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

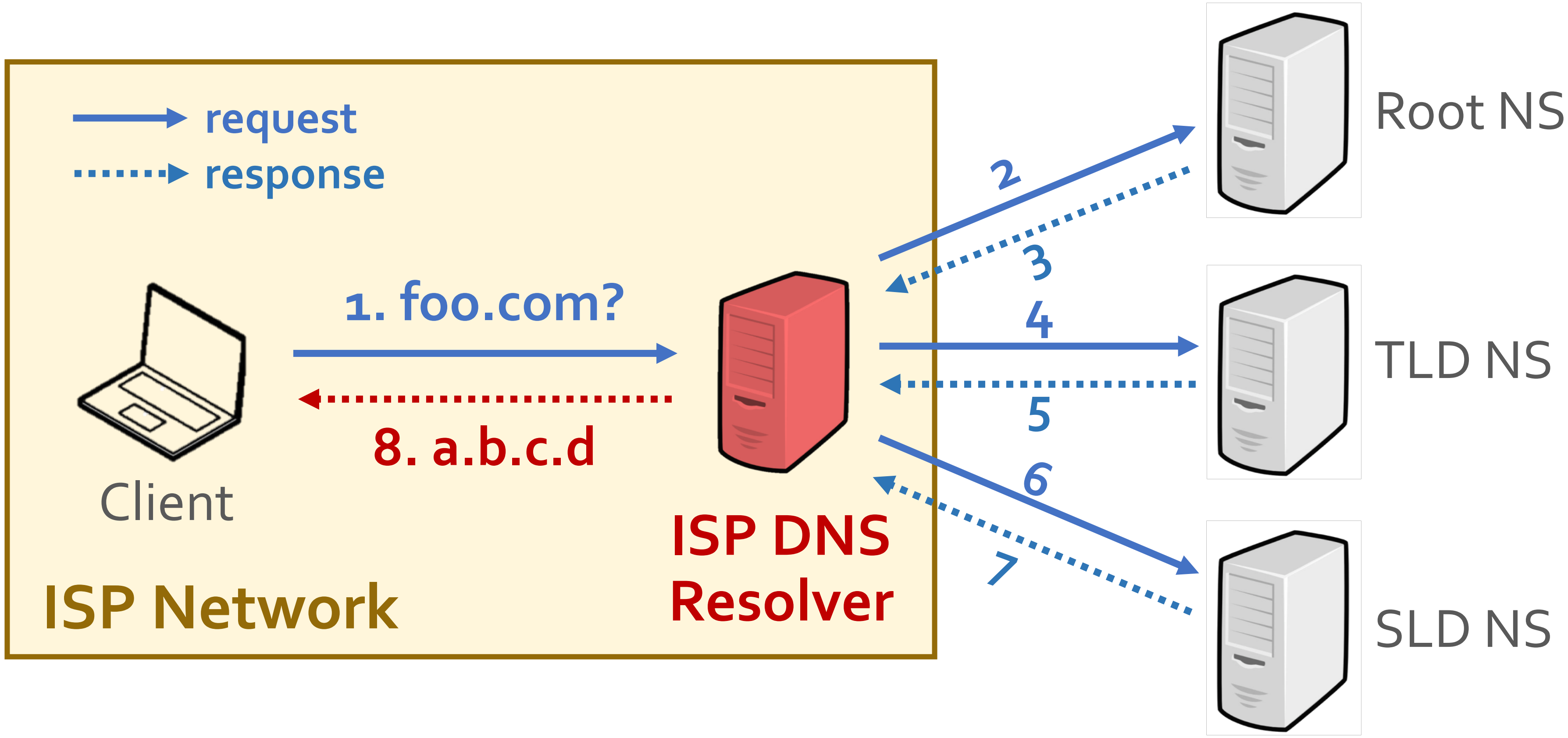
TSINGHUA UNIVERSITY 1911

UT DALLAS
The University of Texas at Dallas

FUDAN UNIVERSITY 1905

DNS Resolution

- ISP DNS Resolver
  - Might have security problems [Dagon, NDSS'08] [Weaver, SATIN'11] [Weaver, FOCI'11] [Kuhrer, IMC'15] [Chung, IMC'16] …



DNS Resolution

- Public DNS Resolver
  - Performance (e.g., load balancing)
  - Security (e.g., DNSSEC support)
  - DNS extension (e.g., EDNS Client Subnet)

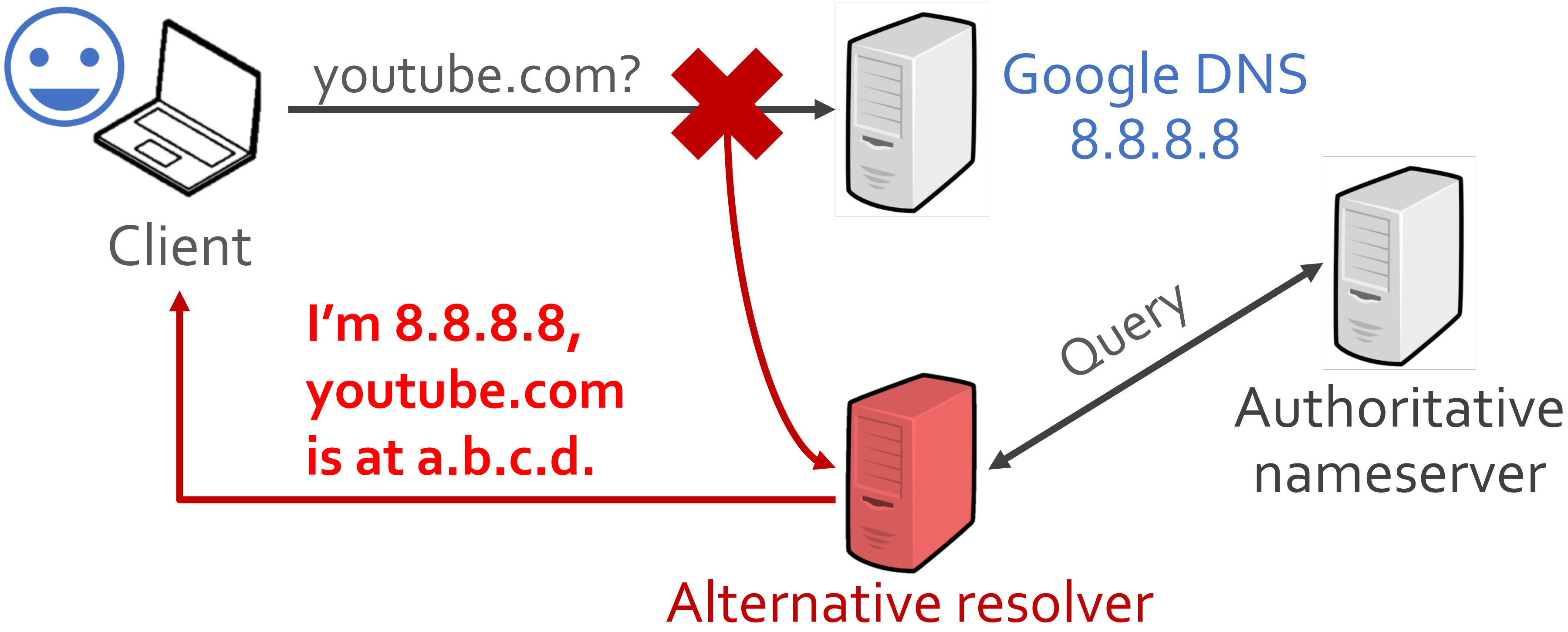
Google Public DNS

OpenDNS

CLOUDFLARE 1.1.1.1 DNS

DNS Interception

- Who is answering my queries?



