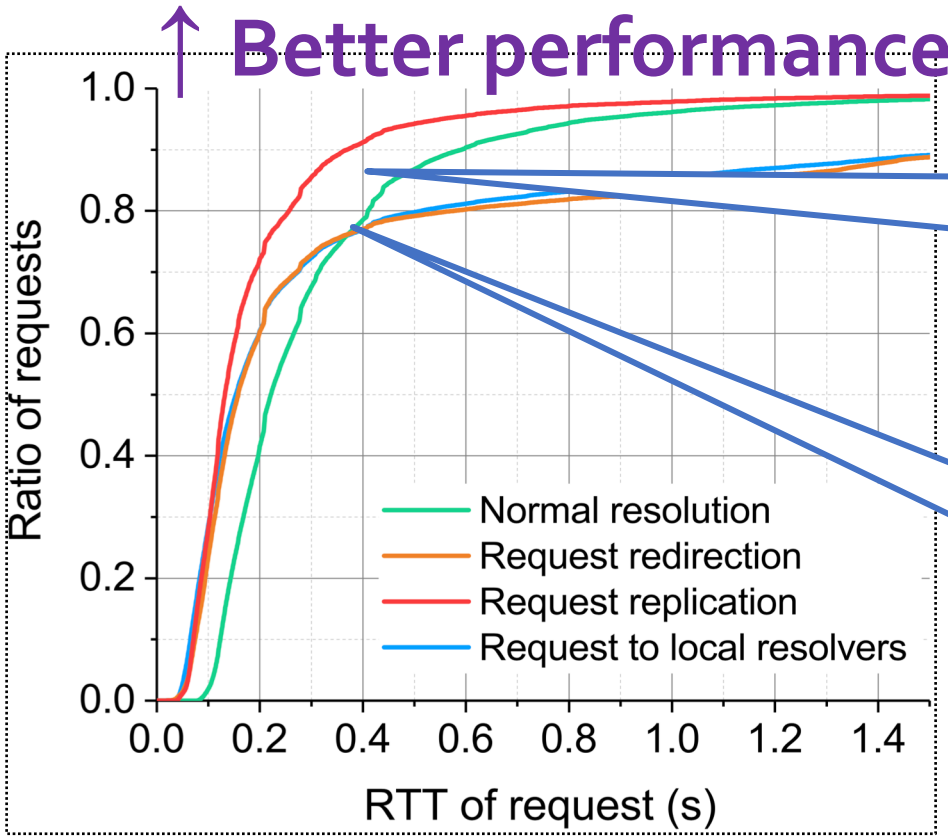
AS	Organization	Redirection	Replication	Alternative Resolver
AS4134	China Telecom	5.19%	0.2%	116.9.94.* (AS4134)
AS4837	China Unicom	4.59%	0.51%	202.99.96.* (AS4837)
AS9808	China Mobile	**32.49%**	**8.85%**	112.25.12.* (AS9808)
AS56040	China Mobile	**45.09%**	0.04%	120.196.165.* (AS56040)

Complex interception policies, and they vary among ASes.

Do my queries get faster?

DNS Lookup Performance

- RTT of requests
  - Which requests complete faster?



Request replication vs. Normal resolution:

Better.

Request redirection vs. Normal resolution:

Not always better.

Are my responses tampered?

Response Manipulation

- DNS record values
  - Most responses are ***not tampered***.
  - Some exceptions:

Classification	#	Response Example	Client AS
Gateway	54	192.168.32.1	AS4134, CN, China Telecom
Monetization	10	39.130.151.30	AS9808, CN, GD Mobile
Misconfiguration	26	::218.207.212.91	AS9808, CN, GD Mobile
Others	54	fe80::1	AS4837, CN, China Unicom

Response Manipulation

- Example: traffic monetization

China Mobile Group of Yunnan: **advertisements of an APP**.

So why should I care?
Any threats?

Security Threats

*"Not all the intercepted DNS queries were modified or recorded, **but they could be**, which has huge implications for **privacy and security** online"*

(From: Nick Sullivan's email to The Register)

* https://www.theregister.co.uk/2018/08/20/dns_interception/

Security Threats

- Ethics & privacy
  - Users may ***not be aware*** of the interception behavior
- Alternative resolvers' security
  - An analysis on **205 open alternative resolvers**

Only 43% resolvers support DNSSEC

BIND

Berkeley Internet Domain Name

ALL BIND versions should be deprecated before 2009

Why intercepting my queries?

