网络空间中的信任与冲突

段海新

清华大学网络空间安全论坛, 2016

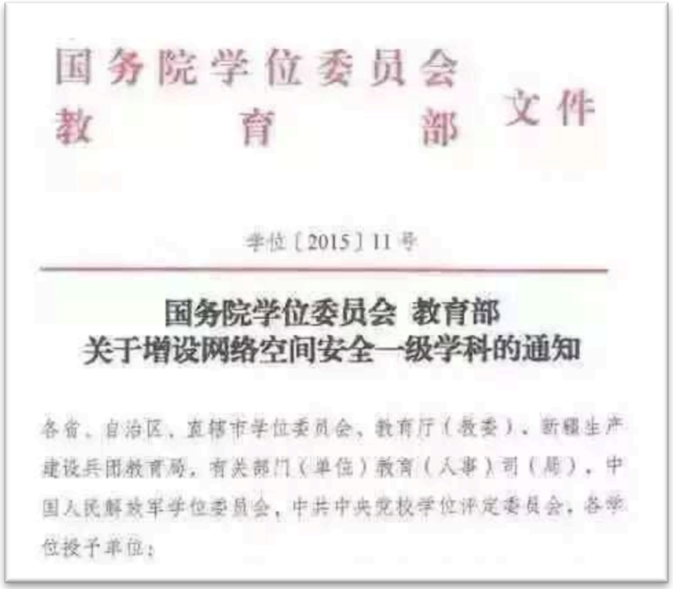
Outline

- Trust models and trust anchors
- In Routing, We Trust…
- In DNS, We Trust …
- In Web PKI, We Trust

网络空间（Cyberspace）

- 通过互联网和计算机进行通信、控制和信息共享的虚拟空间(oxford dictionary)
- 网络空间里没有明确的、固定的边界，没有集中的控制权威

--《网络空间安全一级学科论证报告》，2015年5月



国务院学位委员会
教　　育　　部　文件

学位〔2015〕11号

国务院学位委员会 教育部
关于增设网络空间安全一级学科的通知

各省、自治区、直辖市学位委员会、教育厅（教委），新疆生产建设兵团教育局，有关部门（单位）教育（人事）司（局），中国人民解放军学位委员会，中共中央党校学位评定委员会，各学位授予单位：

信任（Trust）

- 相信某人（组织）或某物：
  - 真实，可靠，不撒谎
  - 有能力（Ability）或强度（Strength）

Oxford Dictionary: Firm belief in the reliability, truth, ability, or strength of someone or something