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

Potential Interceptors

Internet Service Provider
(ISP)

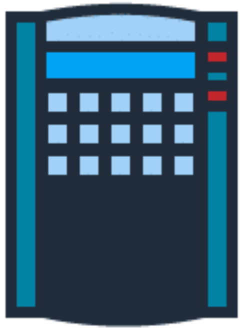
Censorship / firewall

Anti-virus software / malware

(E.g., Avast anti-virus)

Enterprise proxy

(E.g., Cisco Umbrella intelligent proxy)



Q1:

How to ***globally measure*** *the hidden DNS interception?*

Q2:

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

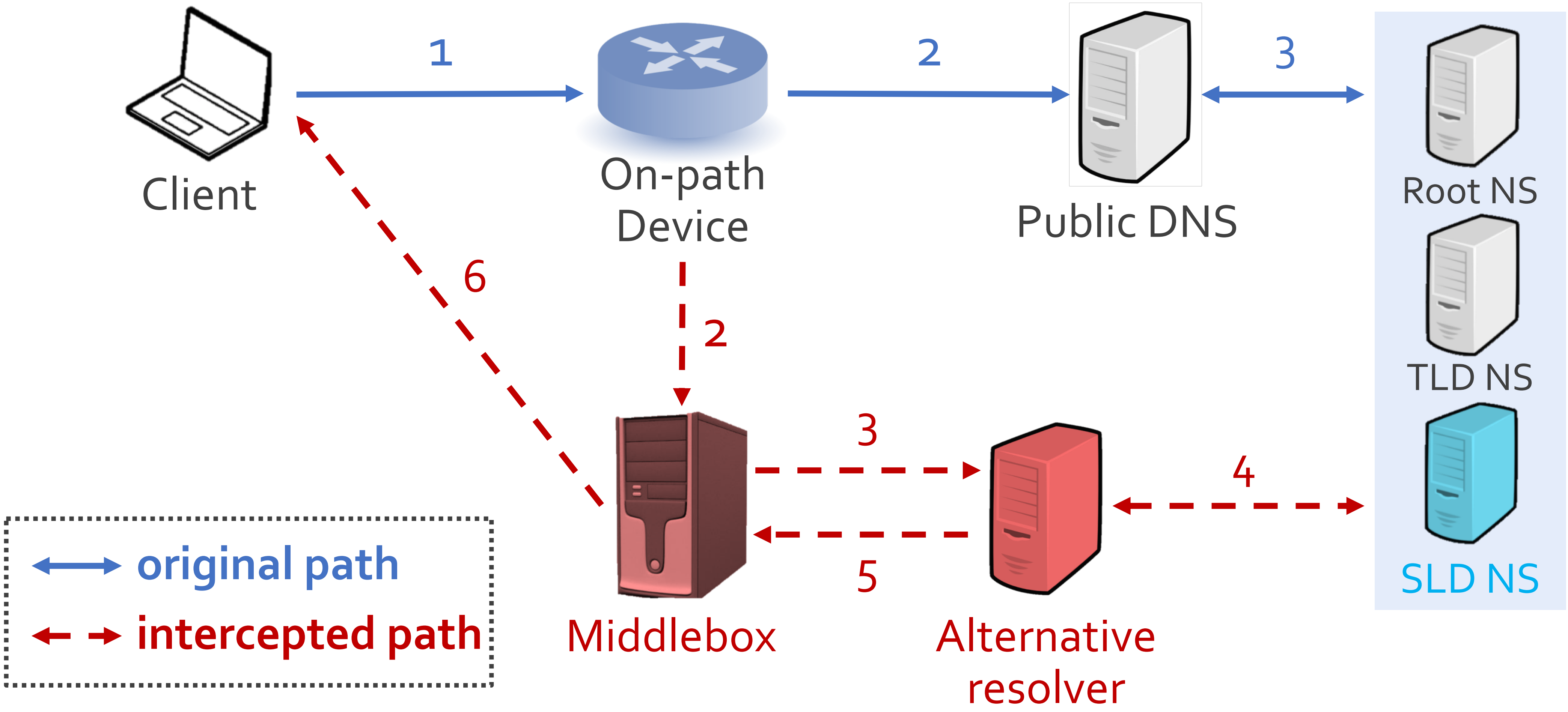
Motivation

Threat Model

Methodology

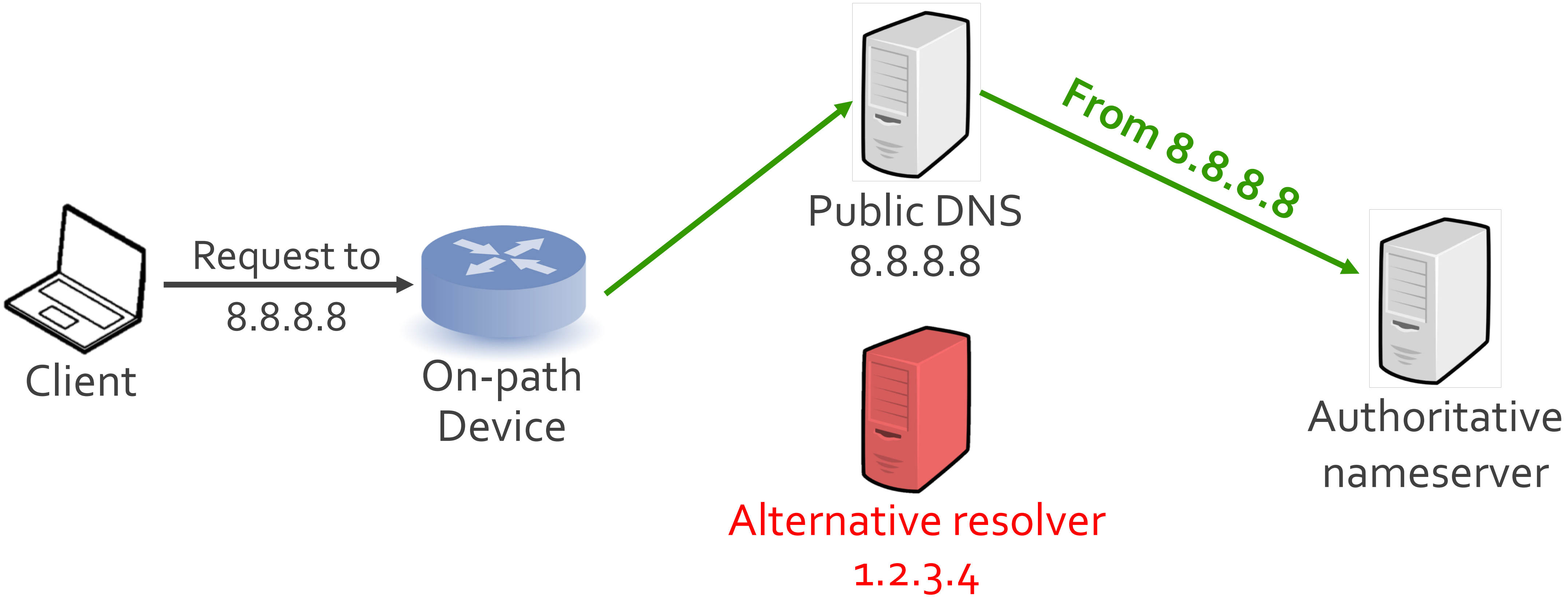
Analysis

Threat Model



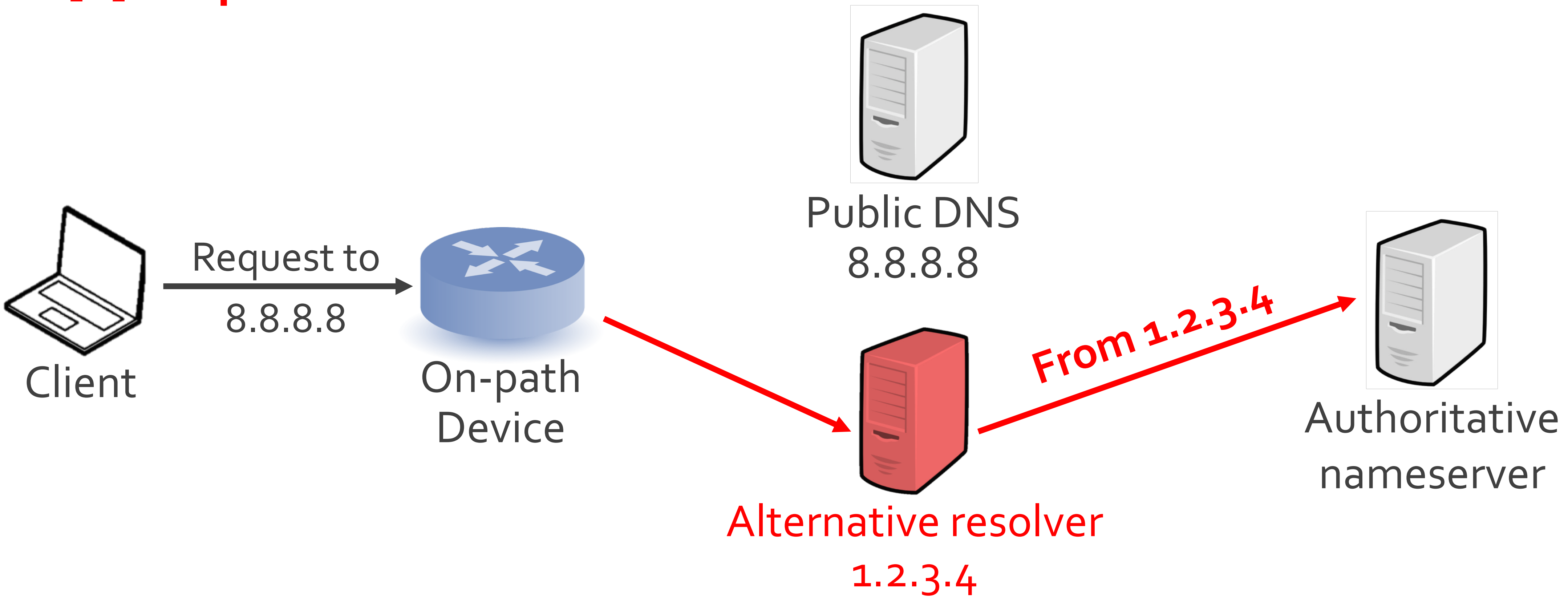
Threat Model

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



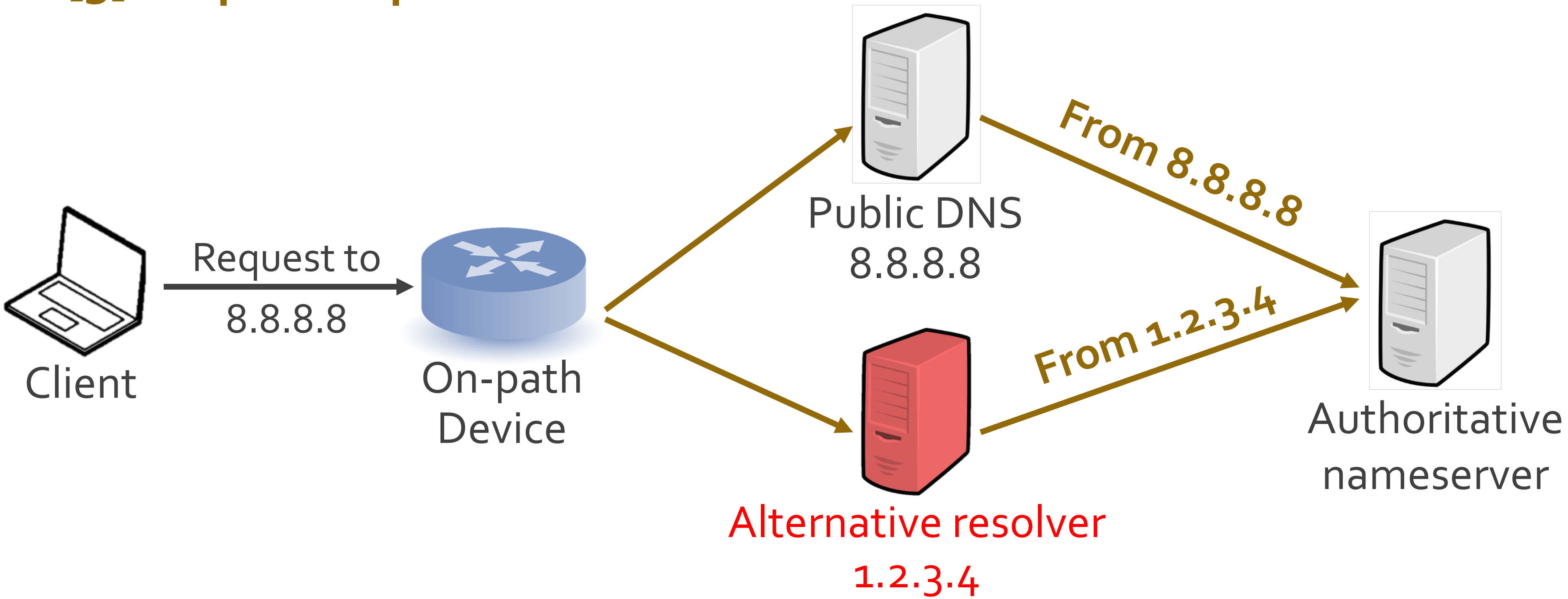
