谁劫持了我的DNS：
全球域名解析路径劫持测量与分析

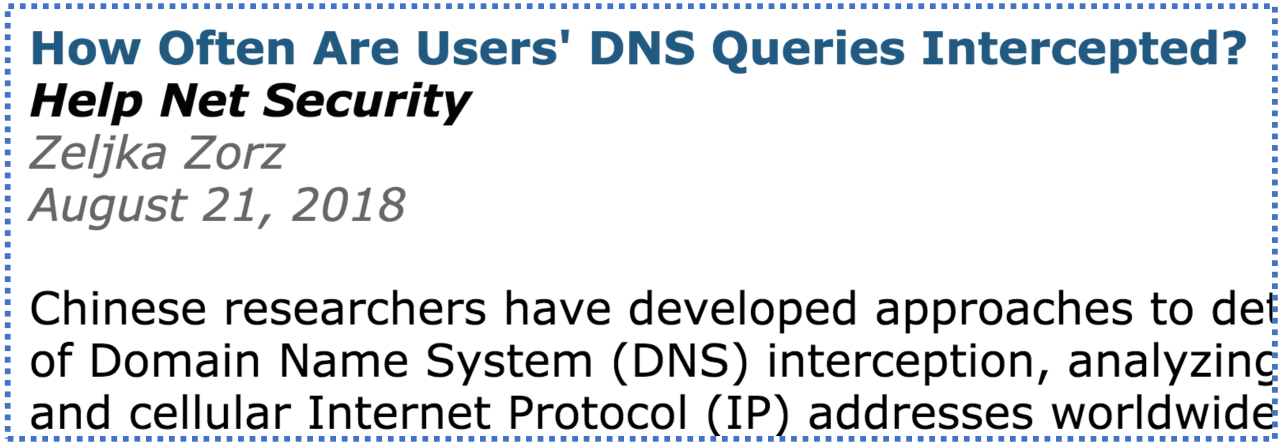
刘保君

清华大学 计算机系

媒体报道

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

Security

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

Uninvited middlemen may be messing with message

The Register

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

HackRead

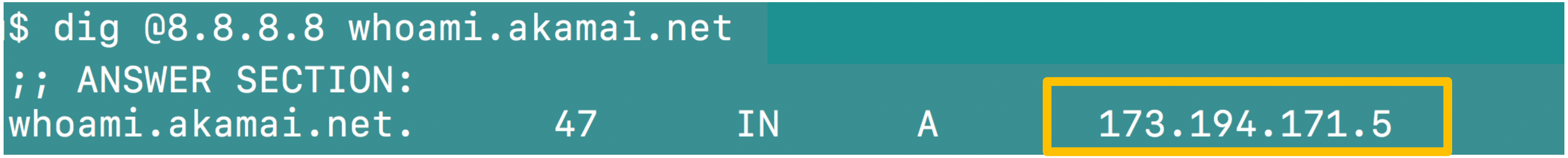
https://www.hackread.com/hackers-can-intercept-and-manipulate-dns-queries-researchers-warn/

Hackers can intercept and manipulate DNS queries, researchers warn

AUGUST 20TH, 2018 WAQAS SECURITY 0 COMMENTS

我的请求到哪去了？

- 向Google DNS发送查询请求
  - 通过查询诊断域名，查看实际使用的解析服务器地址
  - 客户端1：



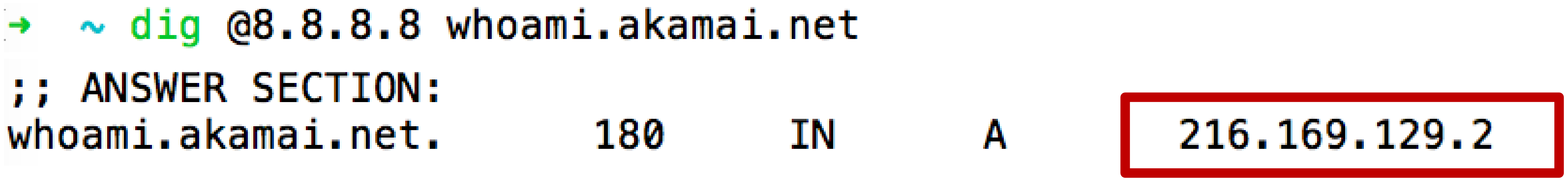
```
$ dig @8.8.8.8 whoami.akamai.net
;; ANSWER SECTION:
whoami.akamai.net.        47        IN        A        173.194.171.5
```

173.194.171.5: AS15169 Google LLC

正常

我的请求到哪去了？

- 向Google DNS发送查询请求
  - 通过查询诊断域名，查看实际使用的解析服务器地址
  - 客户端2：



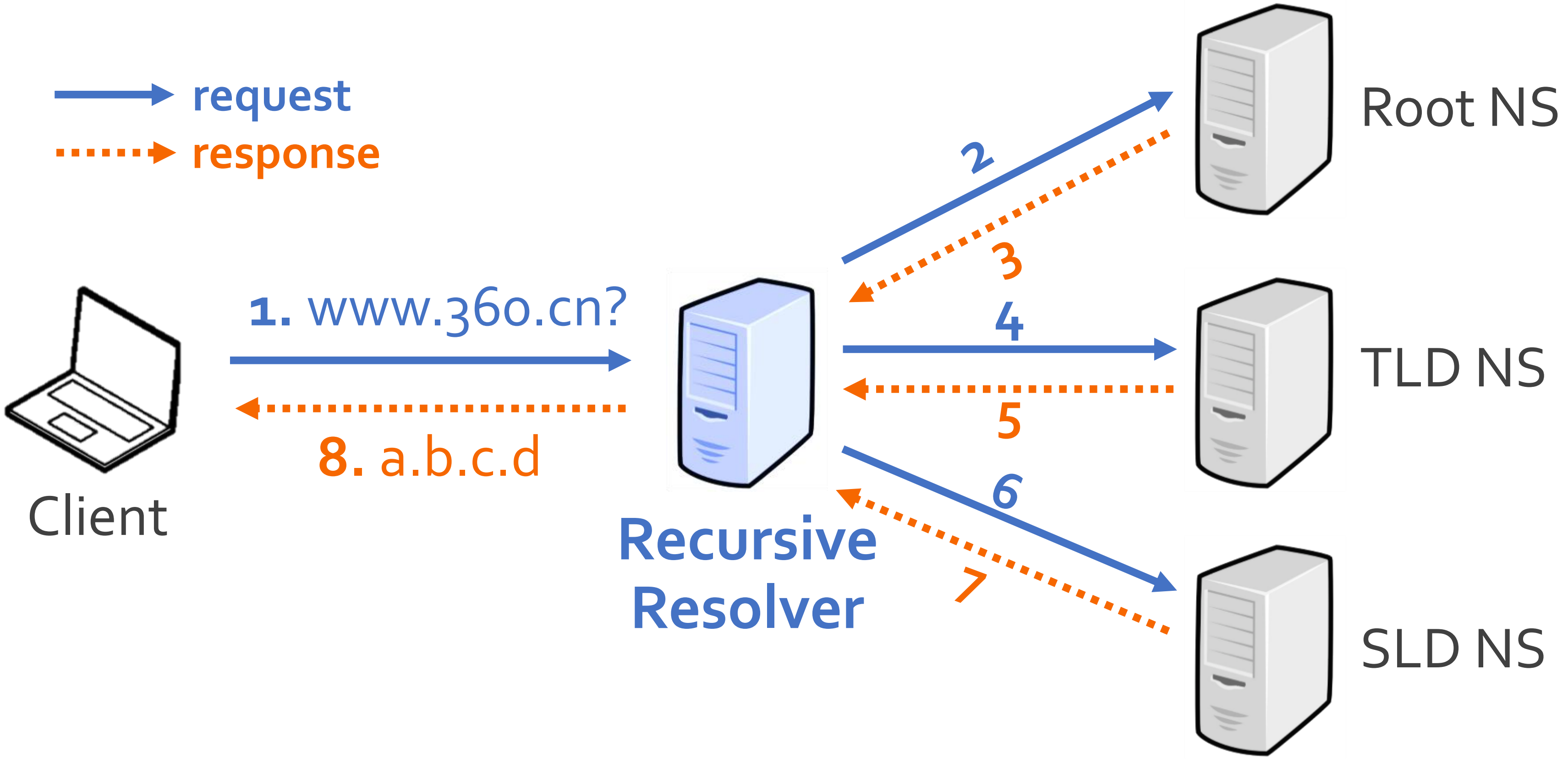
```
➜  ~ dig @8.8.8.8 whoami.akamai.net
;; ANSWER SECTION:
whoami.akamai.net.      180     IN      A       216.169.129.2
```