Interception Motivations

- What interceptors have to say
  - Devices & software vendors

异网DNS收敛功能将异网DNS请求管控起来，将访问调度至网内资源，不仅提高访问体验，同时也节约了出口流量。

包装响应包使异网DNS请求的管控对用户完全透明。

Improve DNS performance

Reduce traffic settlement

- 优化用户体验，降低安全风险的同时，缩减网间流量结算成本。

Mitigate security threats

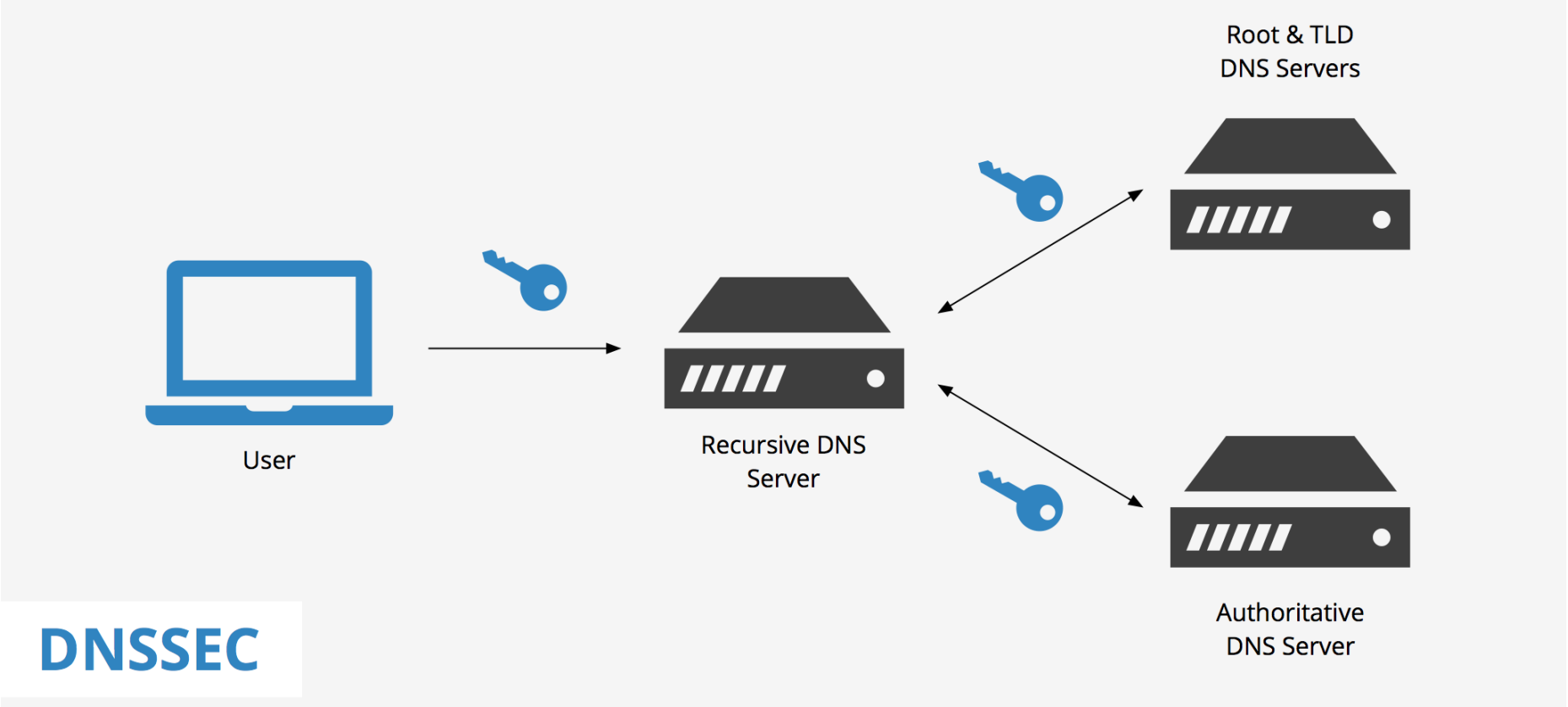
Interception Motivations

- What interceptors have to say
  - Devices & software vendors
- Motivations
  - Improving DNS security ?
  - Improving DNS lookup performance ?
  - Reducing traffic financial settlement

Geez…
How can I prevent this?