Threat Model

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



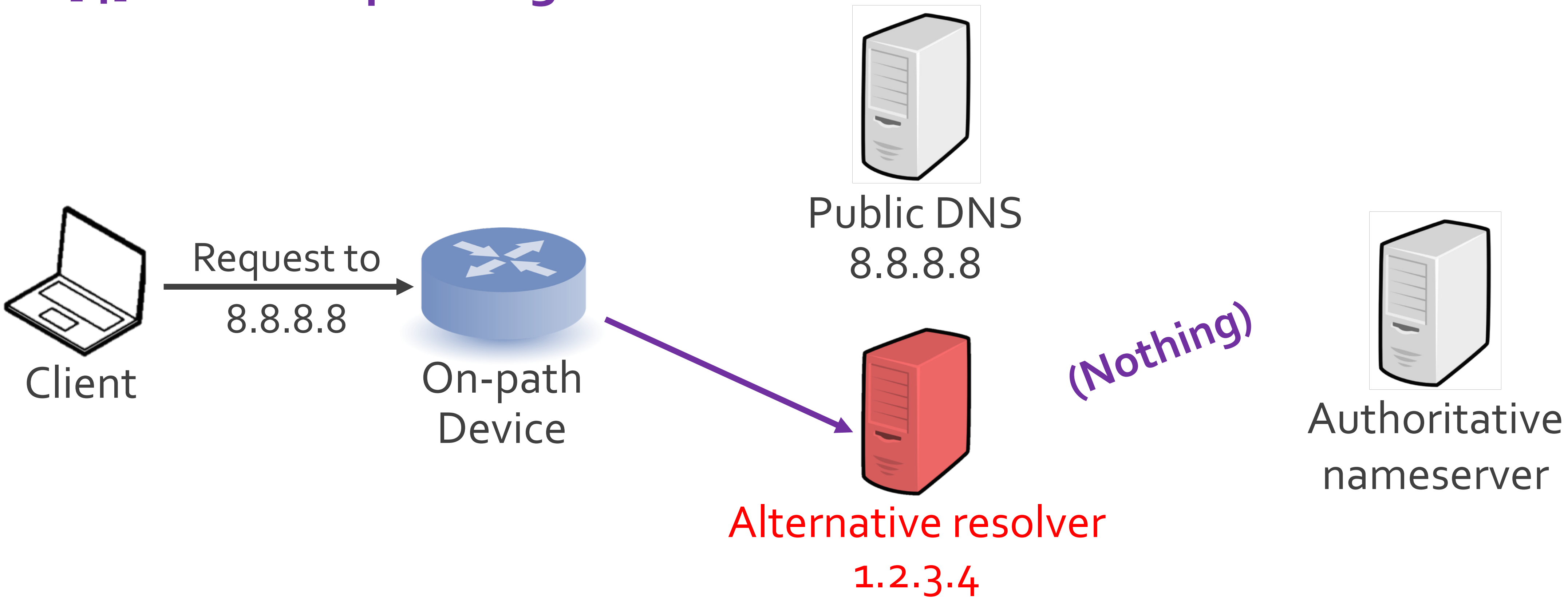
Threat Model

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



Threat Model

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



Motivation

Threat Model

Methodology

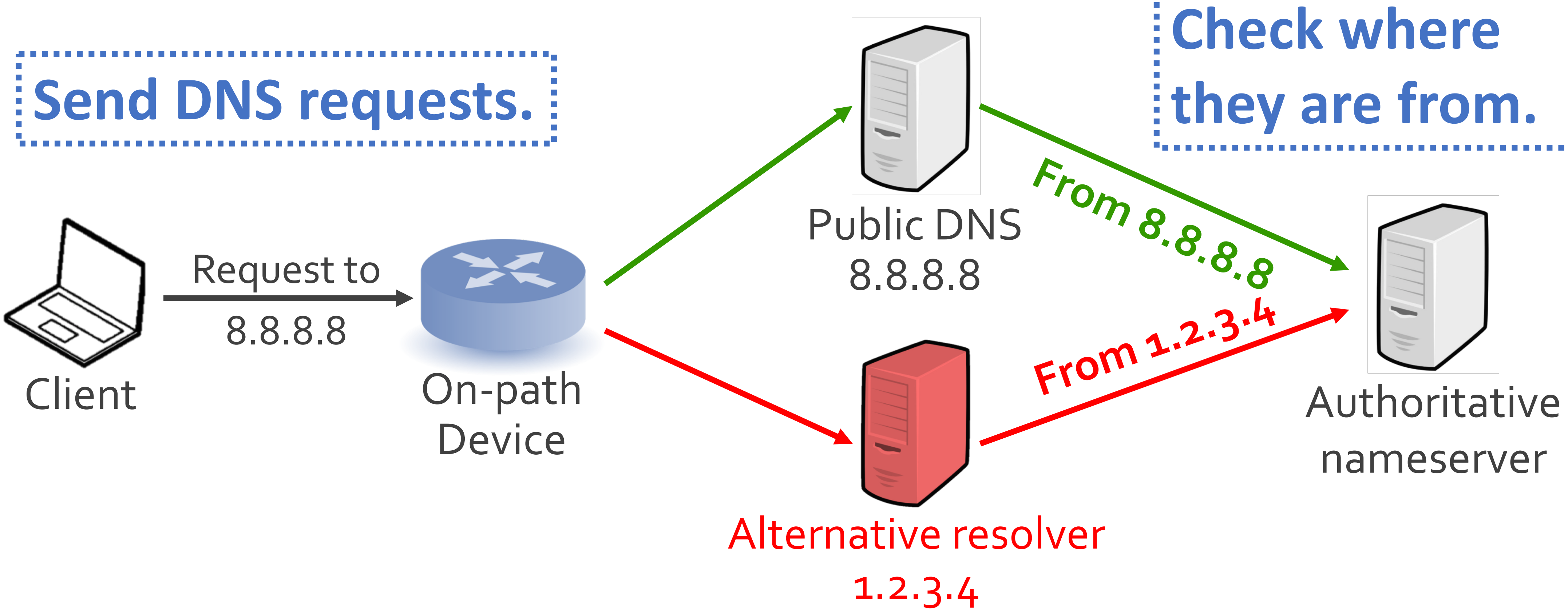
Analysis

How to Detect?