216.169.129.2: AS22781 Strong Technology, LLC

不是Google的地址，异常

DNS解析

- 域名解析：互联网活动的开始
  - – 通常由解析服务器（resolver）完成



DNS解析

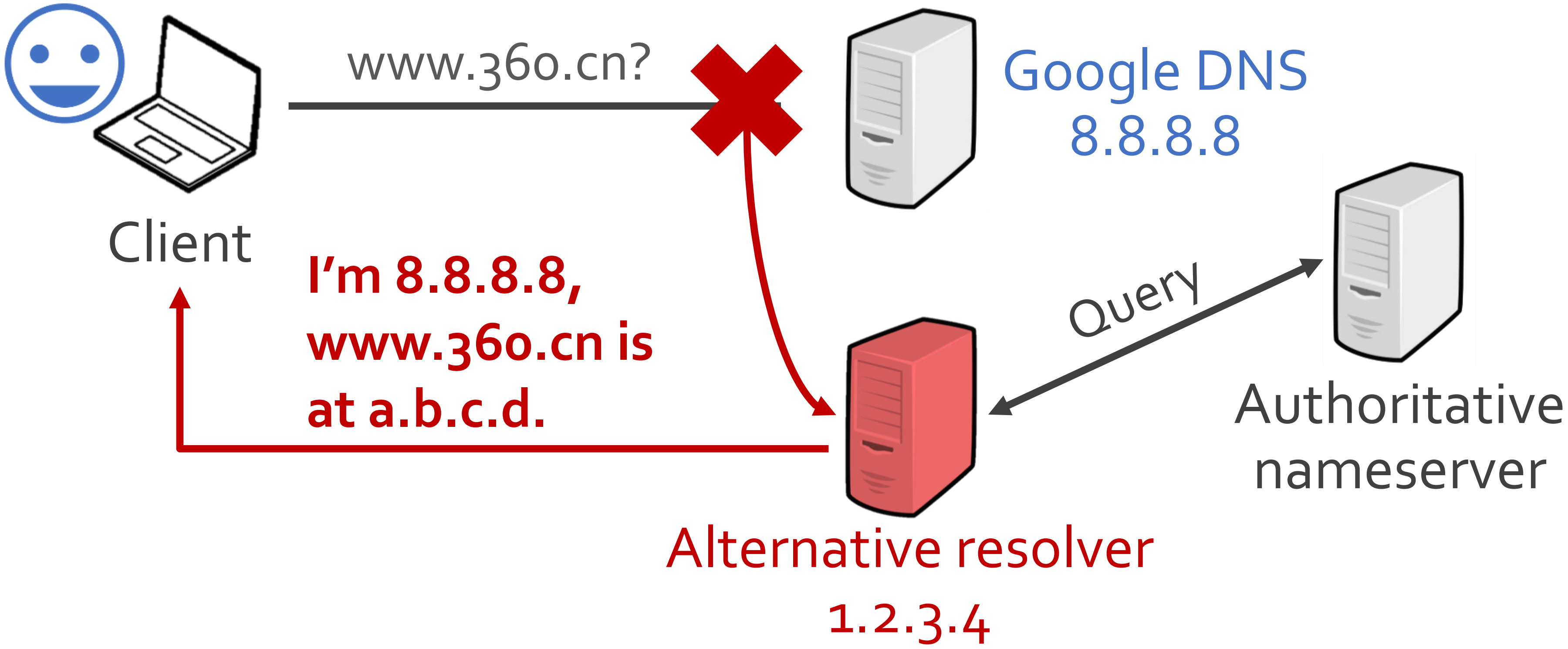
- 公共DNS服务
  - 良好性能（ e.g., 使用负载均衡 ）
  - 安全性（ e.g., 支持DNSSEC ）
  - 支持DNS扩展功能（ e.g., EDNS Client Subnet ）

