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

Presenter: Zhou Li (UC Irvine EECS)

Tsinghua University 1911

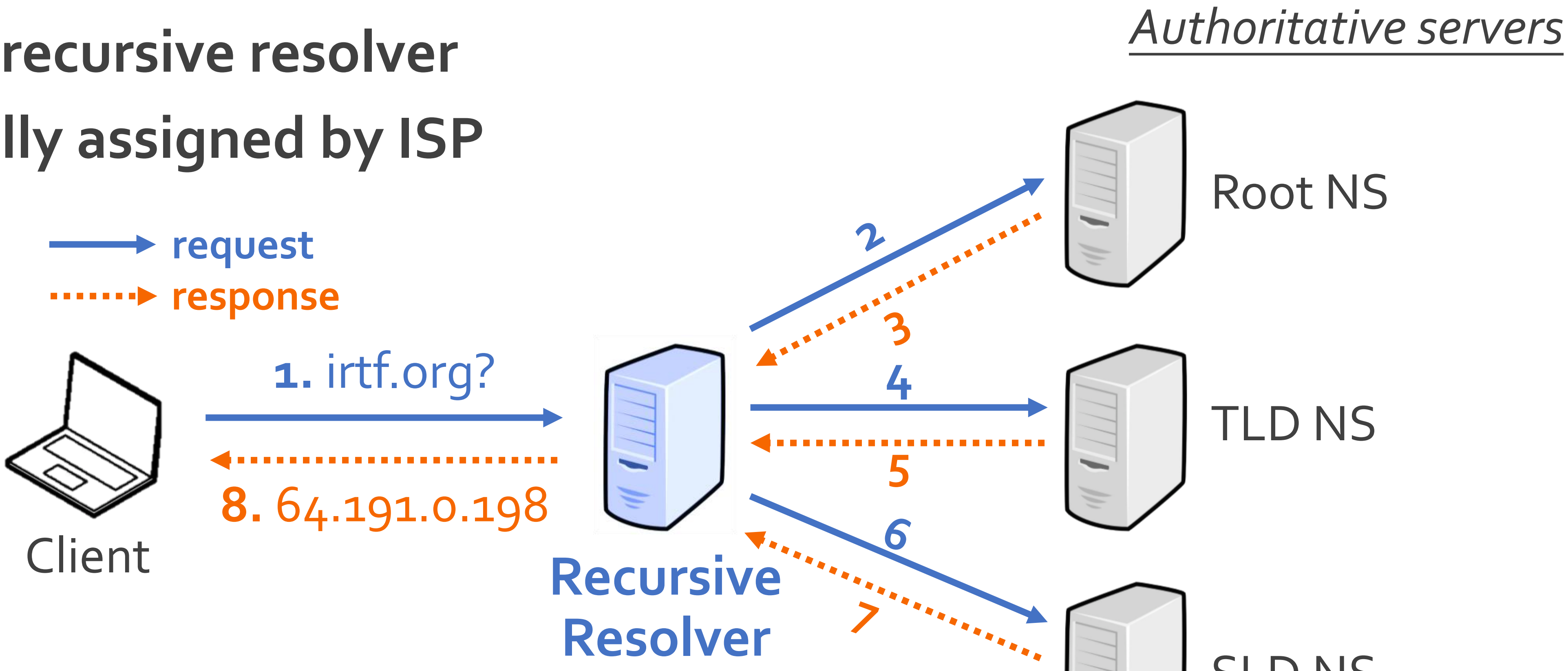
UCI Samueli School of Engineering
University of California, Irvine

UT DALLAS The University of Texas at Dallas

FUDAN UNIVERSITY 1905

DNS Resolution

- DNS: the beginning of Internet activities
  - By a **recursive resolver**
  - **Usually assigned by ISP**