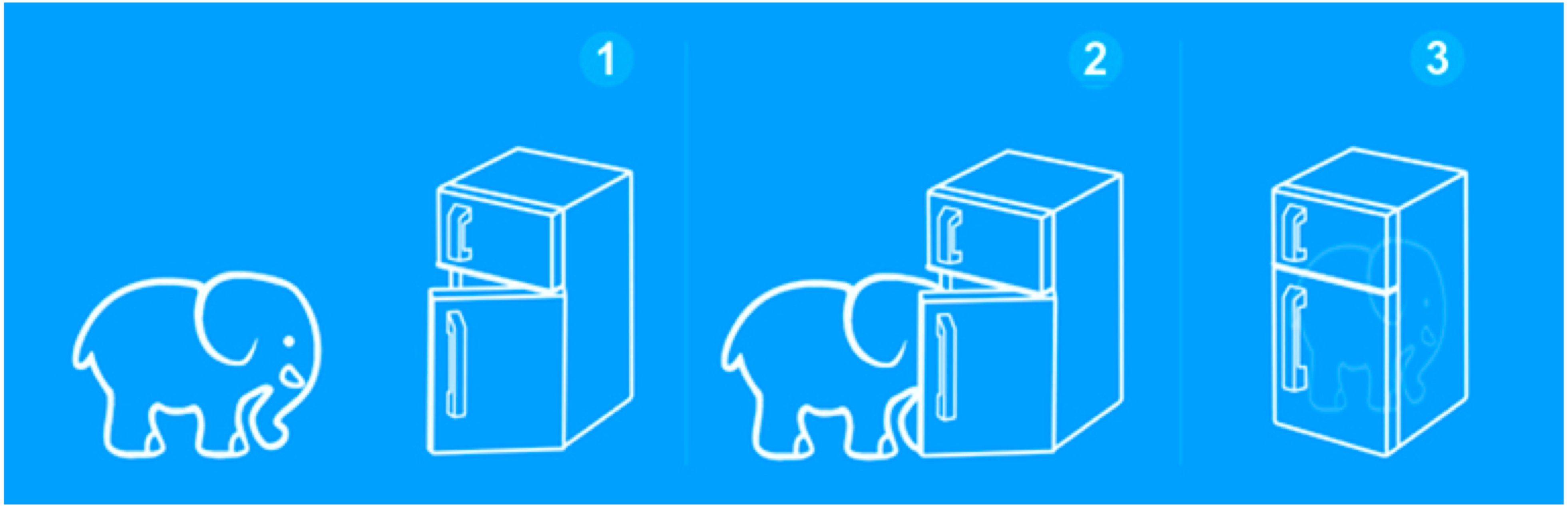
- At a glance

Send DNS requests.

Check where they are from.



How to Detect?



[1] Open the refrigerator

[2] Put in the elephant

[3] Close the door

→

[1] Collect vantage points

[2] Send DNS requests

[3] Collect requests on NS

* Pic source: cdc.tencent.com

Collect vantage points

Diversify DNS requests

Identify egress IP

Vantage Points

- Requirements
  - Ethical
  - Large-scale and geo-diverse
  - **Directly send DNS packets to specified IP**

Measurement frameworks

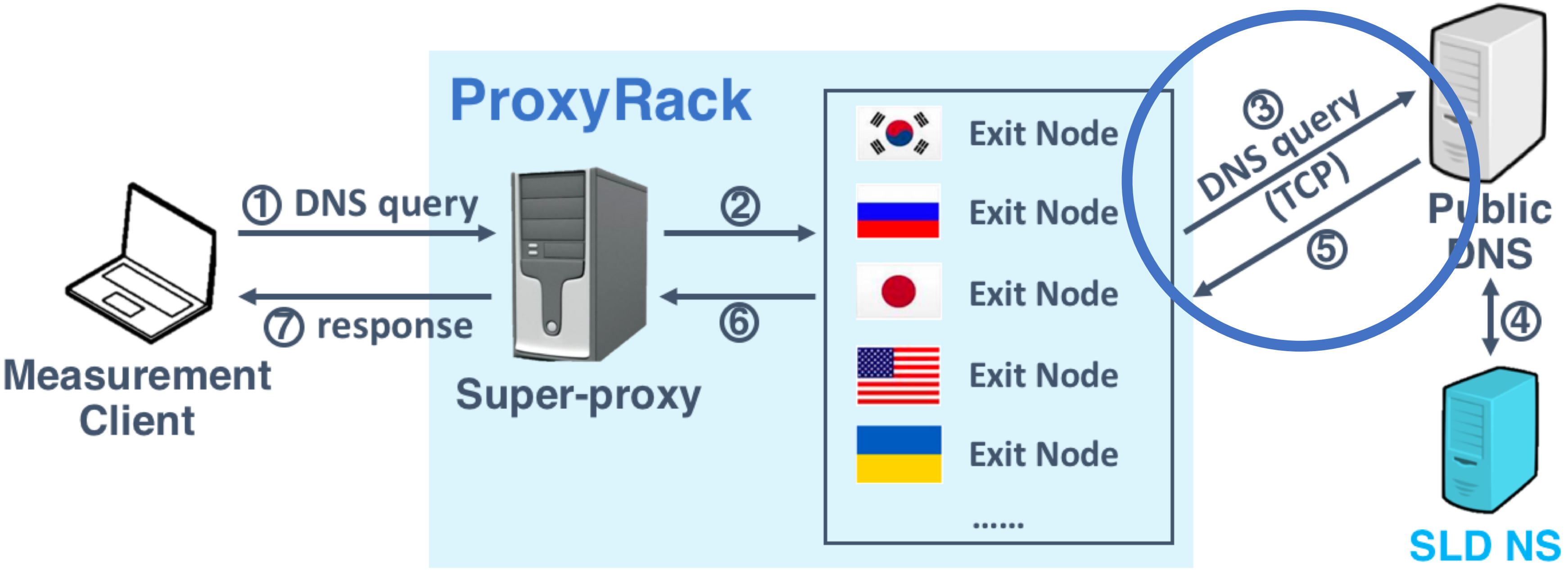
- Advertisement Networks
  - Flash applet [Huang, W2SP'11] [Chen, CCS'16]
  - JavaScript [Burnett, Sigcomm'15]
- HTTP Proxy Networks
  - Luminati [Chung, IMC'16] [Tyson, WWW'17], [Chung, Security'17]
- Internet Scanners
  - Open DNS resolver [Kuhrer, IMC'15] [Pearce, Security'17]
  - Scanners [Zakir, Security'13] [Pearce, SP'17]

☹

Cannot be used in this study.