Google Public DNS

OpenDNS

CLOUDFLARE 1.1.1.1 DNS

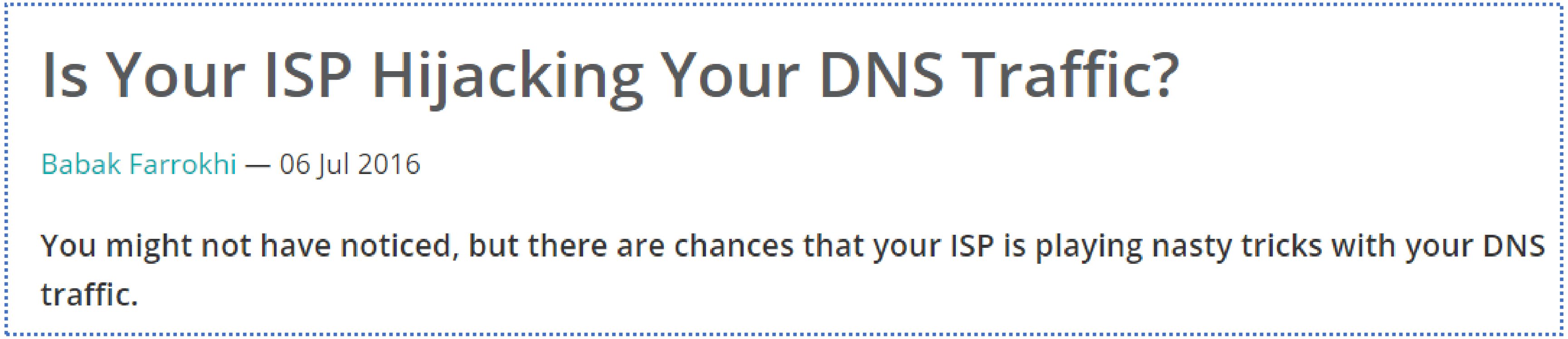
域名解析路径劫持



劫持解析路径，并伪装成指定的DNS应答

可能的劫持者

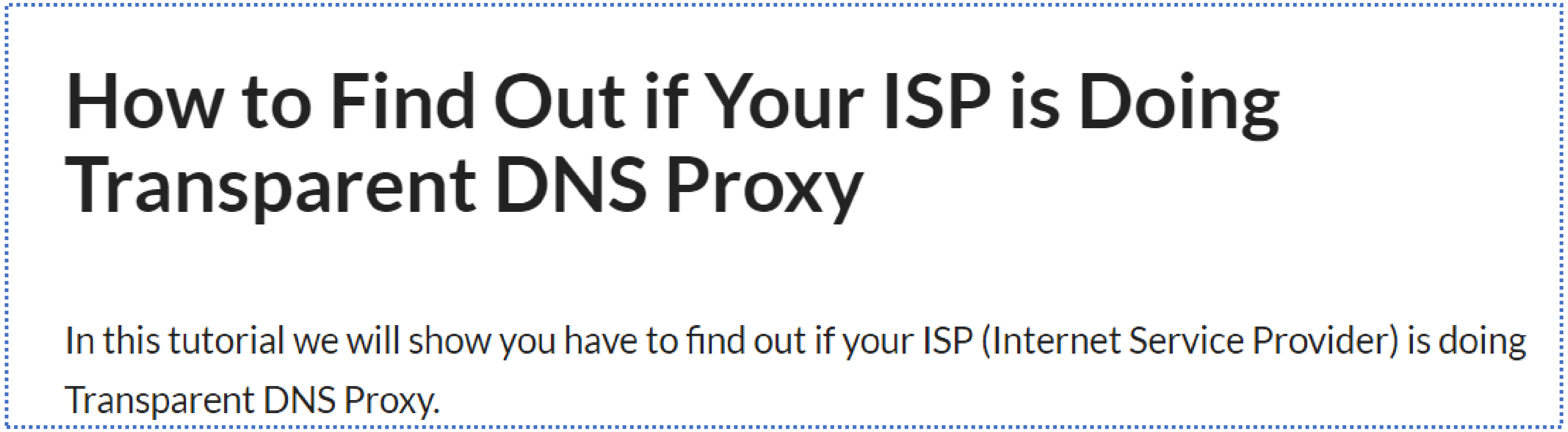
网络服务提供商



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

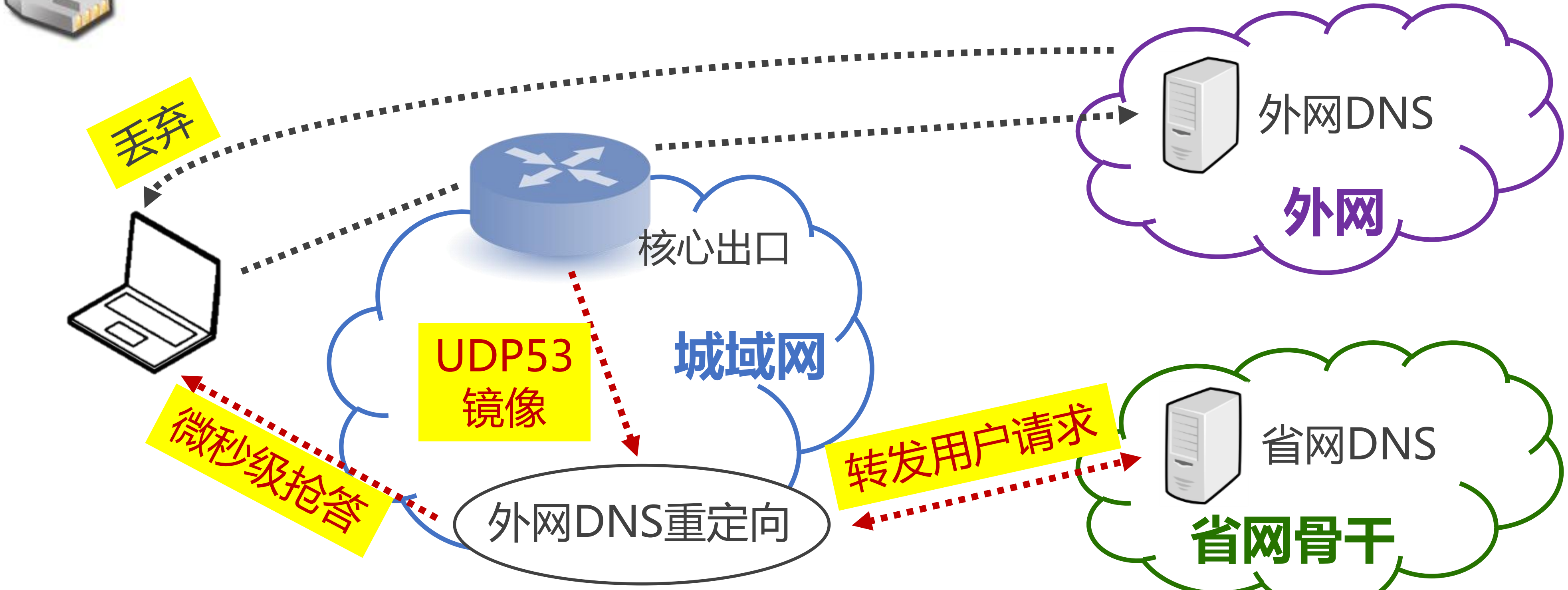
In this tutorial we will show you have to find out if your ISP (Internet Service Provider) is doing Transparent DNS Proxy.

* 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/

可能的劫持者

网络服务提供商

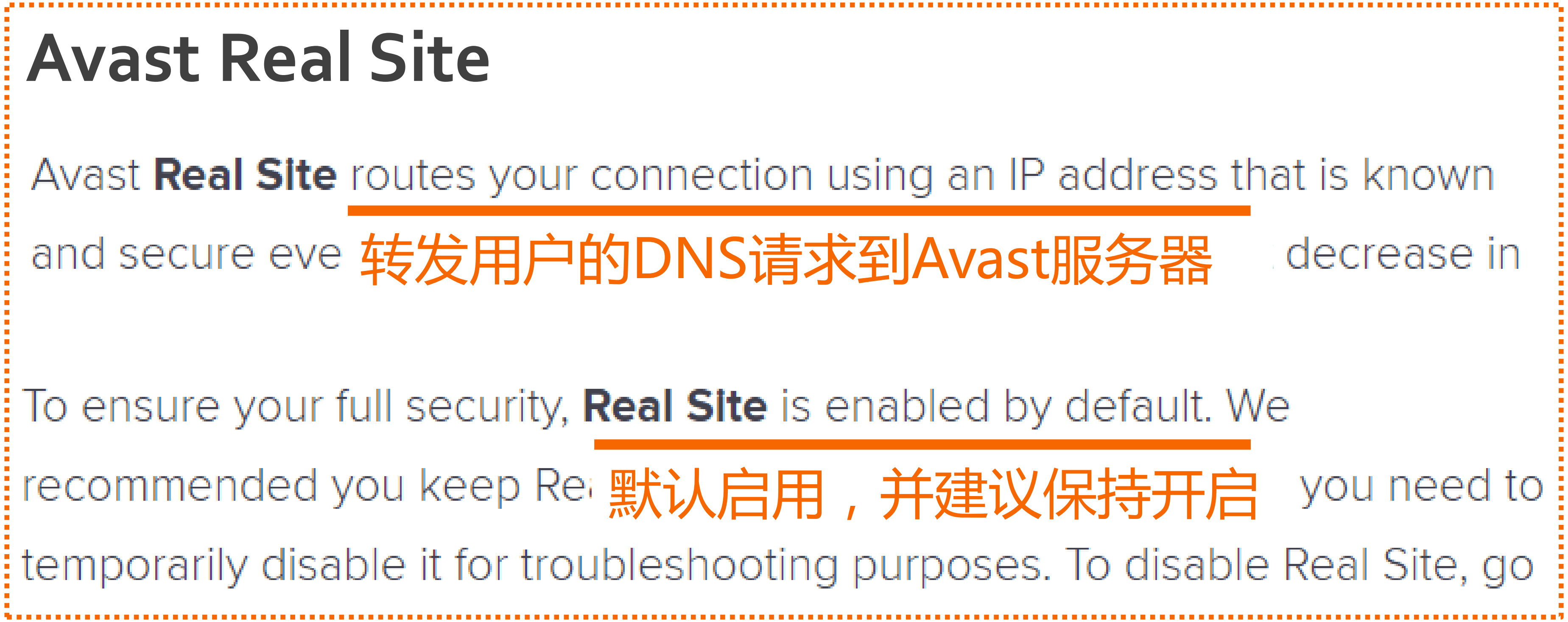
巫俊峰, 沈瀚. 基于旁路抢答机制的异网DNS管控实践. 电信技术[J], 2016



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

可能的劫持者

恶意软件 / 反病毒软件



Avast Real Site

Avast **Real Site** routes your connection using an IP address that is known

and secure eve 转发用户的DNS请求到Avast服务器 decrease in

To ensure your full security, **Real Site** is enabled by default. We

recommended you keep Re 默认启用，并建议保持开启 you need to

temporarily disable it for troubleshooting purposes. To disable Real Site, go

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

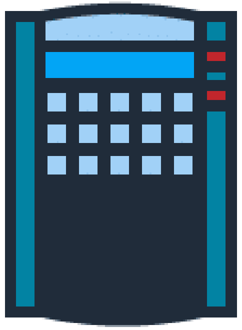
可能的劫持者

网络服务提供商

内容审查 / 防火墙

恶意软件 / 反病毒软件
(E.g., Avast anti-virus)

企业代理设备
(E.g., Cisco Umbrella intelligent proxy)