DNS Resolution

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

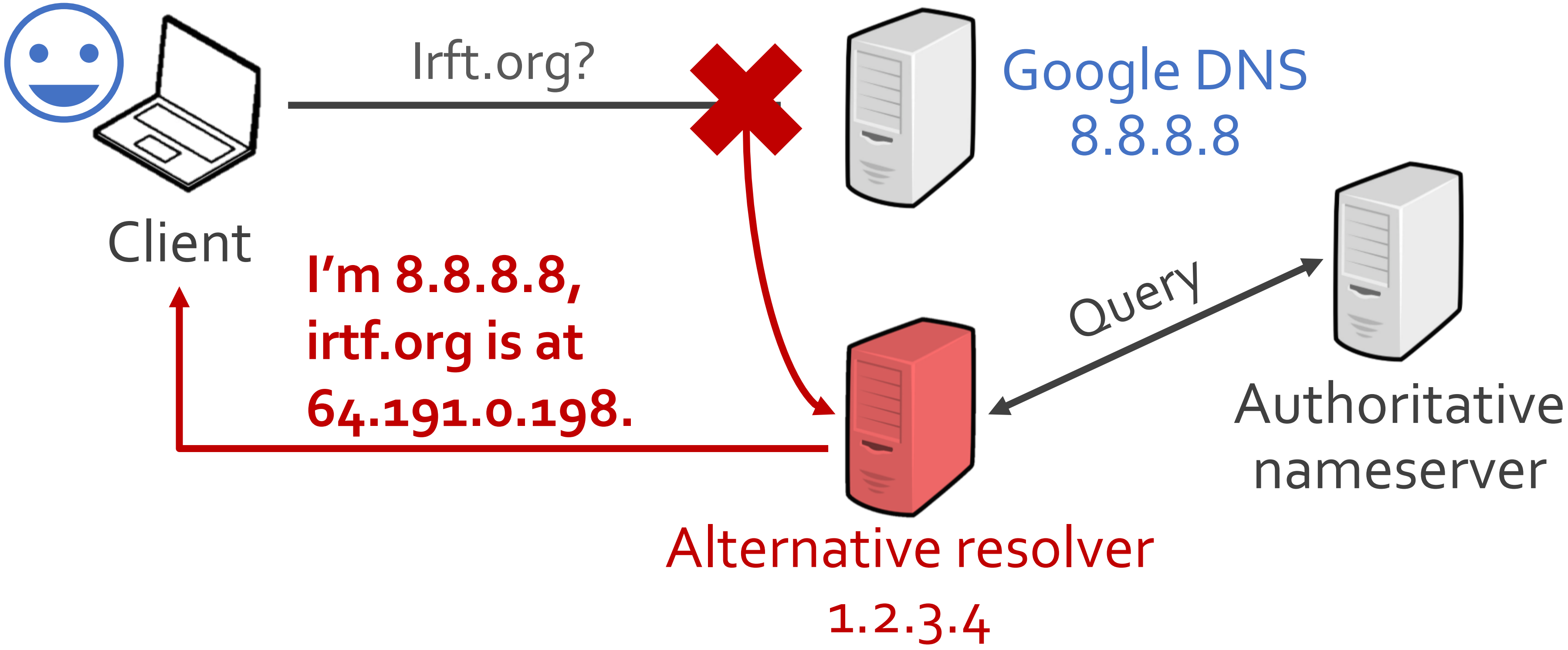
Google Public DNS

OpenDNS

CLOUDFLARE 1.1.1.1 DNS

DNS Interception

- Who is answering my queries?



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

Potential Interceptors

Network Providers (ISP)

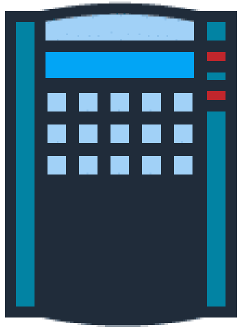
Censorship / firewall

Anti-virus software / malware

(E.g., Avast anti-virus)

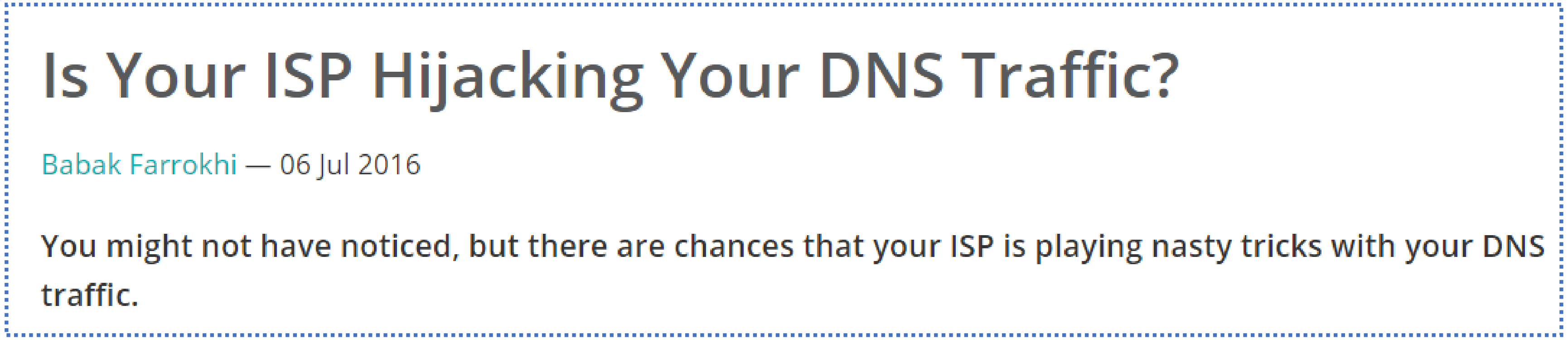
Enterprise proxy

(E.g., Cisco Umbrella intelligent proxy)