Vantage Points

- Phase I: Global Analysis
  - ProxyRack: SOCKS5 residential proxy networks
  - Limitation: **TCP** traffic only



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**

Vantage Points

- Ethics considerations

Global (ProxyRack)	Pay for access
	Abide by ToS
	Only query our domain
China-wide (network debugging tool)	One-time consent
	Restrict traffic amount
	Only query our domain

Collect vantage points

Diversify DNS requests

Identify egress IP

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]

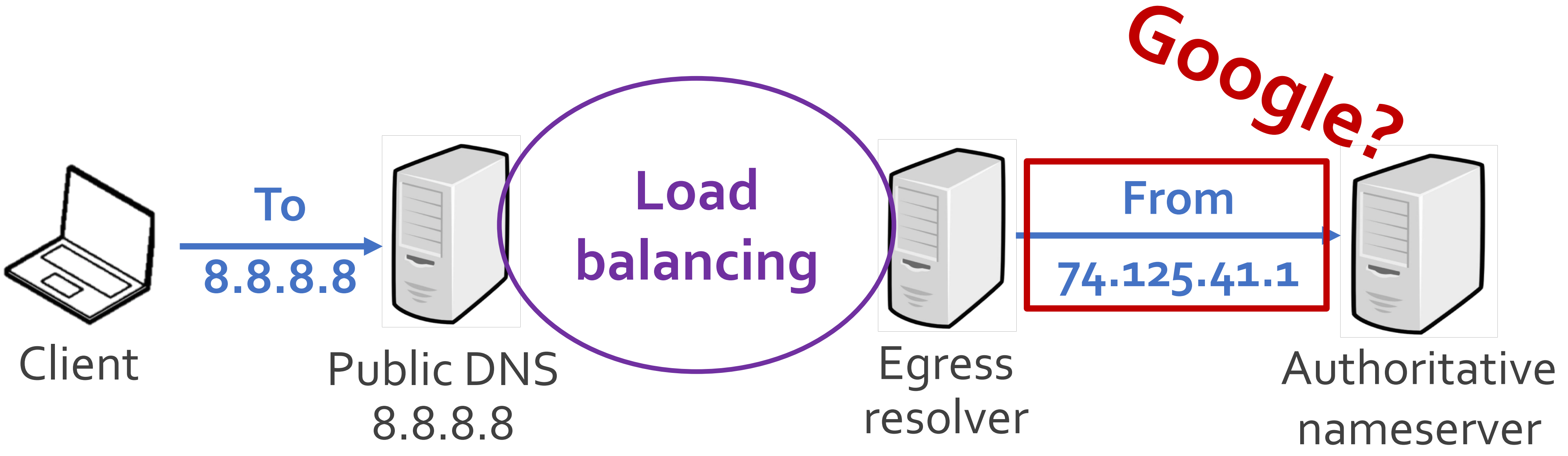
Collect vantage points

Diversify DNS requests

Identify egress IP

Egress IP

- Ownership of resolver IP
  – Is a request from public DNS?



Egress IP

- Ownership of resolver IP
  - Is a request from public DNS?
- Solution
  - **PTR & SOA records** of reverse lookups

```
$ dig -x 74.125.41.1

;; AUTHORITY SECTION:
125.74.in-addr.arpa.60   IN   SOA  ns1.google.com.
dns-admin.google.com. 207217296 900 900 1800 60
```