问题一：

解析路径劫持现象，有多普遍？

问题二：

解析路径劫持，都有什么特征？

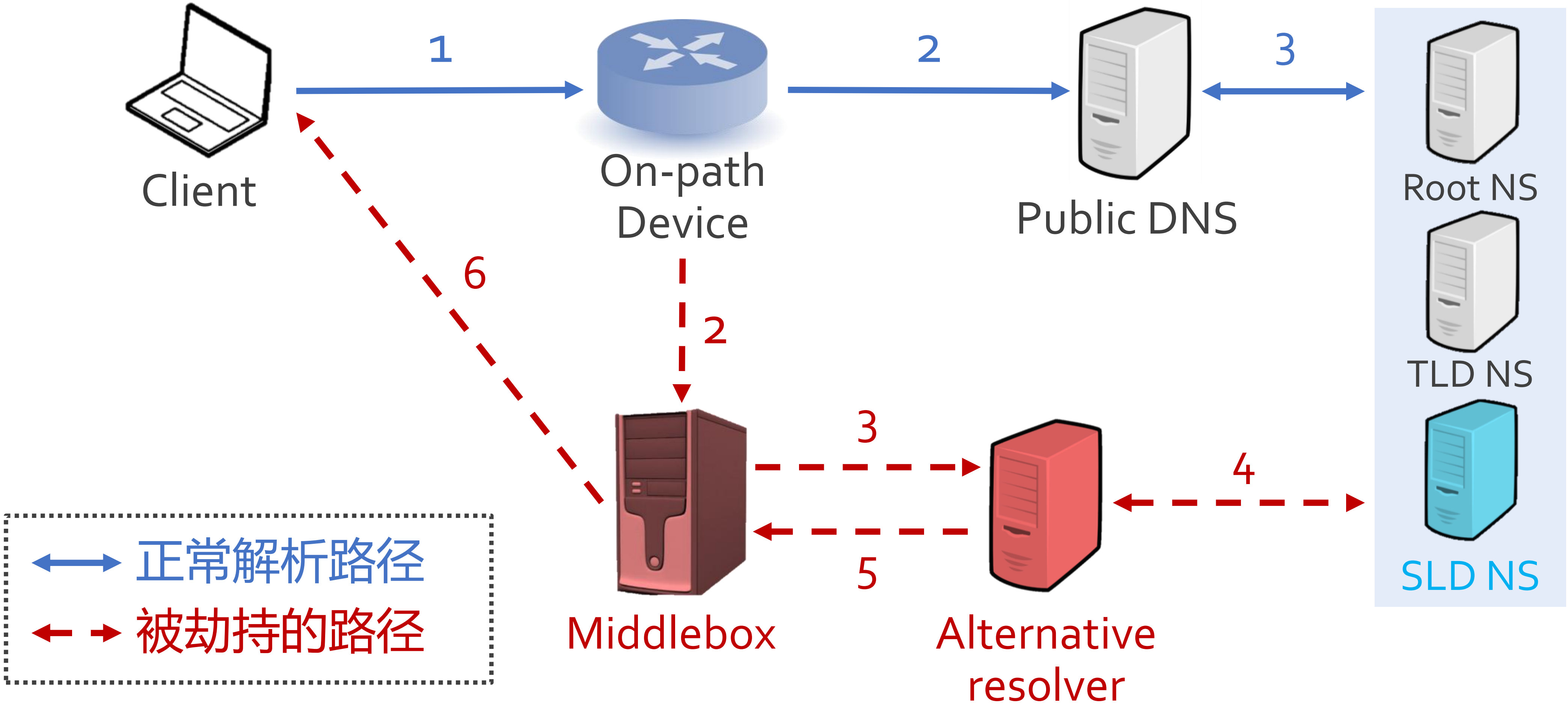
Motivation

Threat Model

Methodology

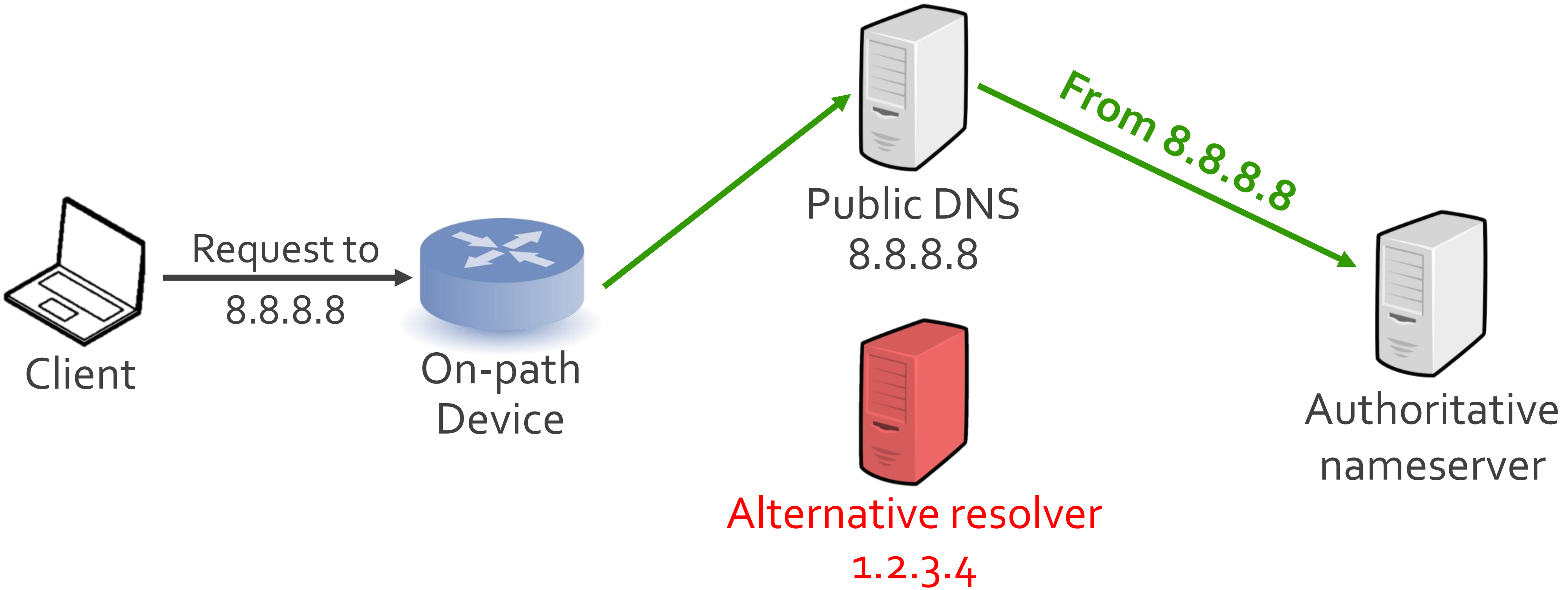
Analysis

威胁模型


1
2
3
Client
On-path Device
Public DNS
Root NS
TLD NS
SLD NS
6
2
3
4
5
Middlebox
Alternative resolver
正常解析路径
被劫持的路径