Potential Interceptors

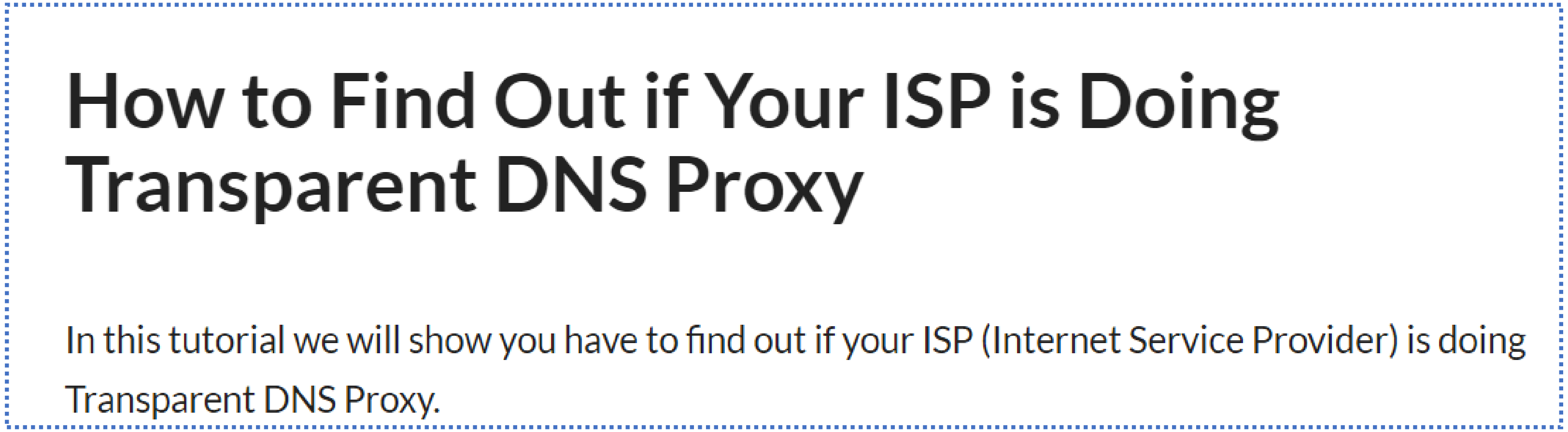
Network Providers



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/

Q1:

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

Q2:

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

Motivation

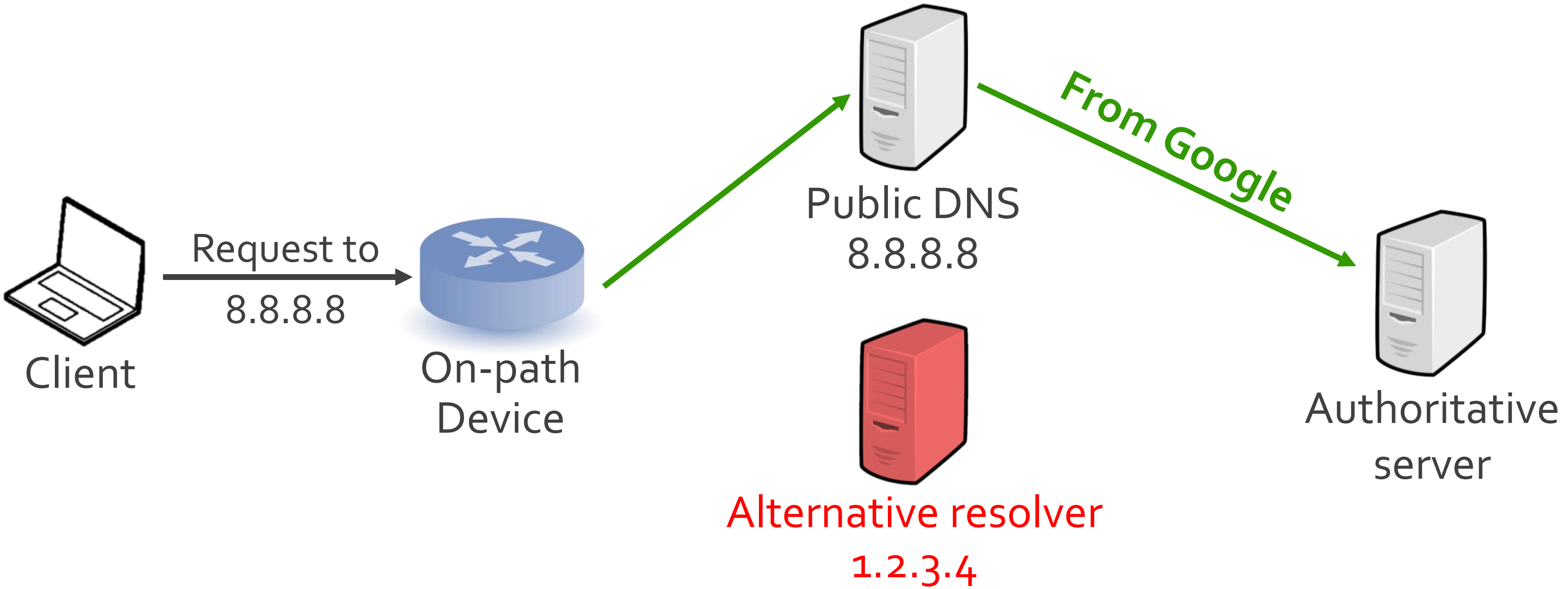
Threat Model

Methodology

Analysis

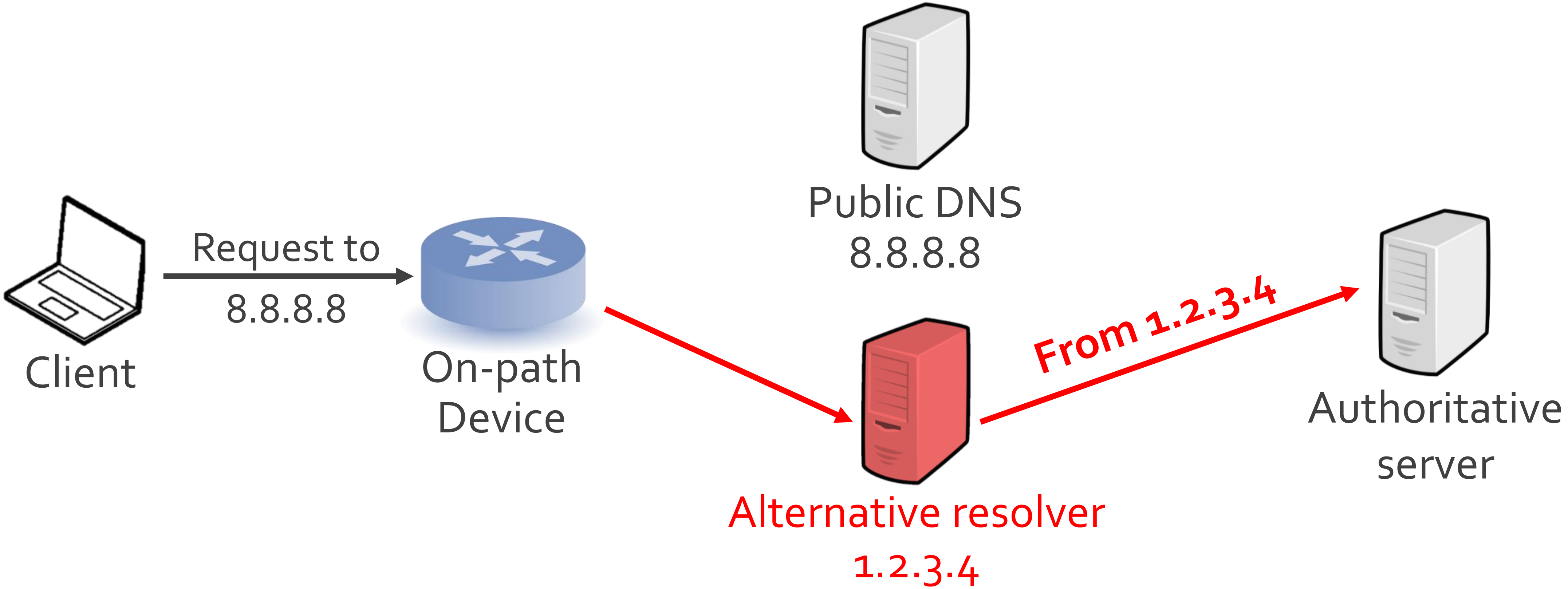
Threat Model

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



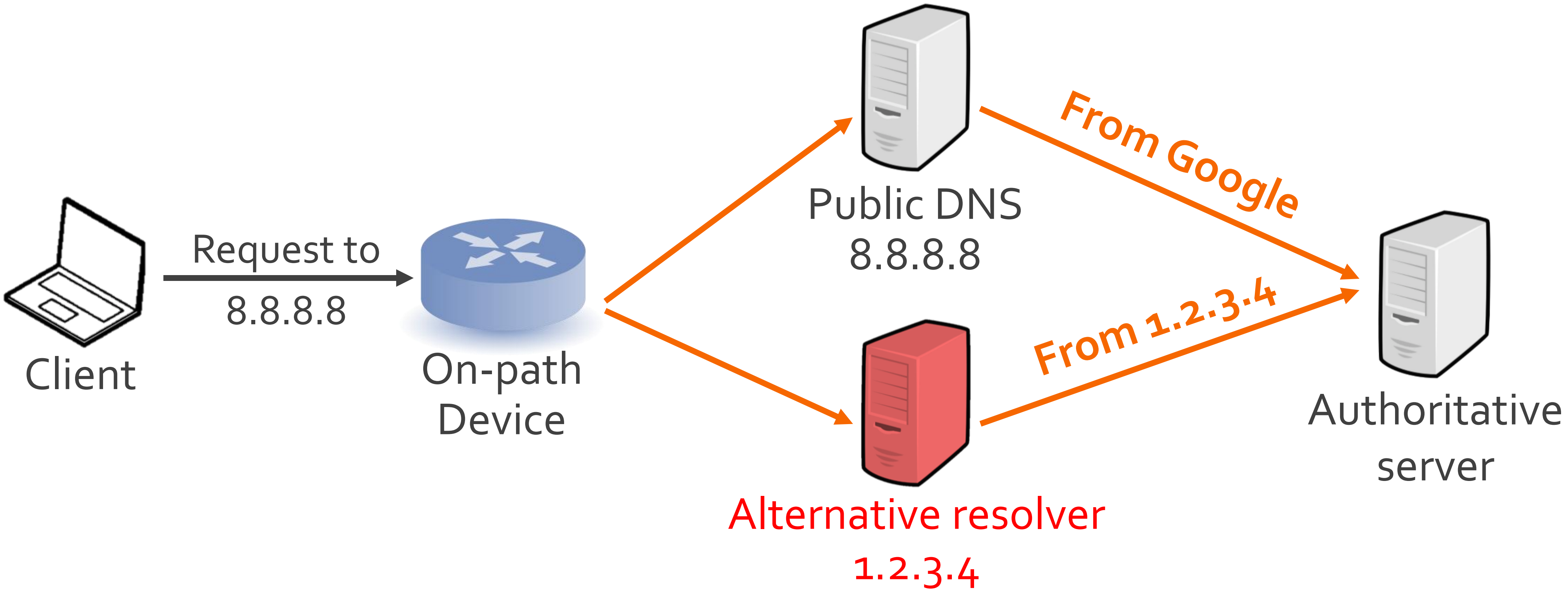
Threat Model

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



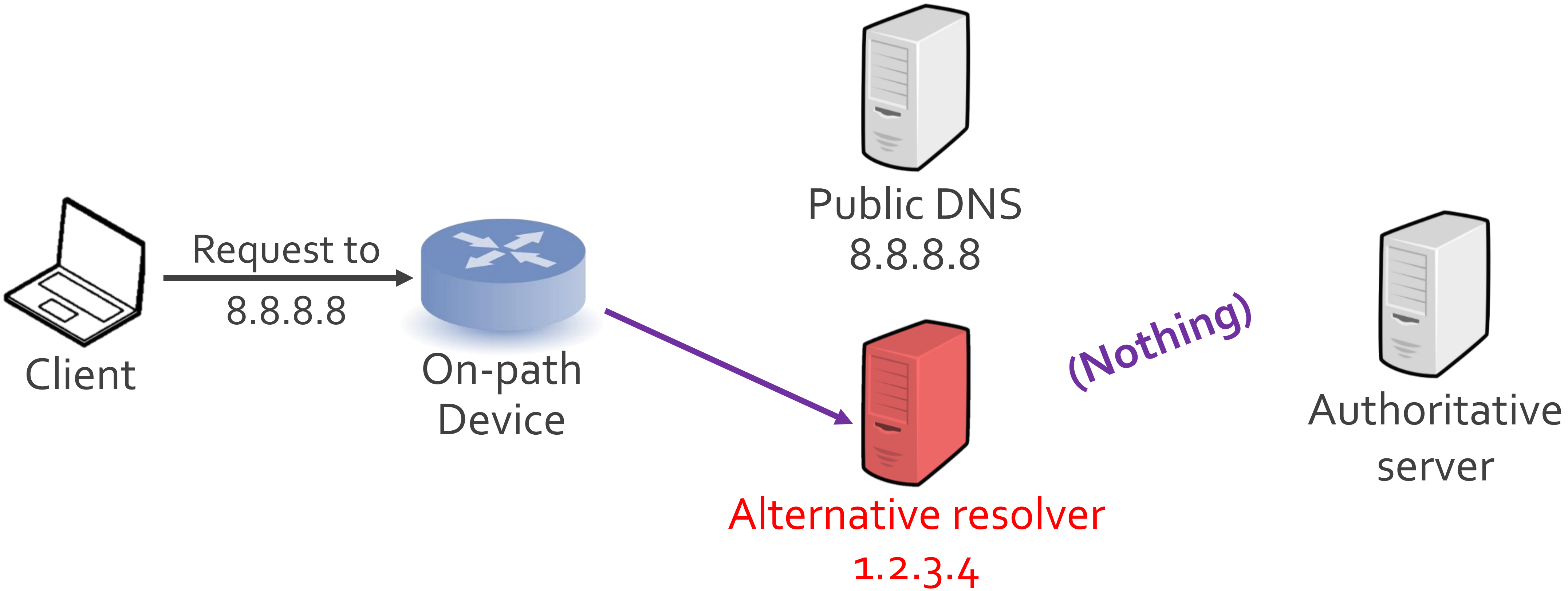