Solutions

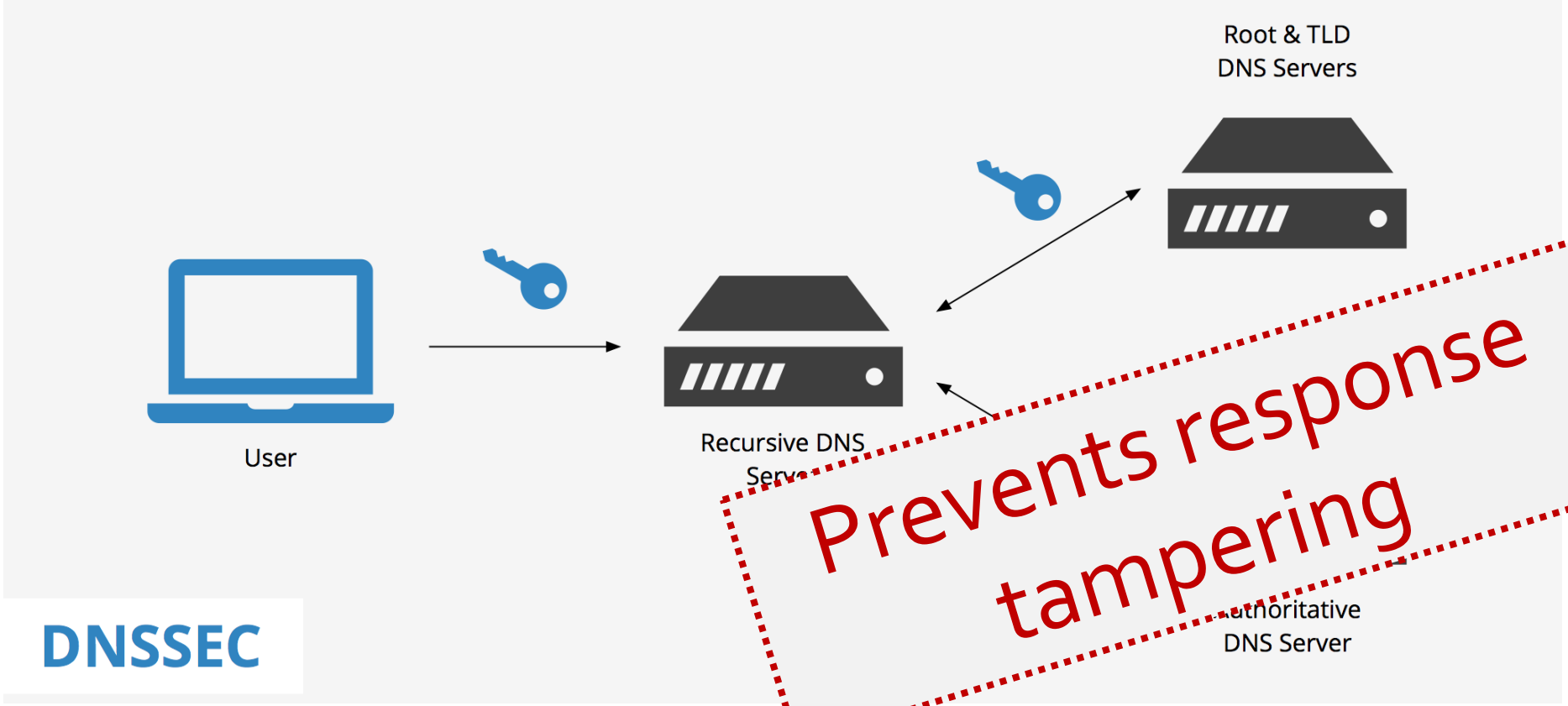
- DNSSEC



* Pic from: https://www.keycdn.com/support/dnssec/

Solutions