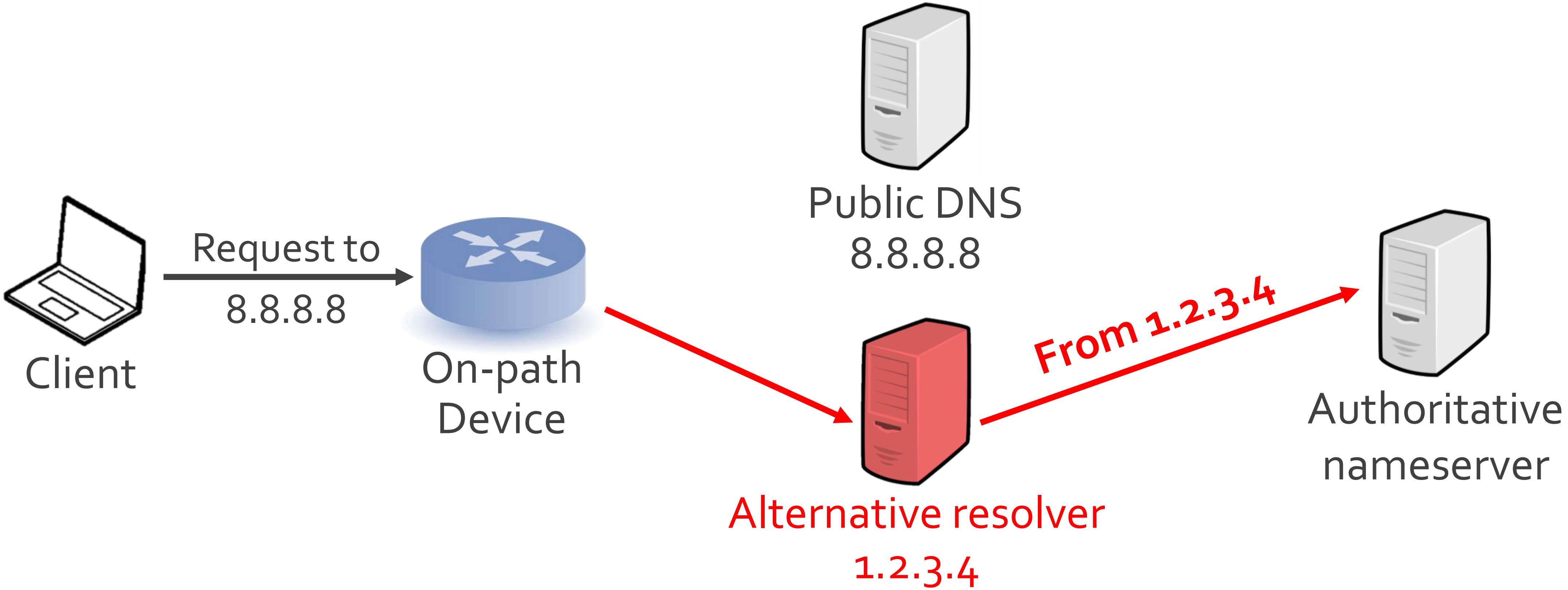
威胁模型

- 请求路径分类
  - **[1] Normal resolution（正常解析）**



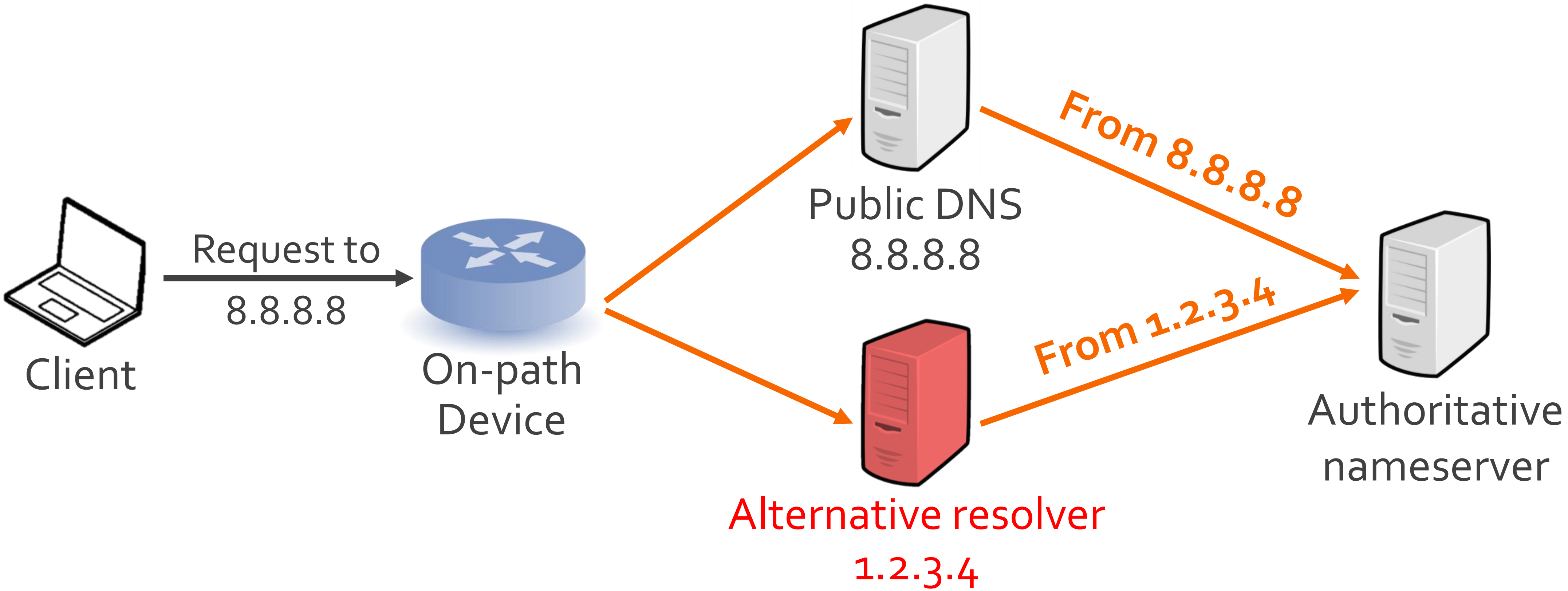
威胁模型

- 请求路径分类
  - **[2] Request redirection（请求转发）**



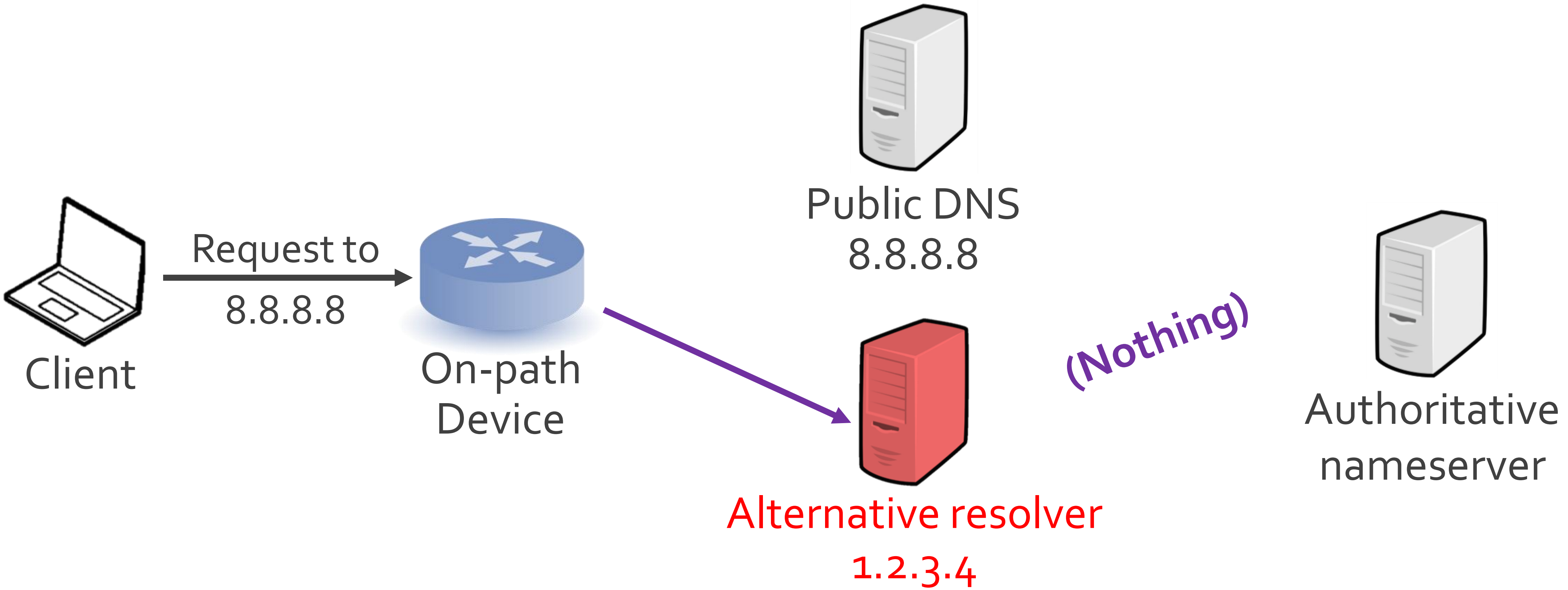
威胁模型

- 请求路径分类
  - **[3] Request replication（请求复制）**



威胁模型

- 请求路径分类
  - **[4] Direct responding（直接应答）**



Motivation

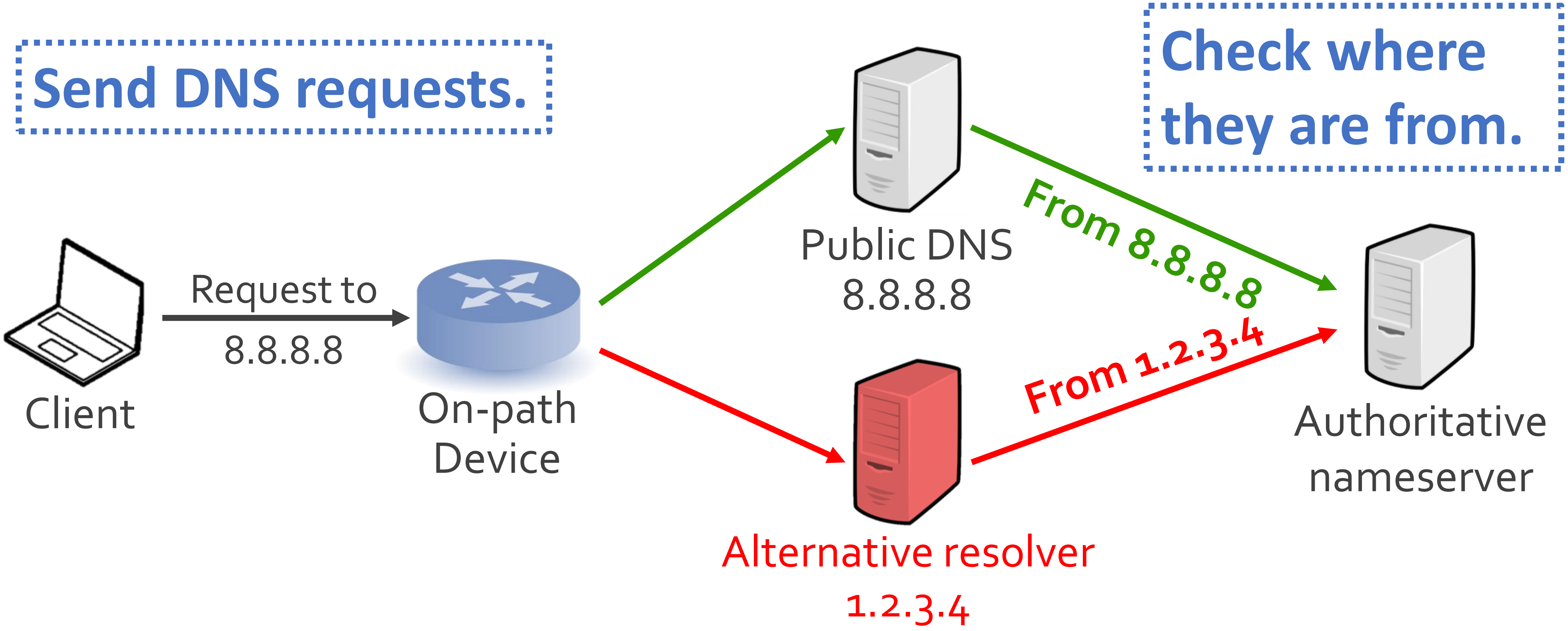
Threat Model

Methodology

Analysis

怎样检测路径劫持？

- 方法概览



获取观测点

- 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**

发送DNS请求

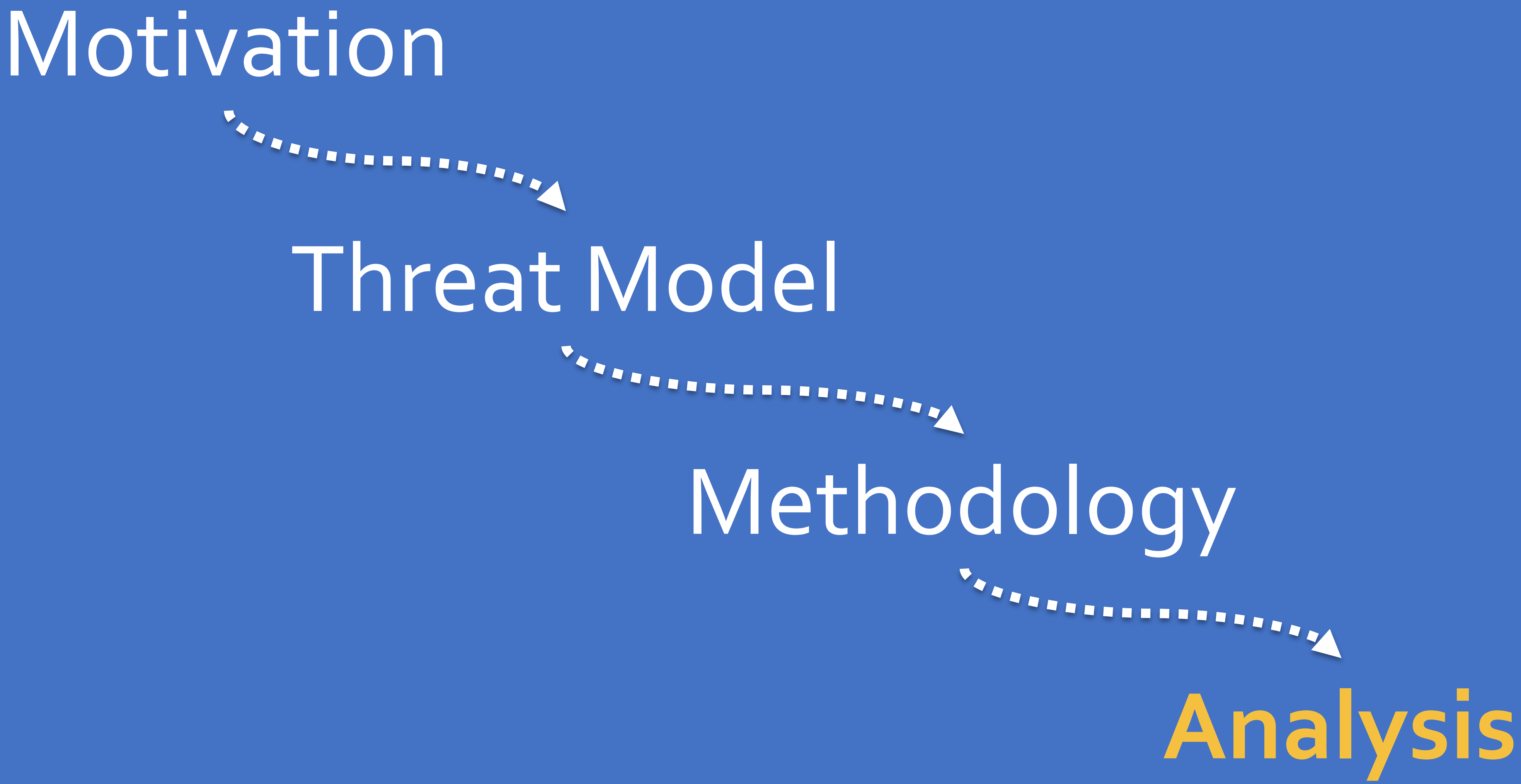
- Requirements
  - **Diverse**: triggering interception behaviors
  - **Controlled**: allowing fine-grained analysis

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]

数据集

- 来自多个观测点的DNS请求
  - **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

劫持规模有多大？