Threat Model

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



Threat Model

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



Motivation

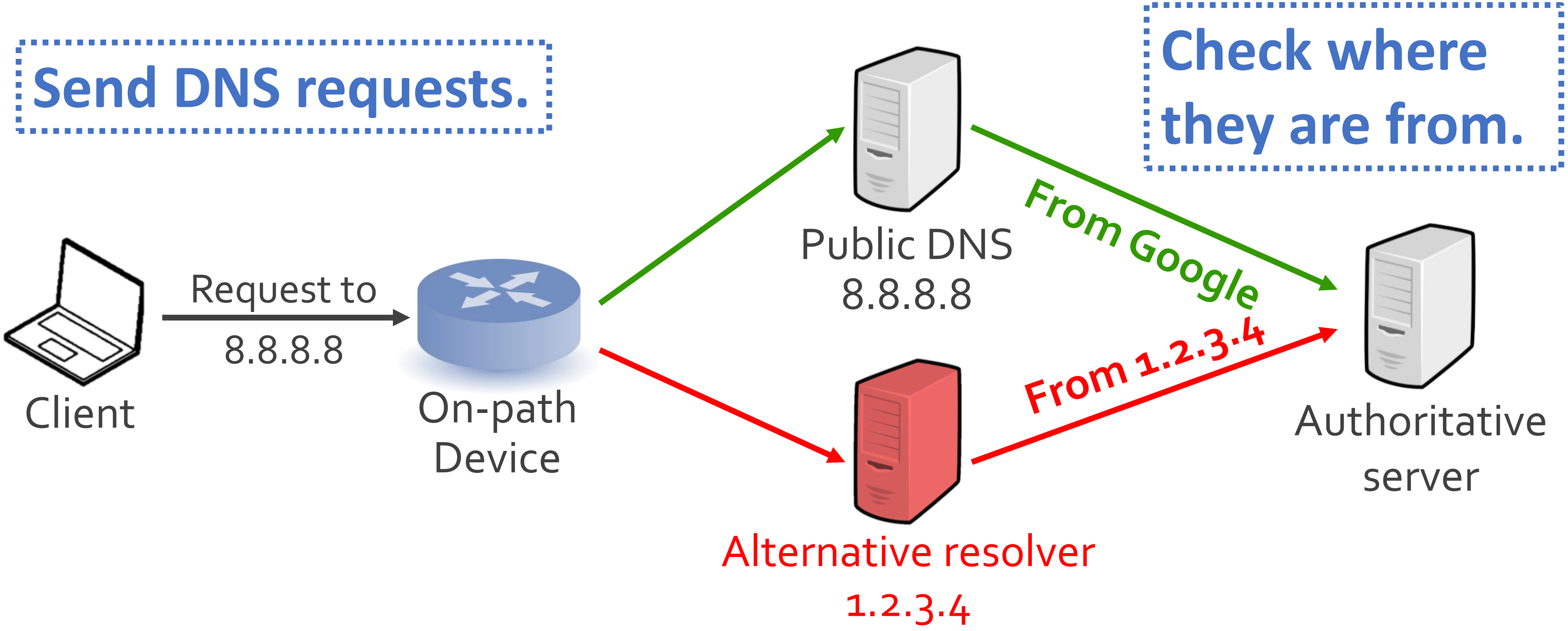
Threat Model

Methodology

Analysis

How to Detect?

- **End-to-end** data collection and comparison



Send DNS requests.

Check where they are from.

Client

Request to 8.8.8.8