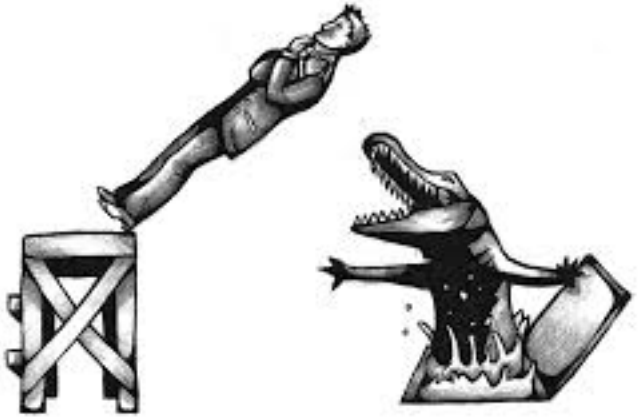
Trust Fall

Trusted in a closed community

Trust in an open world, cyberspace

冷漠

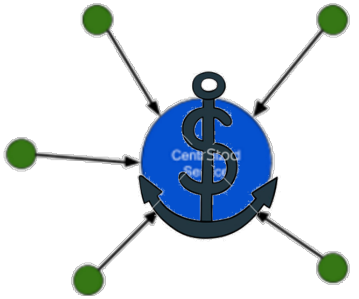
误解



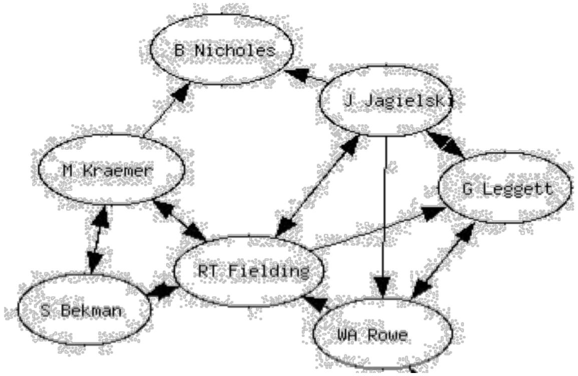
谋利，有意攻击

Trust models or policies

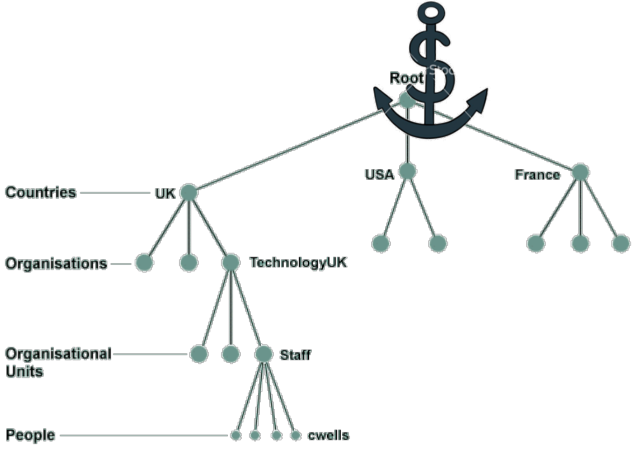
Centralized (e.g. Kerberos)



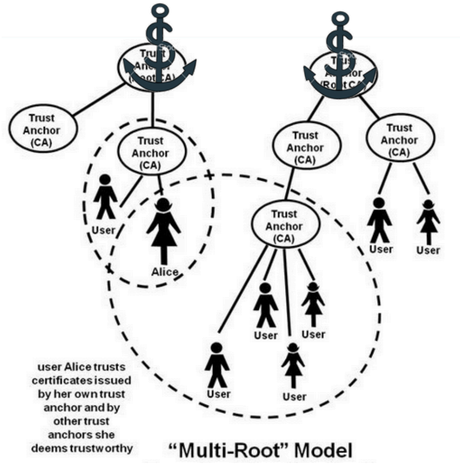
Web of Trust (e.g. PGP, BGP)



Hierarchy and delegation (e.g. DNS, X500)