劫持规模

- 存在劫持流量的自治系统（AS）

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

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

劫持规模

- 被劫持请求占比
  - 国内测量结果，UDP & TCP

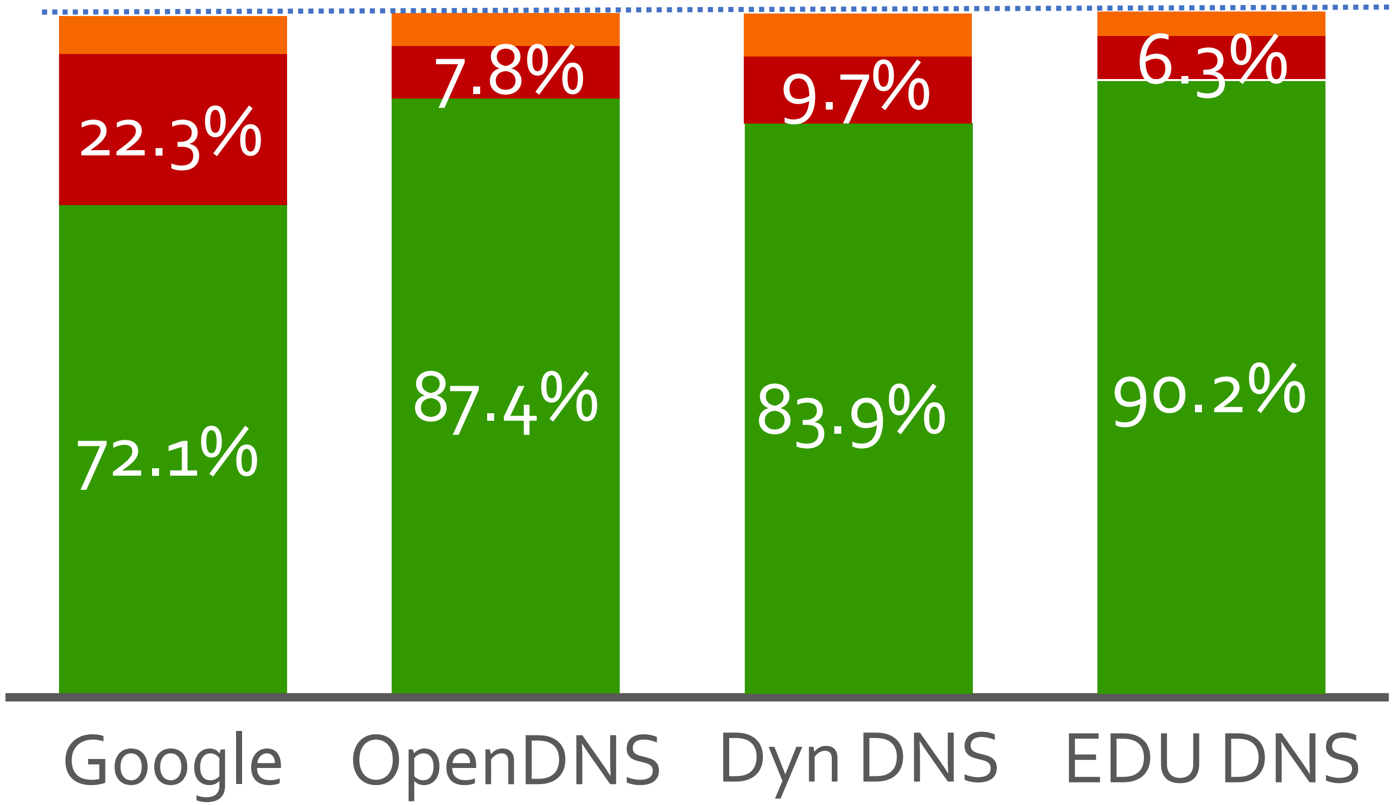
Google Public DNS	27.9% 7.3%	OpenDNS	12.6% 0.9%
ORACLE + Dyn	16.1% 2.3%	EDU DNS（自建）	9.8% 1.1%

去往流行公共DNS的流量，更容易被劫持

怎样劫持的？

路径劫持特征

- 分路径种类来看
  - – Normal resolution Request redirection Request replication



直接应答的数量很少

请求转发的比例 > 请求复制的比例

路径劫持特征

- 分AS来看
  - （以下AS按照收集请求的总数排序，数值为占请求总数比例）

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)

AS内部劫持特征较为复杂；不同网络之间有差异

响应被篡改了吗？

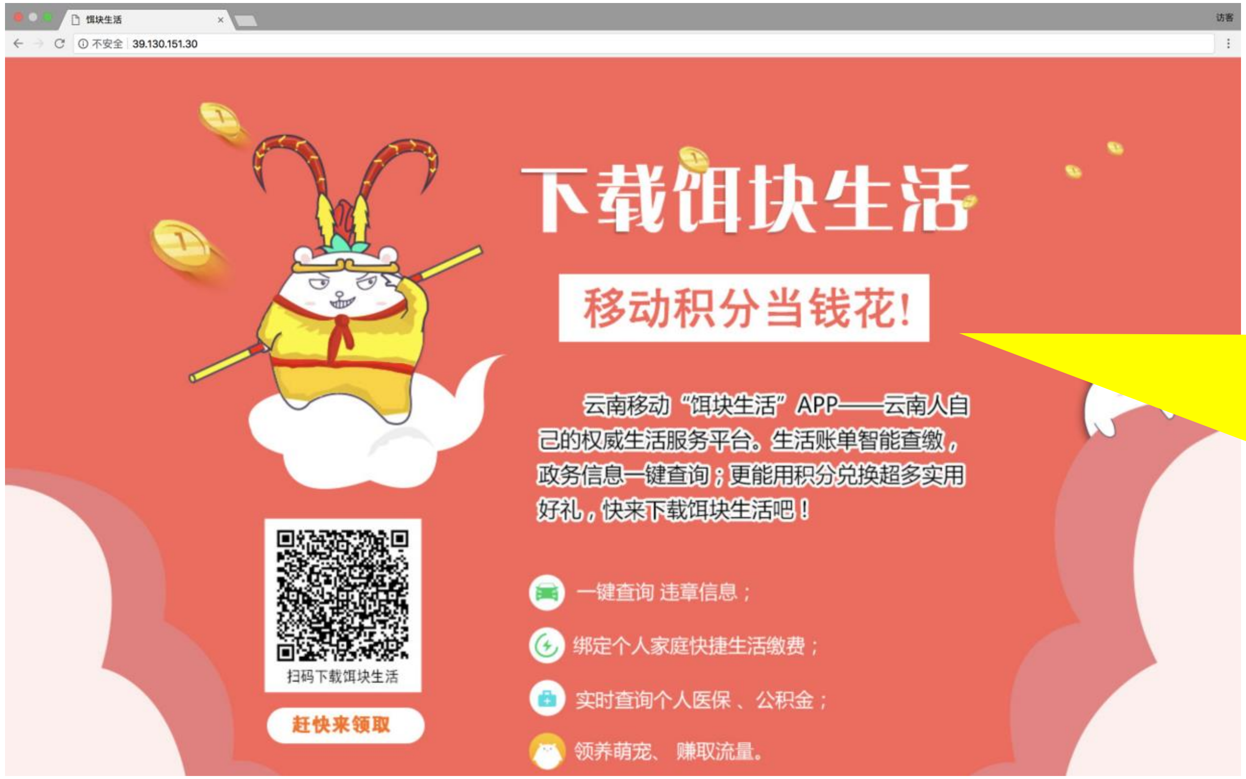
对DNS响应的篡改

- 检查返回的响应是否正确
  - 大部分的响应没有被改动
  - 但也存在少量被篡改的响应：

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

对DNS响应的篡改

- 修改案例：流量变现



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**.