On-path Device

Public DNS 8.8.8.8

Alternative resolver 1.2.3.4

From Google

From 1.2.3.4

Authoritative server

Vantage Points

- Phase I: Global Analysis
  - ProxyRack: SOCKS 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

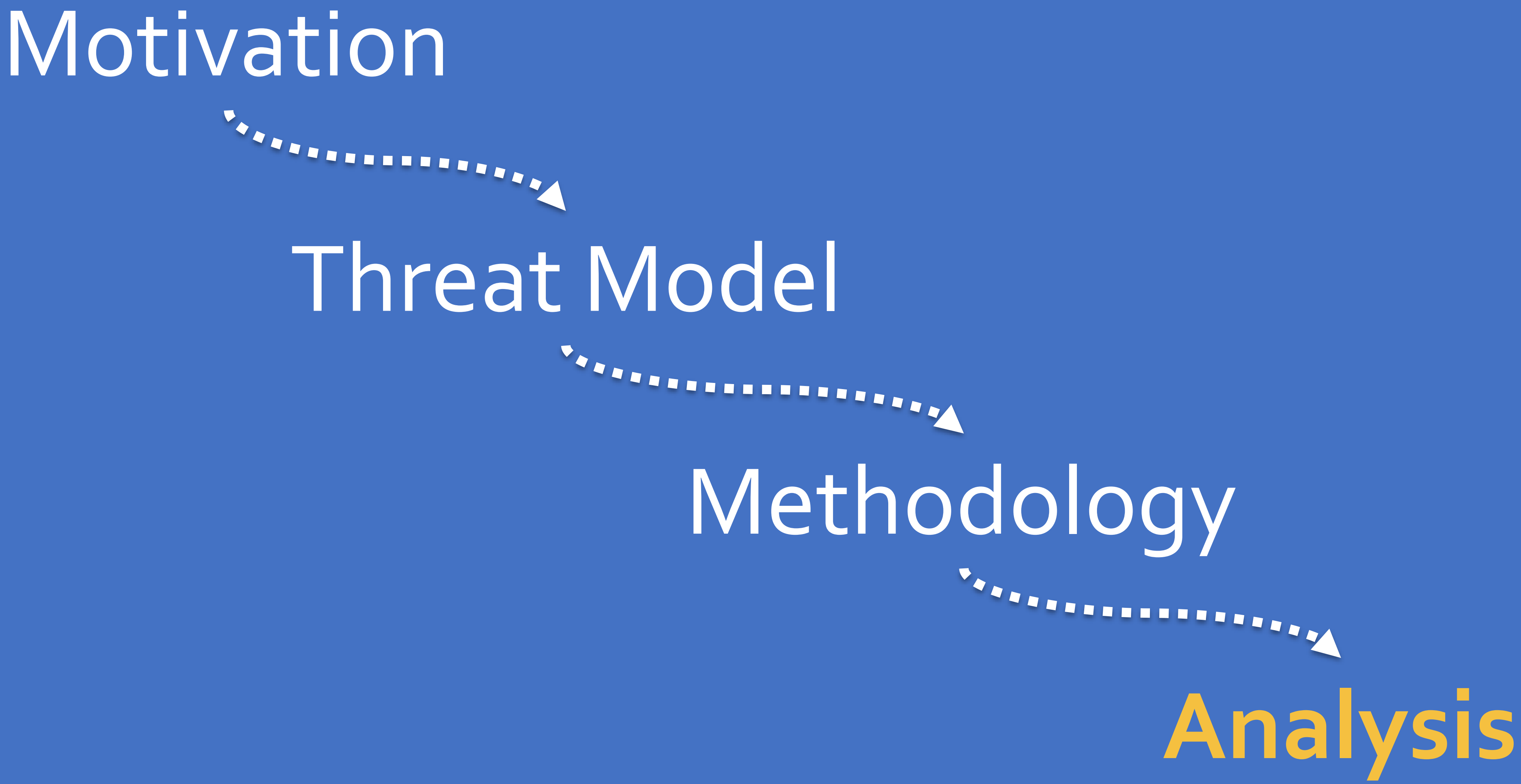
- Requirements
  - **Diverse**: triggering interception behaviors
  - **Controlled**: allowing fine-grained analysis