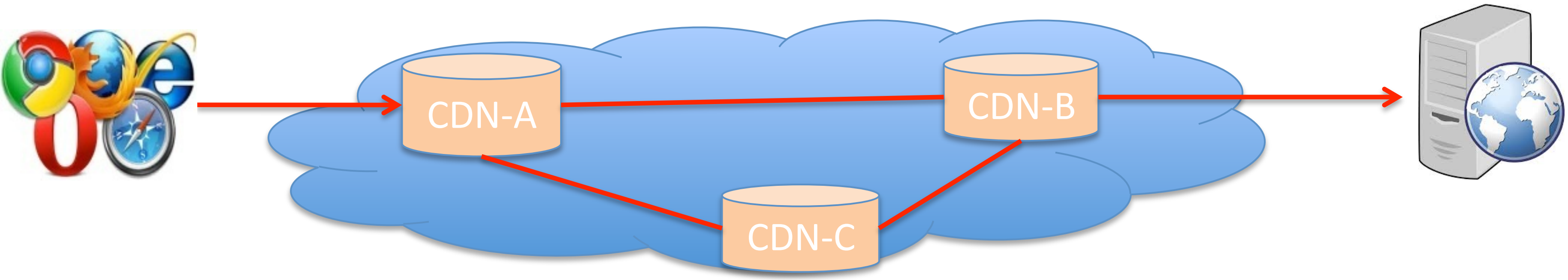


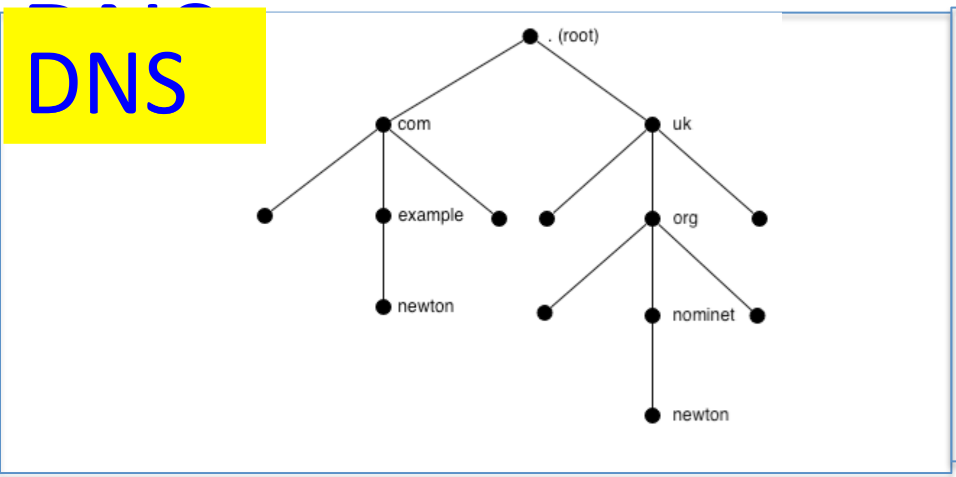
Forest(e.g. CA)