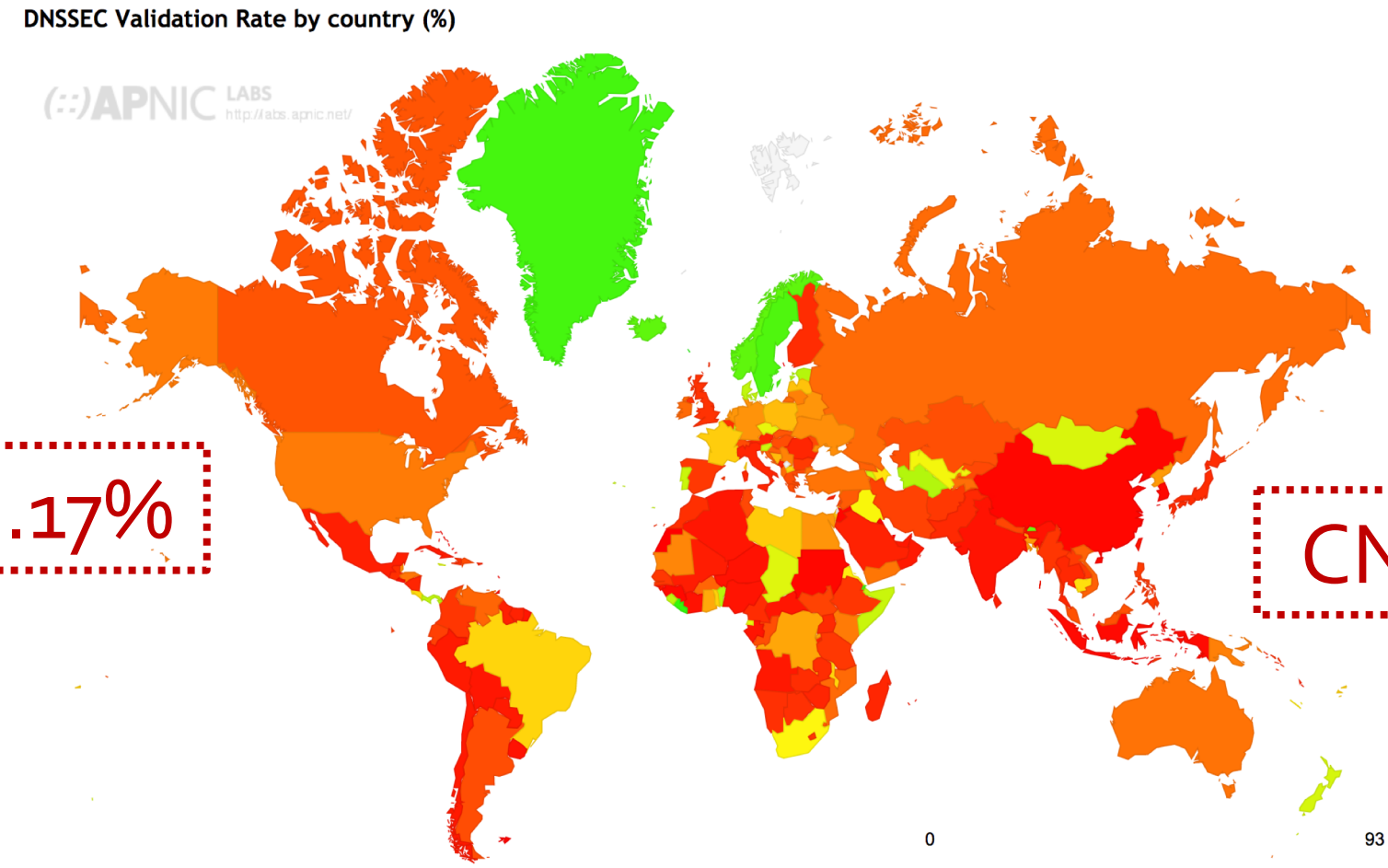
- DNSSEC



* Pic from: https://www.keycdn.com/support/dnssec/

Yippee! ...?