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

Q1: Interception Characteristics

Q2: DNS Lookup Performance

Q3: Response Manipulation

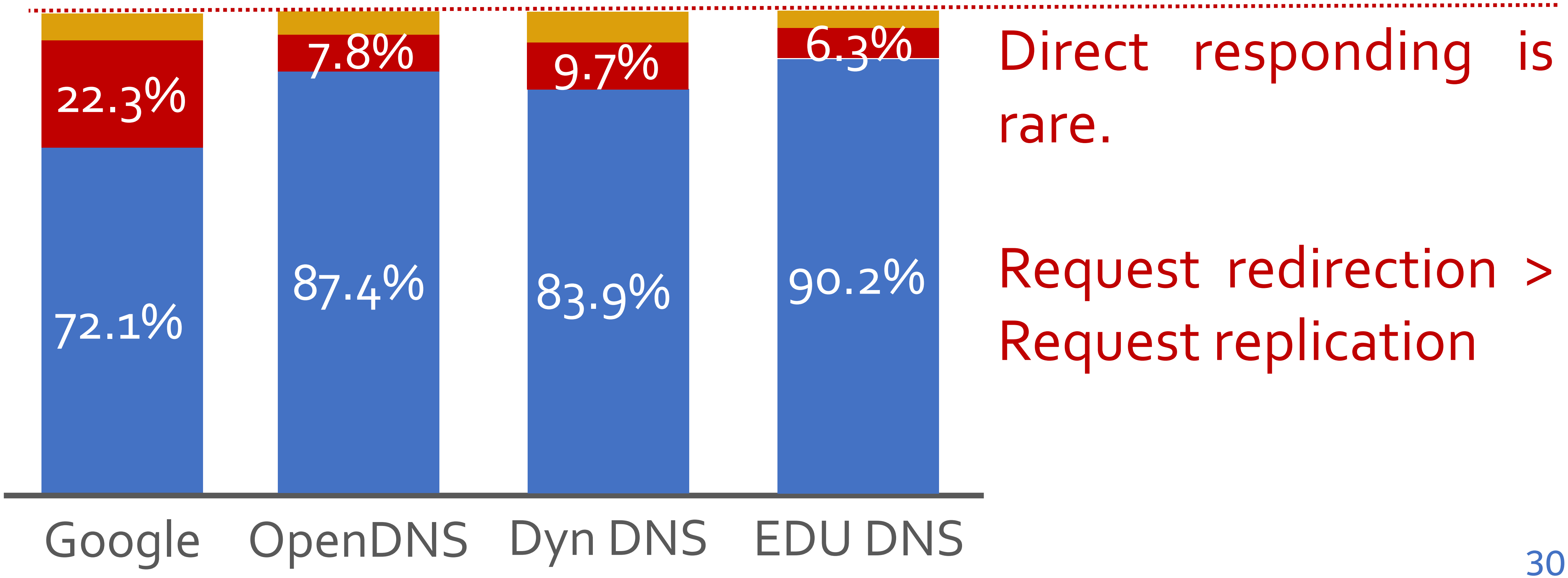
Q4: Security Threats

Q5: Interception Motivations

Q6: Solutions

Interception Characteristics

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

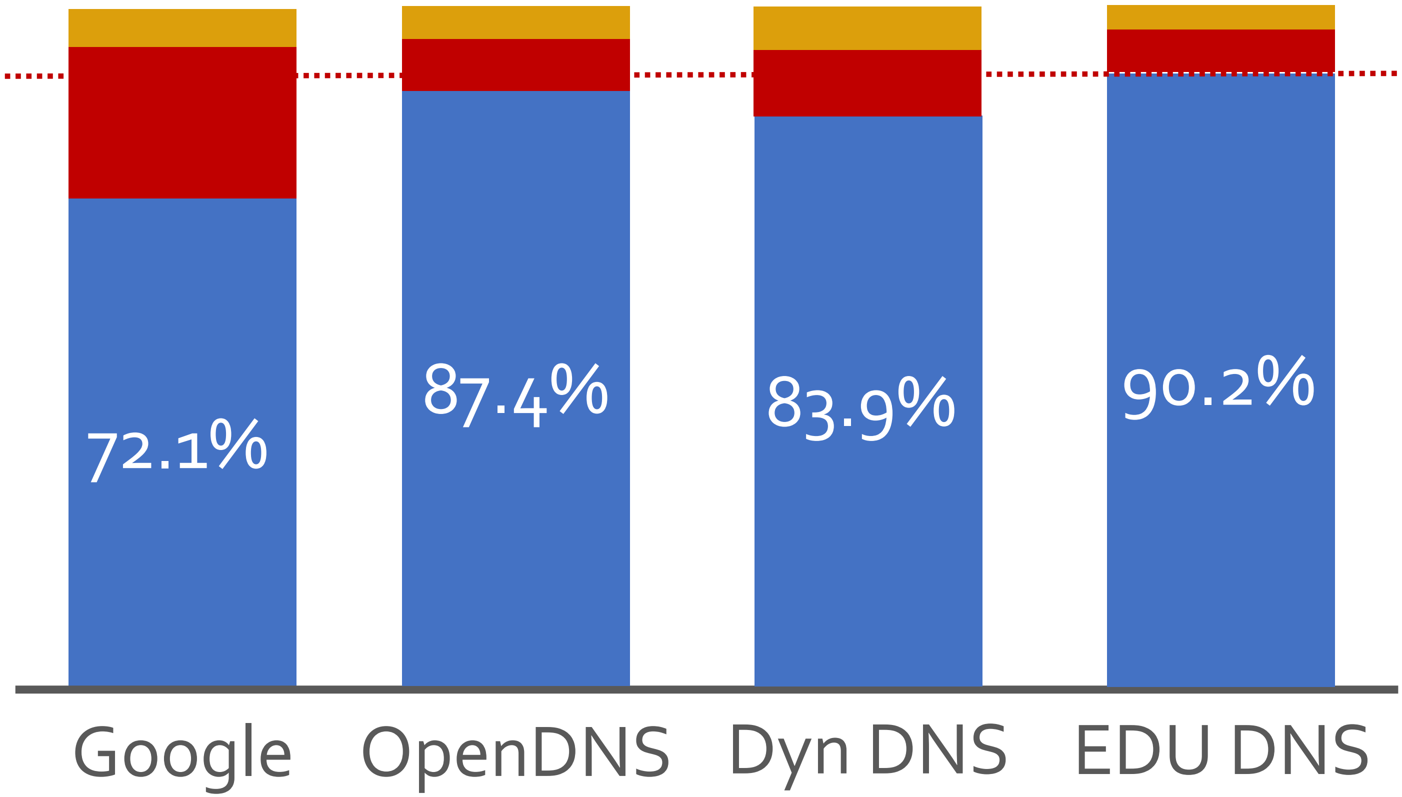


Direct responding is rare.

Request redirection > Request replication

Interception Characteristics

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



Requests to **popular public DNS services** are more likely to be intercepted.

Interception Characteristics

- ASes (% of total requests)
  - Sorted by # of total requests

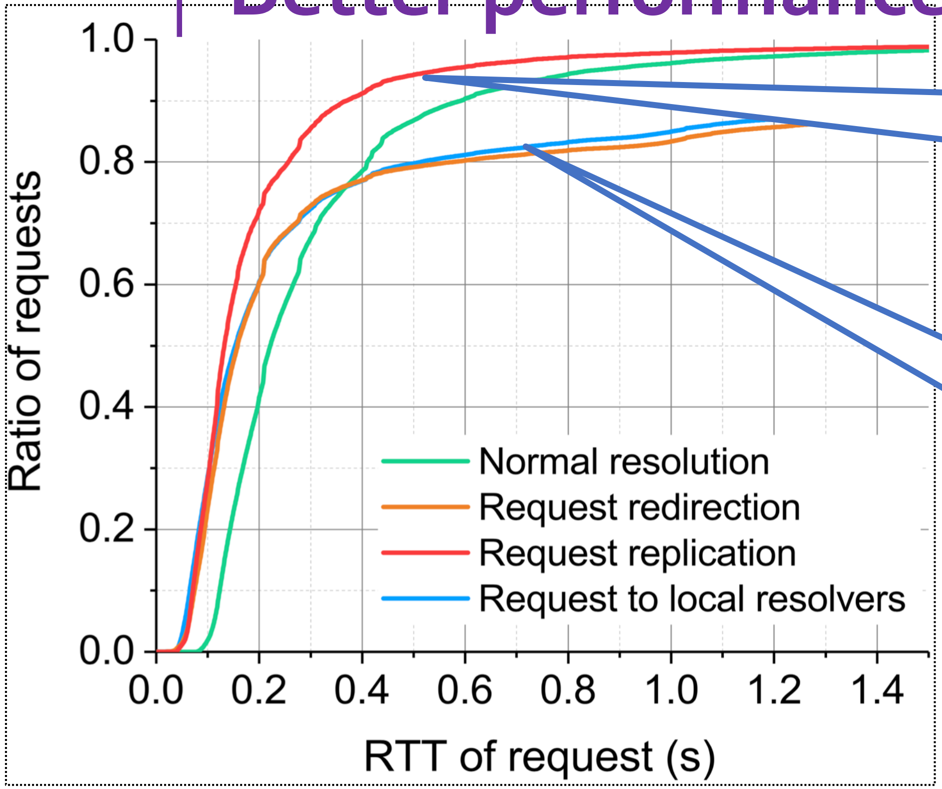
AS	Organization	Redirection	Replication	Alternative Resolver
AS4134	China Telecom	5.19%	0.2%	116.9.94.* (AS4134)
AS4837	China Unicom	4.59%	0.51%	202.99.96.* (AS4837)
AS9808	China Mobile	**32.49%**	**8.85%**	112.25.12.* (AS9808)
AS56040	China Mobile	**45.09%**	0.04%	120.196.165.* (AS56040)

Interception strategies can be **complex**, and **vary** among ASes.

DNS Lookup Performance

- RTT of requests
  - Which requests complete faster?

↑ Better performance



Request replication vs. Normal resolution:

Better.