有什么安全威胁？

安全威胁

“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/

安全威胁

- 道德和隐私问题
  - 用户可能并不知道自己的请求被劫持了
- 解析服务器的安全性
  - 检测了205个开放的解析服务器

DNSSEC

Only 43% resolvers support DNSSEC

BIND

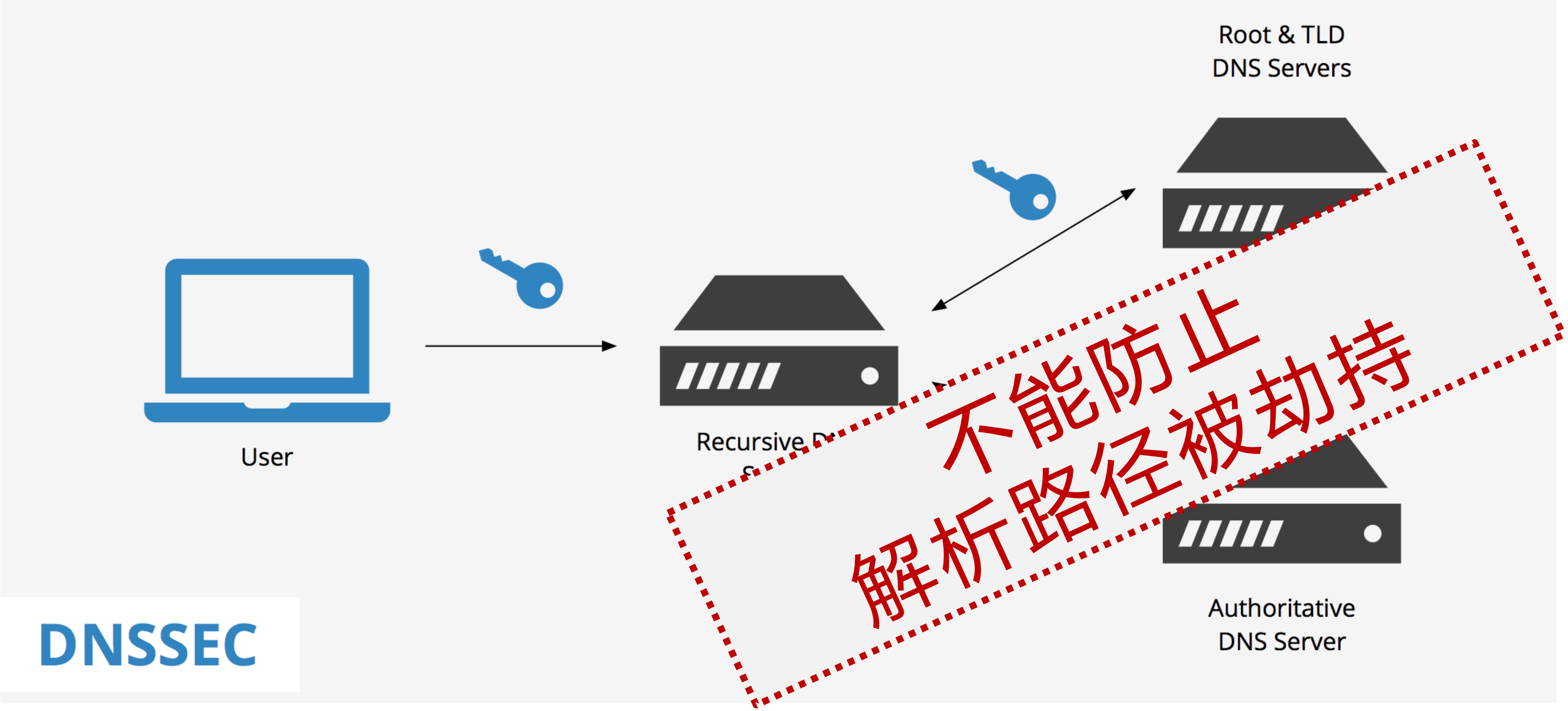
Berkeley Internet Domain Name

ALL BIND versions should be deprecated before 2009

有没有解决办法？

解决方案

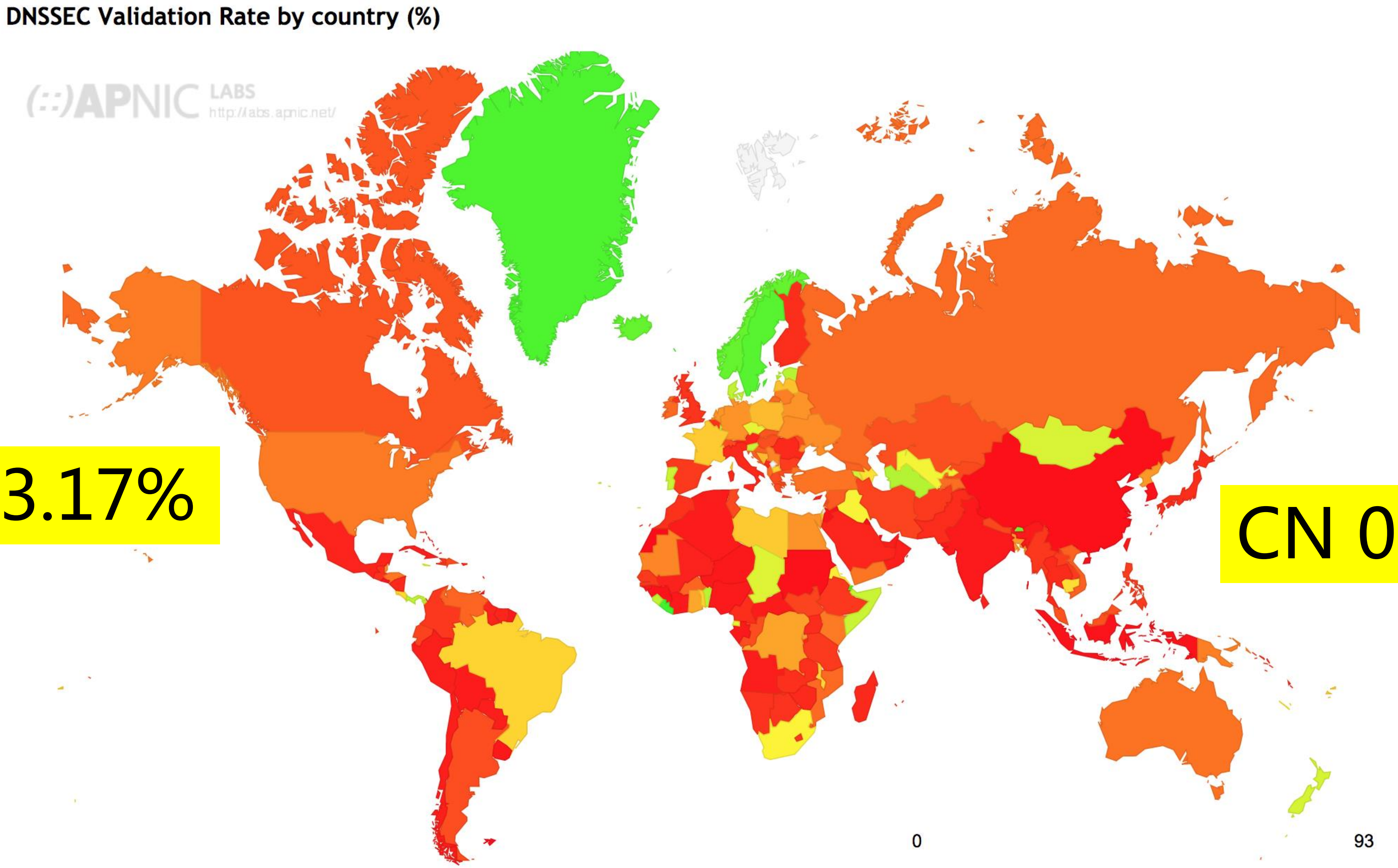
- DNSSEC：能做到吗？



不能防止
解析路径被劫持

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

全球DNSSEC 验证的比例

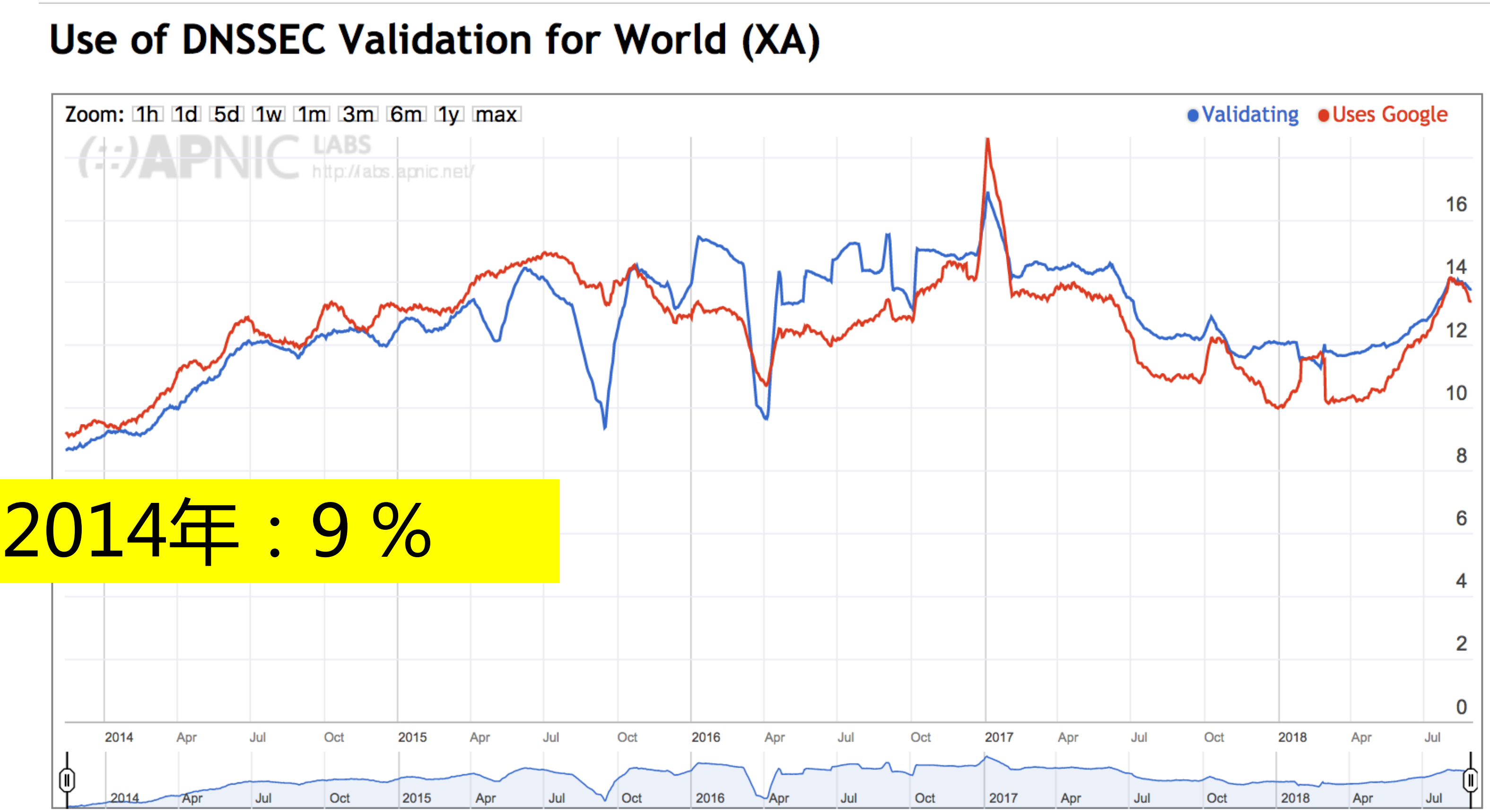

DNSSEC Validation Rate by country (%)
(::)APNIC LABS http://labs.apnic.net/
0
93

US 23.17%

CN 0.93%

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

世界使用DNSSEC验证的用户比例



🟦 支持DNSSEC验证的用户

🟥 使用Google DNS 的用户