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

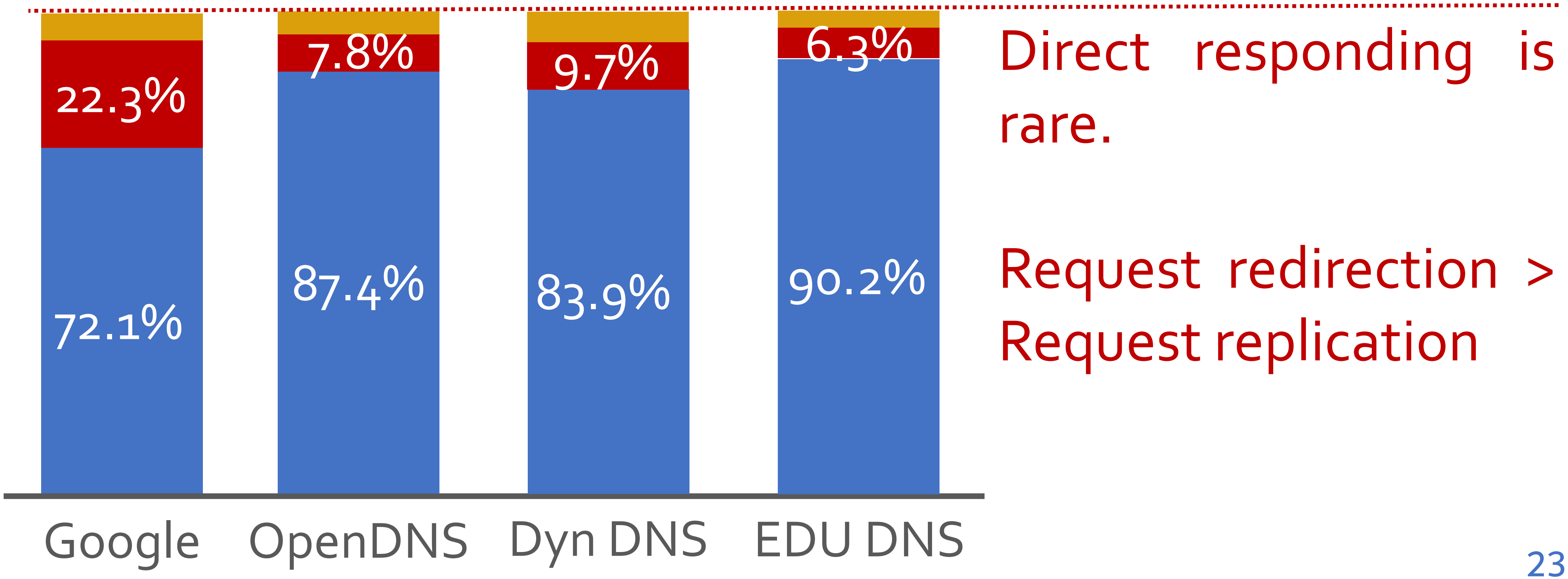
Google Public DNS	**27.9%** 7.3%	OpenDNS	**12.6%** 0.9%
ORACLE + Dyn	**16.1%** 2.3%	EDU DNS	**9.8%** ↓ 1.1%

Popular resolvers are prone to be intercepted.

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

Are my responses tampered?