DNSSEC Validation Rate

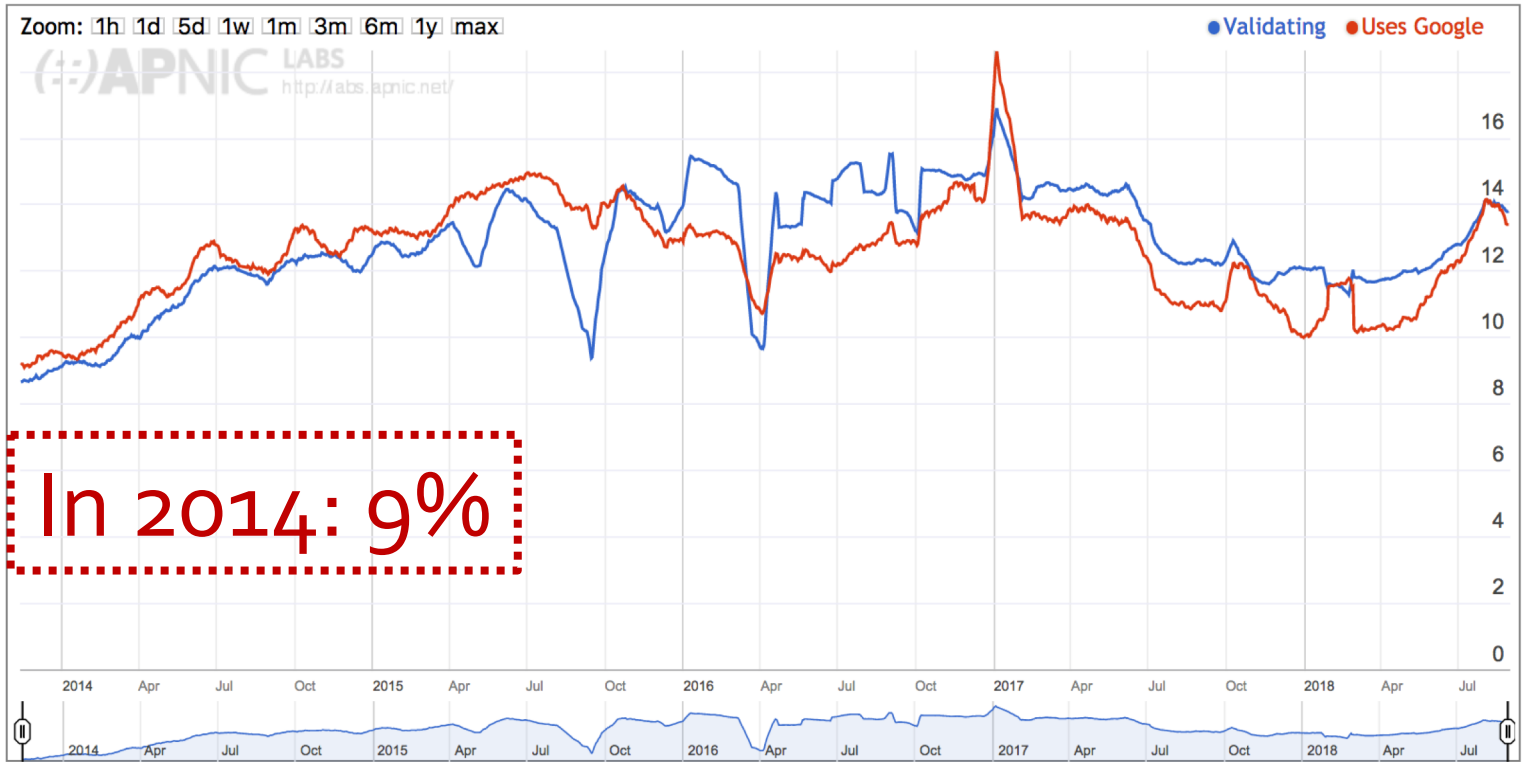


US: 23.17%

CN: 0.93%

Pic from: http://stats.labs.apnic.net/dnssec

DNSSEC Validation Rate



In 2014: 9%

Till Aug 2018: 14%

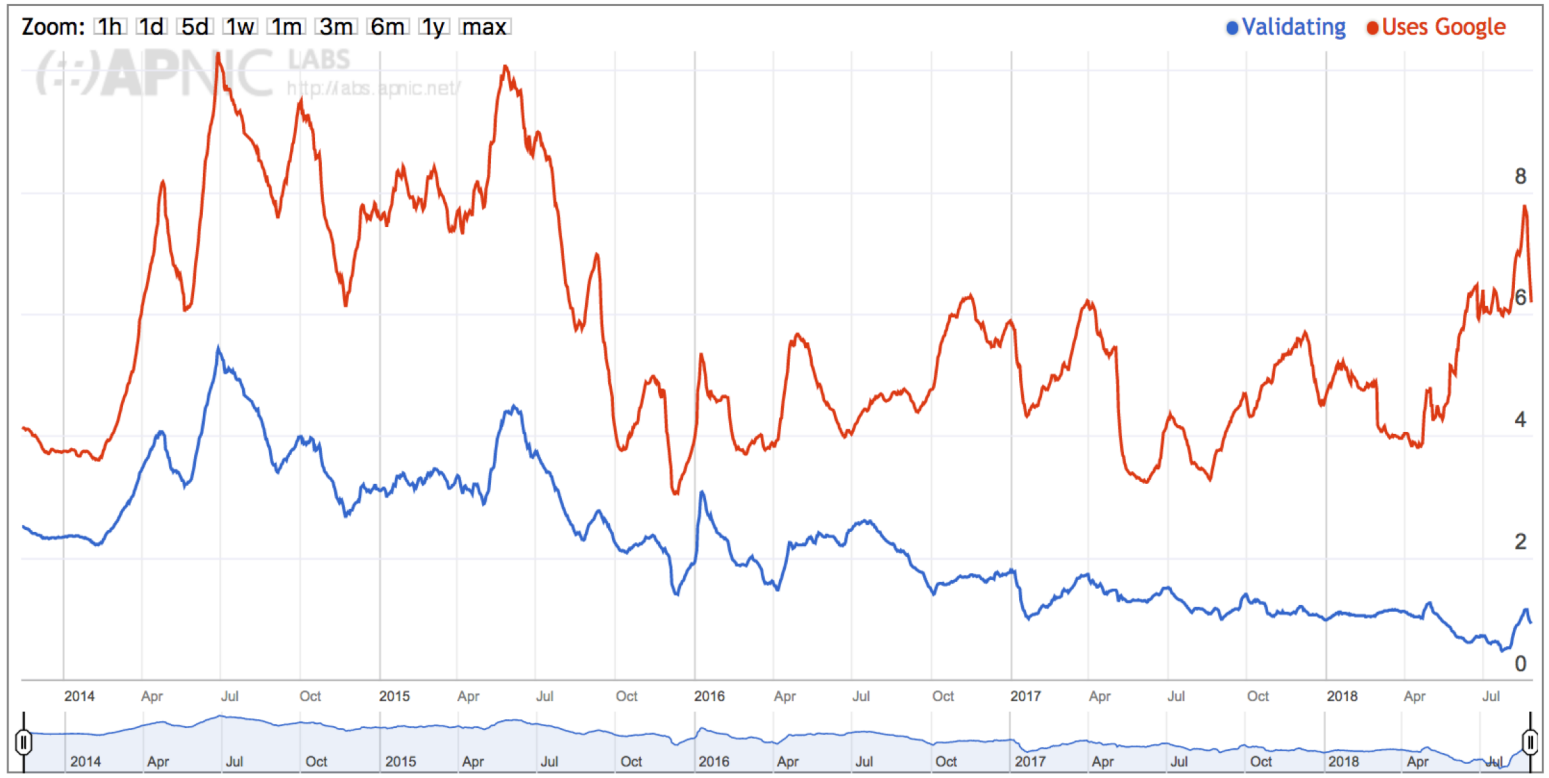
Validating

Uses Google

Pic from: https://stats.labs.apnic.net/dnssec/XA

DNSSEC Validation Rate in China

Use of DNSSEC Validation for China (CN)



Validating < Uses Google ???

Validating

Uses Google

Geoff Huston, DNS, DNSSEC and Google's Public DNS Service, https://labs.apnic.net/?p=368

DNSSEC Validation Rate in China

Use of DNSSEC Validation for China (CN)

Validating < Uses Google ???