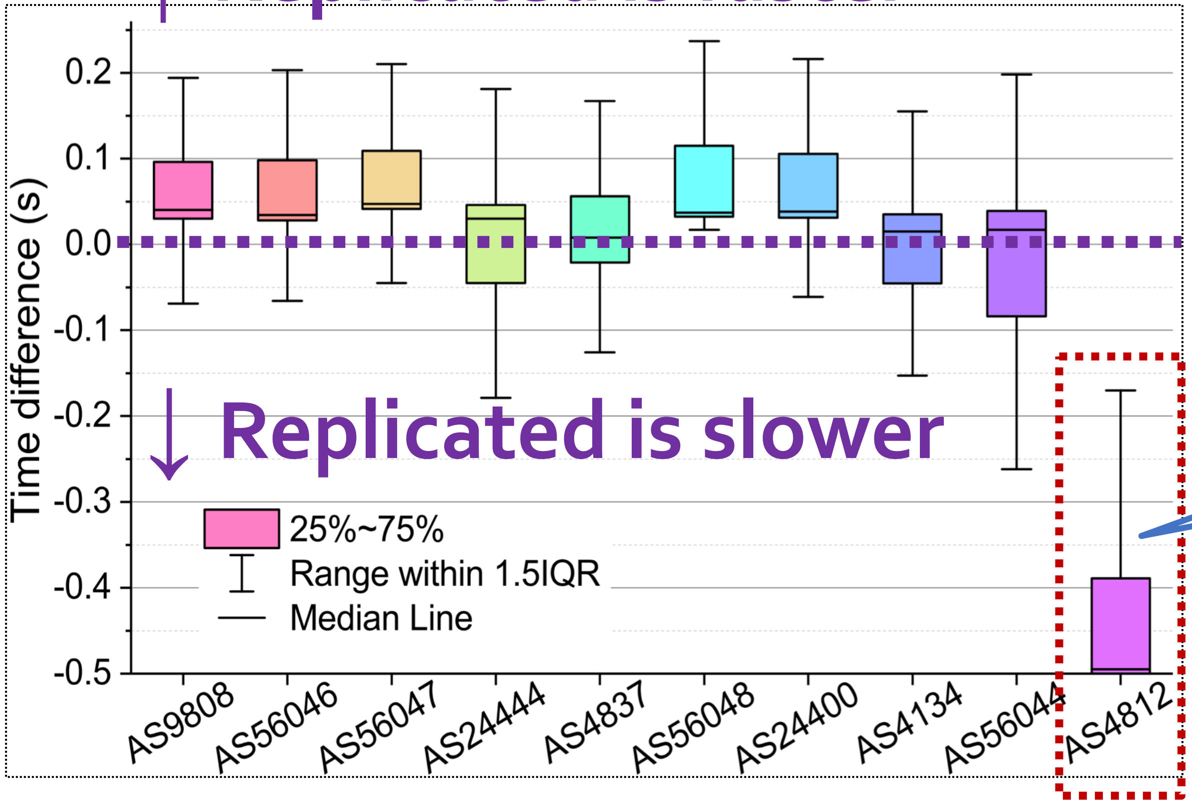
Request redirection vs. Request to local resolver:

Very similar.

DNS Lookup Performance

- Arrival time of replicated requests
  - Which requests reach NS faster?

↑ Replicated is faster



↓ Replicated is slower

In AS4812, **ALL** replicated requests arrive **slower than** their original counterparts.

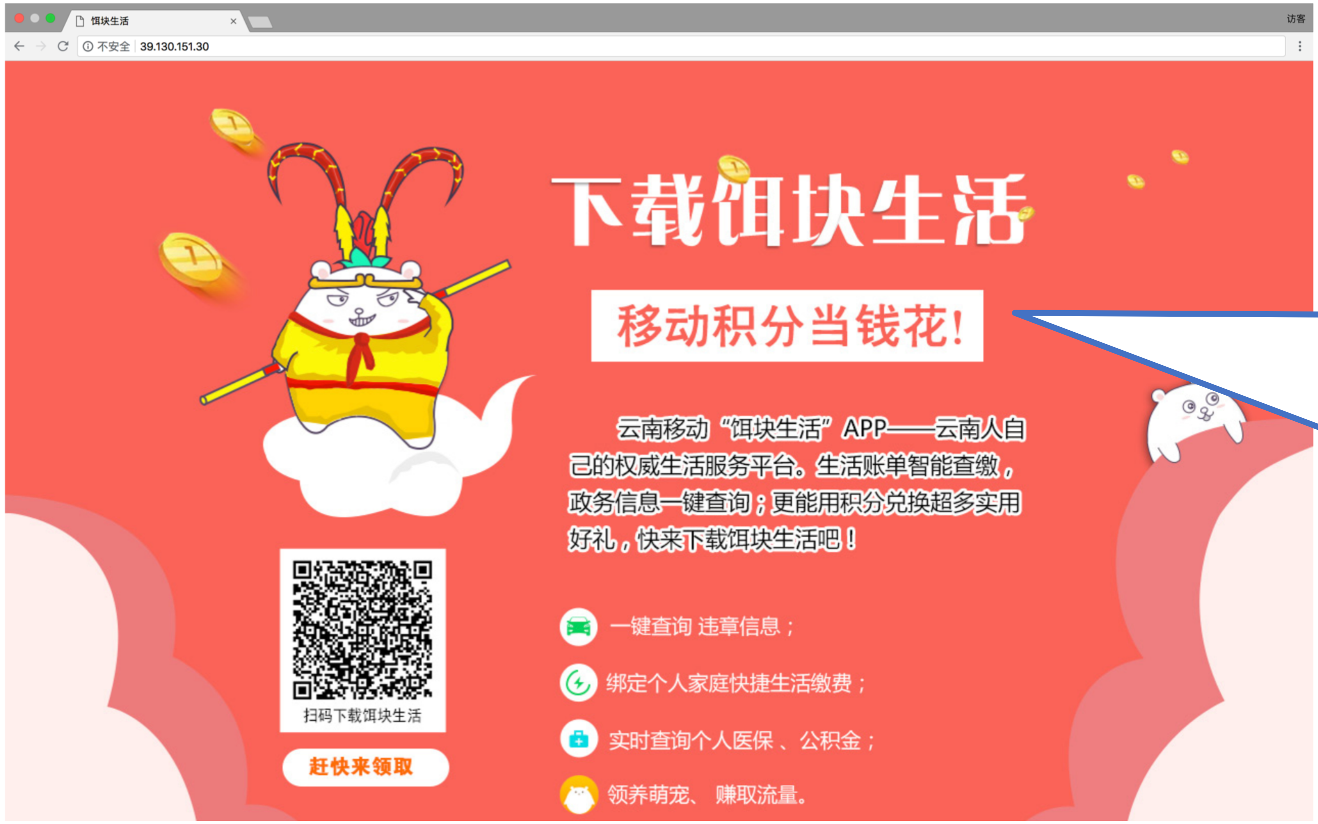
Response Manipulation

- DNS record values
  - Which responses are tampered?

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



下载饵块生活

移动积分当钱花!

云南移动"饵块生活"APP——云南人自己的权威生活服务平台。生活账单智能查缴，政务信息一键查询；更能用积分兑换超多实用好礼，快来下载饵块生活吧！

- 一键查询 违章信息；
- 绑定个人家庭快捷生活缴费；
- 实时查询个人医保 、公积金；
- 领养萌宠、 赚取流量。

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

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

Interception Motivations

- Vendors
  - Routers
  - Software platforms
- Motivations
  - Improving DNS security ?
  - Improving DNS lookup performance ?
  - Reducing traffic financial settlement ✓

Solutions

- Encrypted DNS
  - **Resolver authentication (RFC8310)**
  - DNS-over-TLS (RFC7858)
  - DNS-over-DTLS (RFC8094, experimental)
  - DNS-over-HTTPS
- 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
  - Brings security concerns
- Motivations
  - Reducing traffic financial settlement
- Mitigation
  - 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