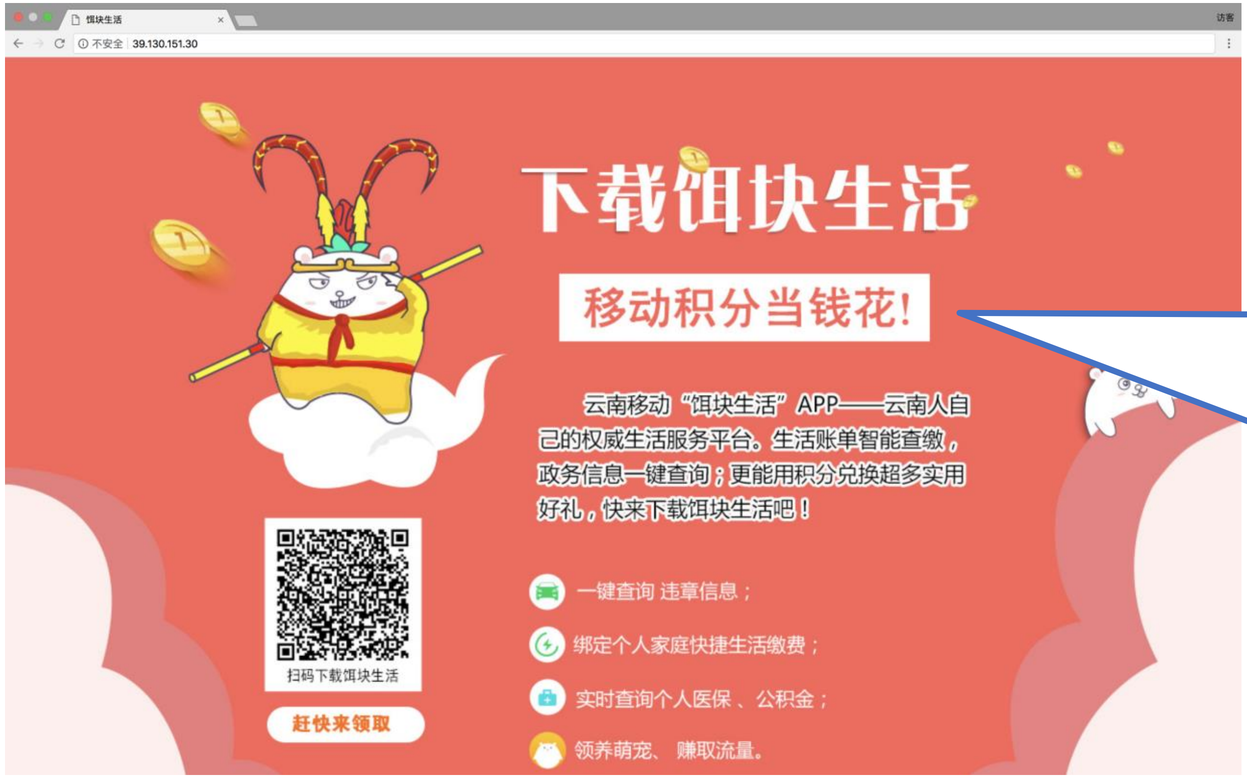
Response Manipulation

- 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



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**.

So why should I care?
Any threats?

Security Threats

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

DNSSEC

Only 43% resolvers support DNSSEC

BIND

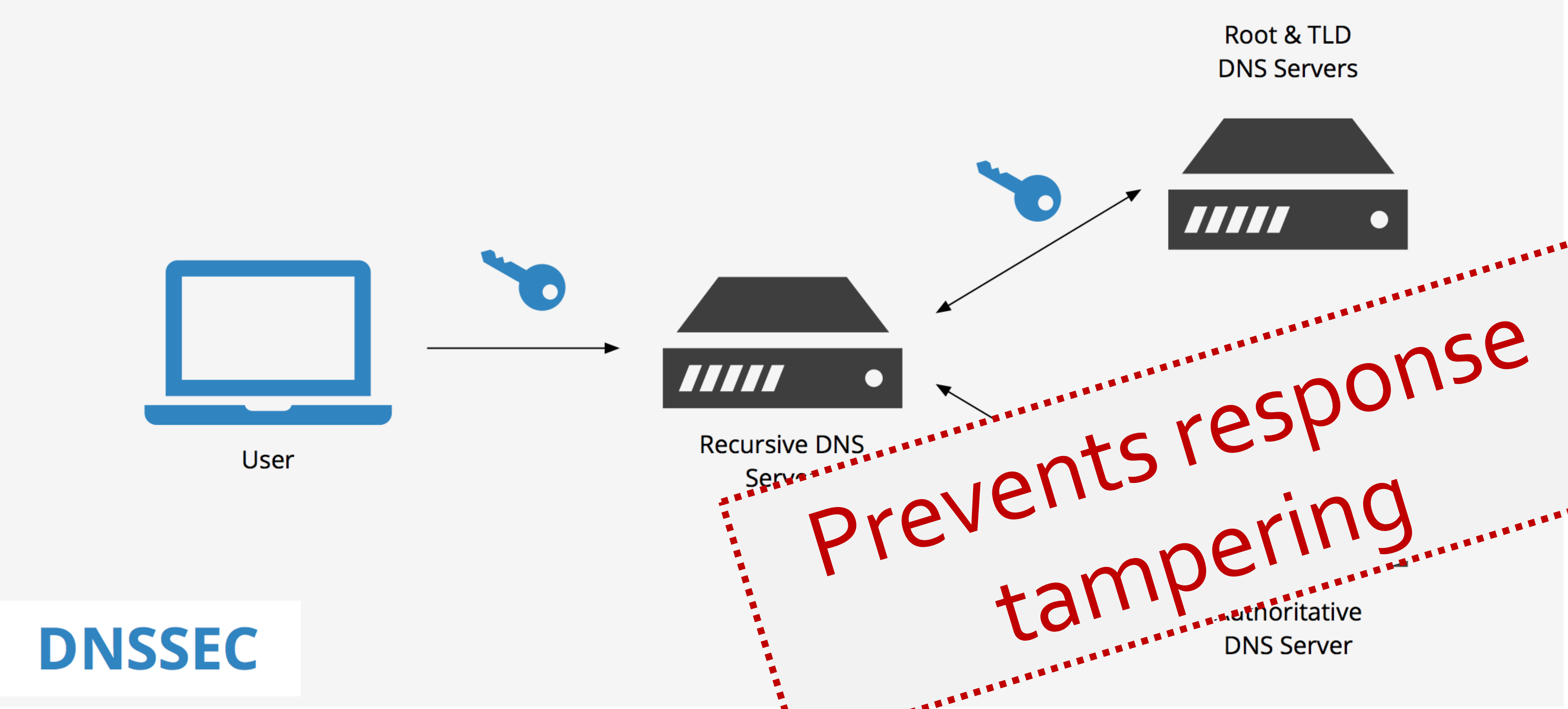
Berkeley Internet Domain Name

ALL BIND versions should be deprecated before 2009

How can I prevent this?

Solutions

- DNSSEC and validation at client-side



Prevents response tampering

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

Solutions

- Encrypted DNS

You
Recursive Server
TLS CONNECTION
//example.com
DNS
TLS CO

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

Thank you!

- Details in our Usenix Security'18 paper
  - Who Is Answering My Queries? Understanding and Characterizing Hidden Interception of the DNS Resolution Path
- UC Irvine author contact
  - Zhou Li (Assistant Professor)
  - zhou.li@uci.edu
  - https://faculty.sites.uci.edu/zhouli/
  - Looking for collaborations ☺