Validating

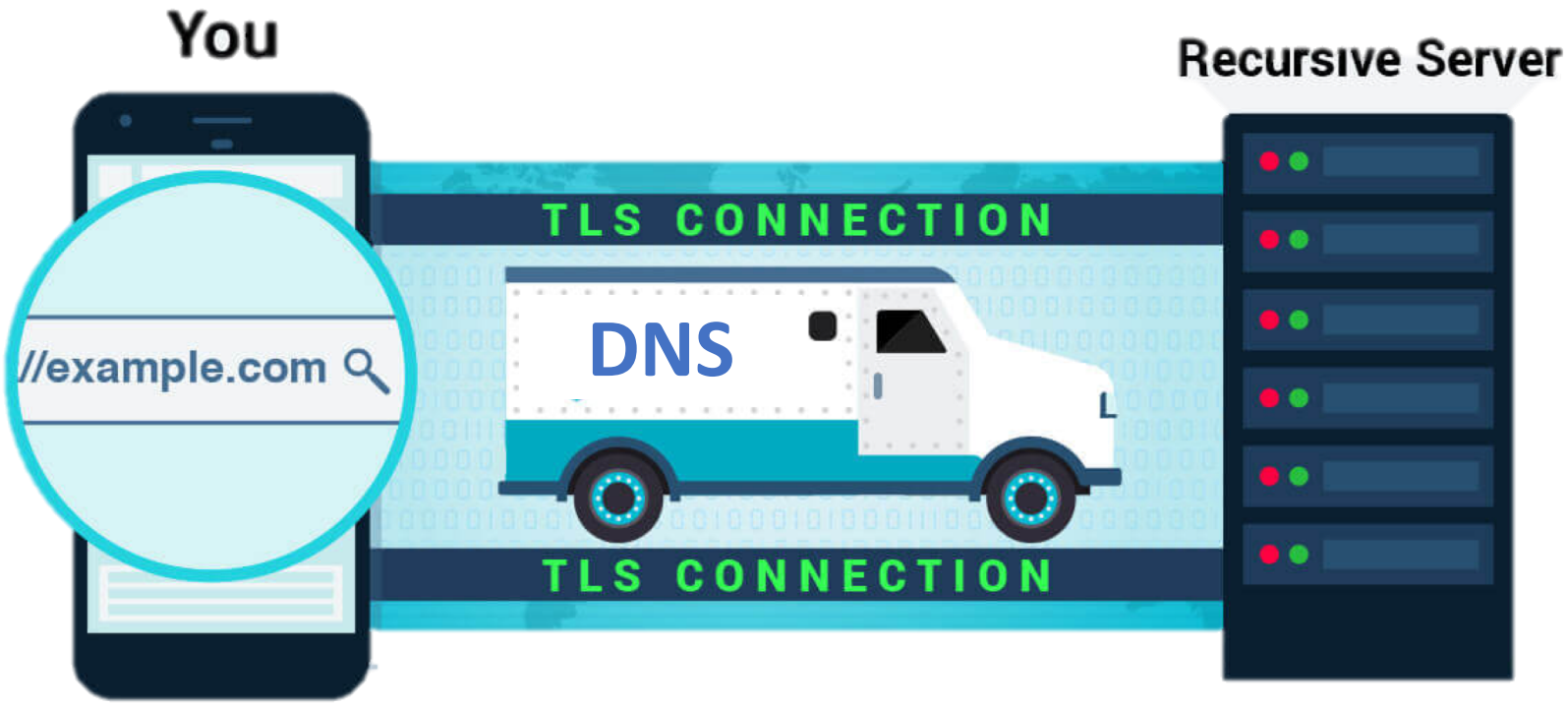
Uses Google

Geoff Huston, DNS, DNSSEC and Google's Public DNS Service, https://labs.apnic.net/?p=368

So how?

Solutions

- Encrypted DNS



* Pic from: https://tenta.com/blog/post/2017/12/dns-over-tls-vs-dnscrypt

Solutions

- Encrypted DNS

Resolvers can be authenticated

* Pic from: https://tenta.com/blog/post/2017/12/dns-over-tls-vs-dnscrypt

Solutions

- Encrypted DNS
  - ***Resolver authentication (RFC8310)***
  - DNS-over-TLS (RFC7858)
  - DNS-over-DTLS (RFC8094, experimental)
  - DNS-over-HTTPS (RFC8484)
- Online checking tool
  - Which resolver are you ***really*** using?
  - http://whatismydnsresolver.com/

Conclusions

- Understanding
  - A measurement platform to systematically study DNS interception
- Findings
  - DNS interception exists in 259 ASes we inspected globally
  - Up to 28% requests from China to Google are intercepted
  - Security concerns
- Mitigation
  - Resolver authentication; online checking tool

Who Is Answering My Queries?
Understanding and Characterizing Hidden Interception of the DNS Resolution Path

Baojun Liu, Chaoyi Lu, Haixin Duan,
Ying Liu, Zhou Li, Shuang Hao and Min Yang

lbj15@mails.tsinghua.edu.cn