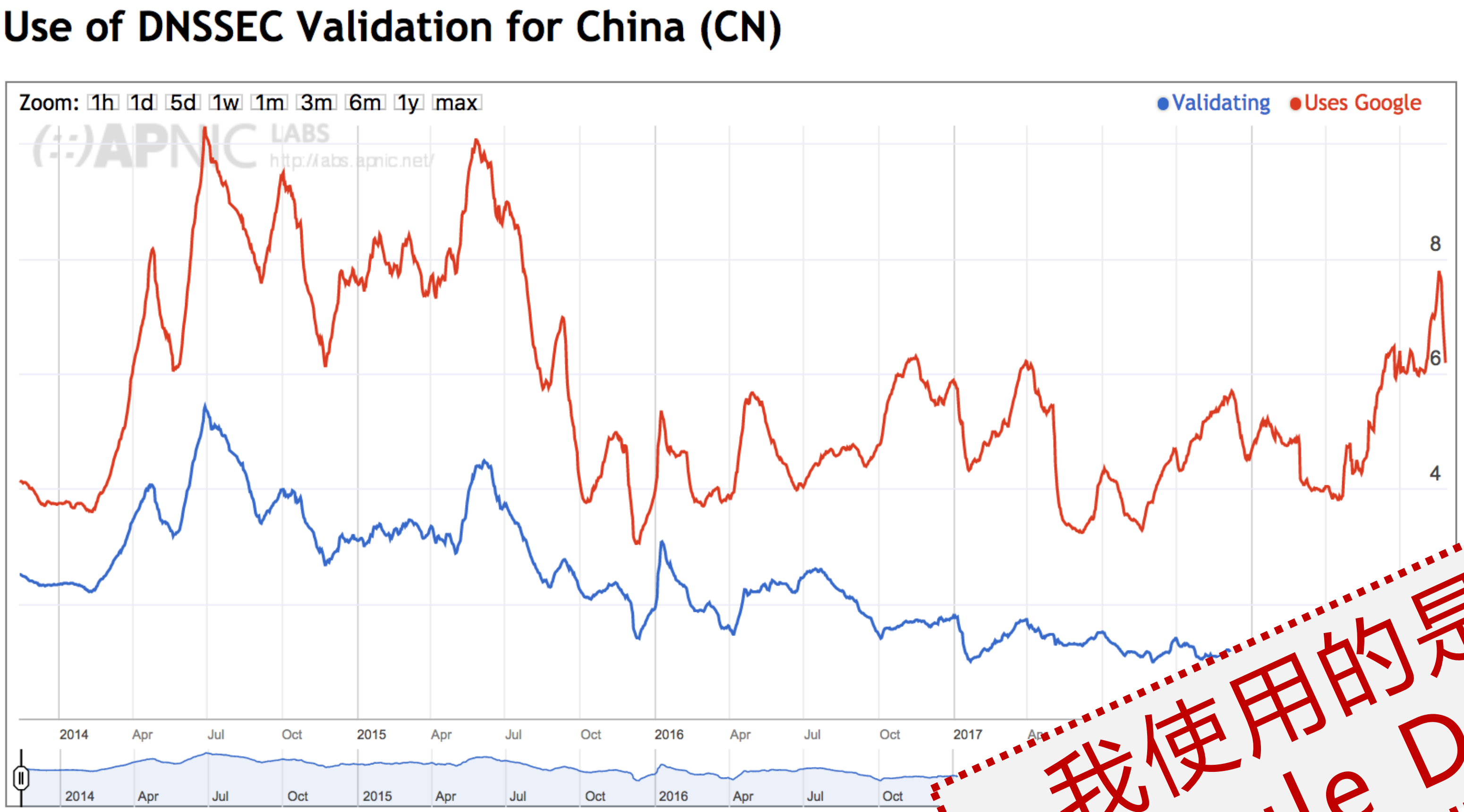
2018年8月：全球14%

2014年：9 %

Google 的公共DNS2013年开始支持DNSSEC验证

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

中国用户使用DNSSEC验证比例


Use of DNSSEC Validation for China (CN)

支持DNSSEC验证的用户

使用Google DNS 的用户

我使用的是个假的Google DNS吧！！

中国：0.9%

为什么使用Google的比例比DNSSEC验证的比例还高？

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

解决方案

- DNS加密

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

流量经过加密
可验证解析服务器身份

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

总结

- 域名解析路径劫持
  - 系统性的研究和测量，梳理不同的劫持方式和劫持者
- 主要发现
  - 在全球259个AS中发现了被劫持的DNS流量
  - 国内发往Google Public DNS的流量有约28%被劫持
  - 存在安全隐患
- 解决方案
  - 加密DNS和解析服务器认证；
  - http://whatismydnsresolver.com/

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