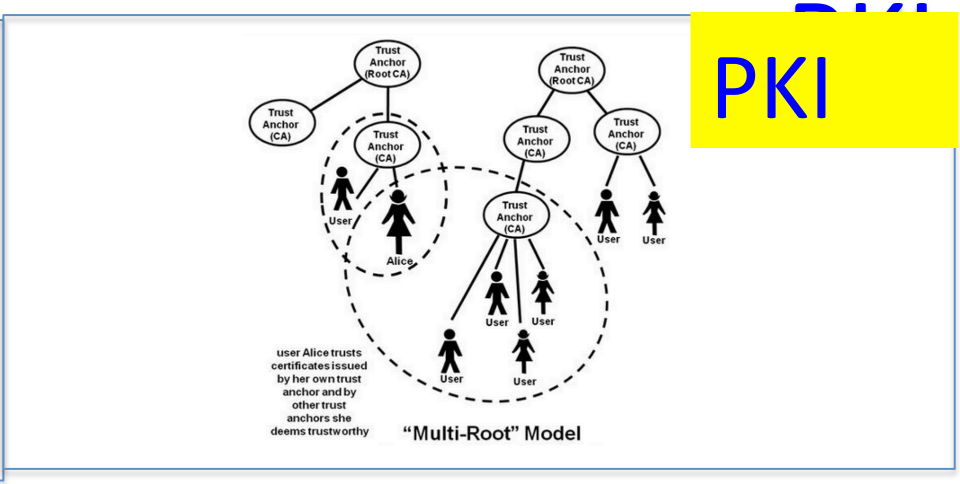


Trust on First Use, e.g. SSH, DNS/Cert Pinning

互联网基础设施的信任模型

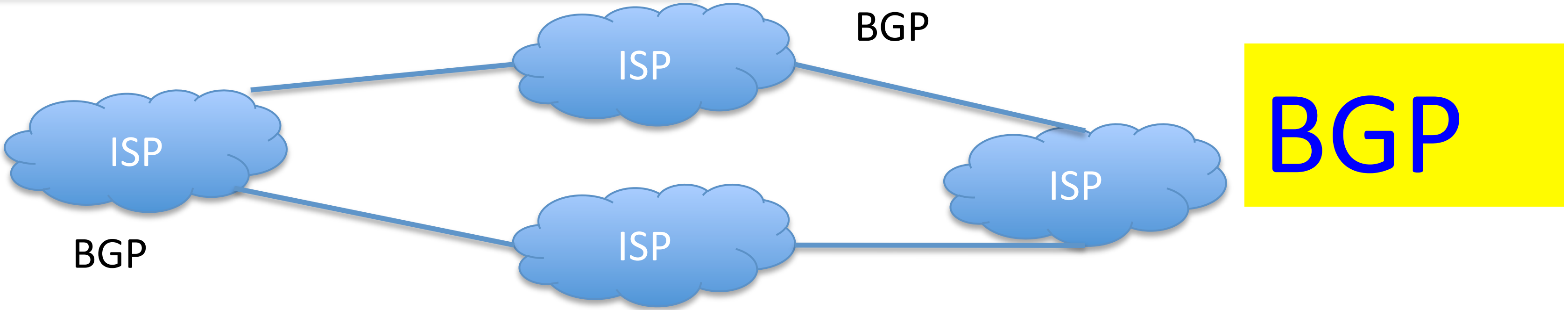






user Alice trusts certificates issued by her own trust anchor and by other trust anchors she deems trustworthy

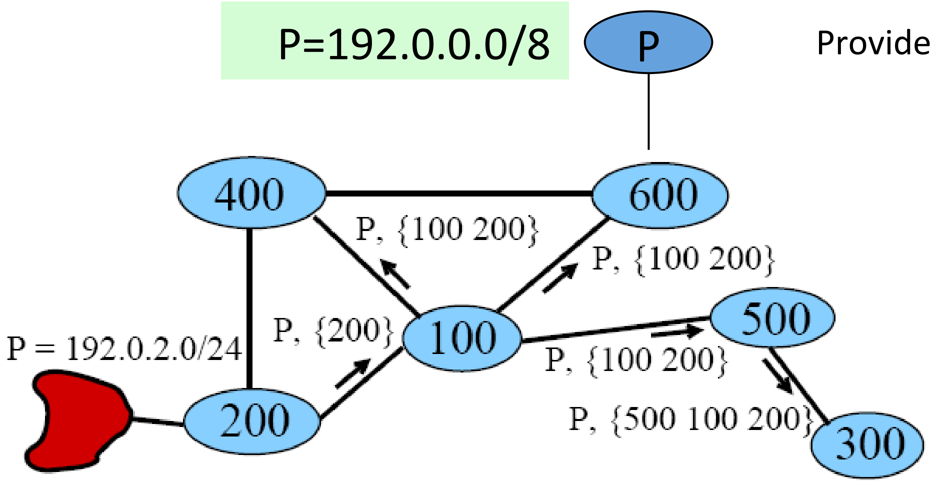
“Multi-Root” Model



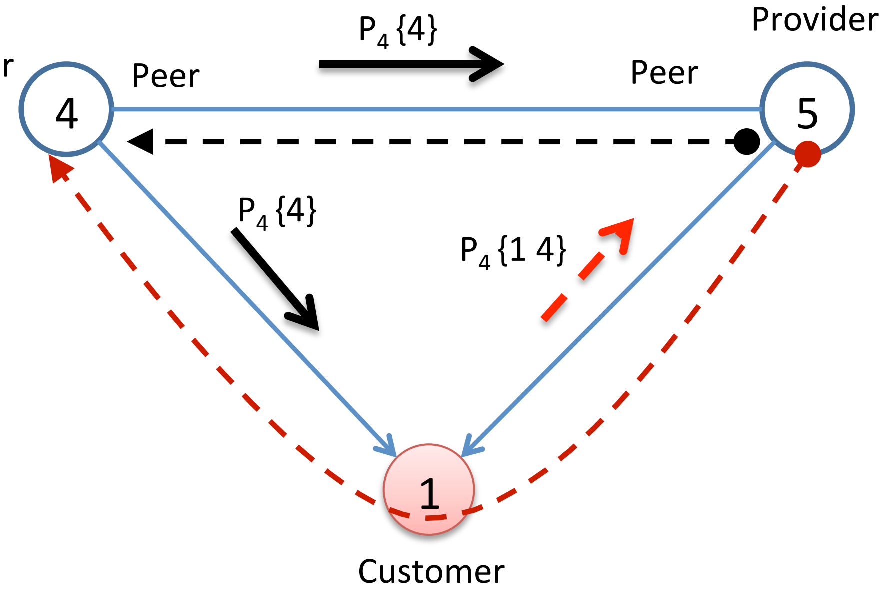
In Routing(without anchor), We Trust

Prefix hijack and route leak

- Malicious AS announces a more specific prefix

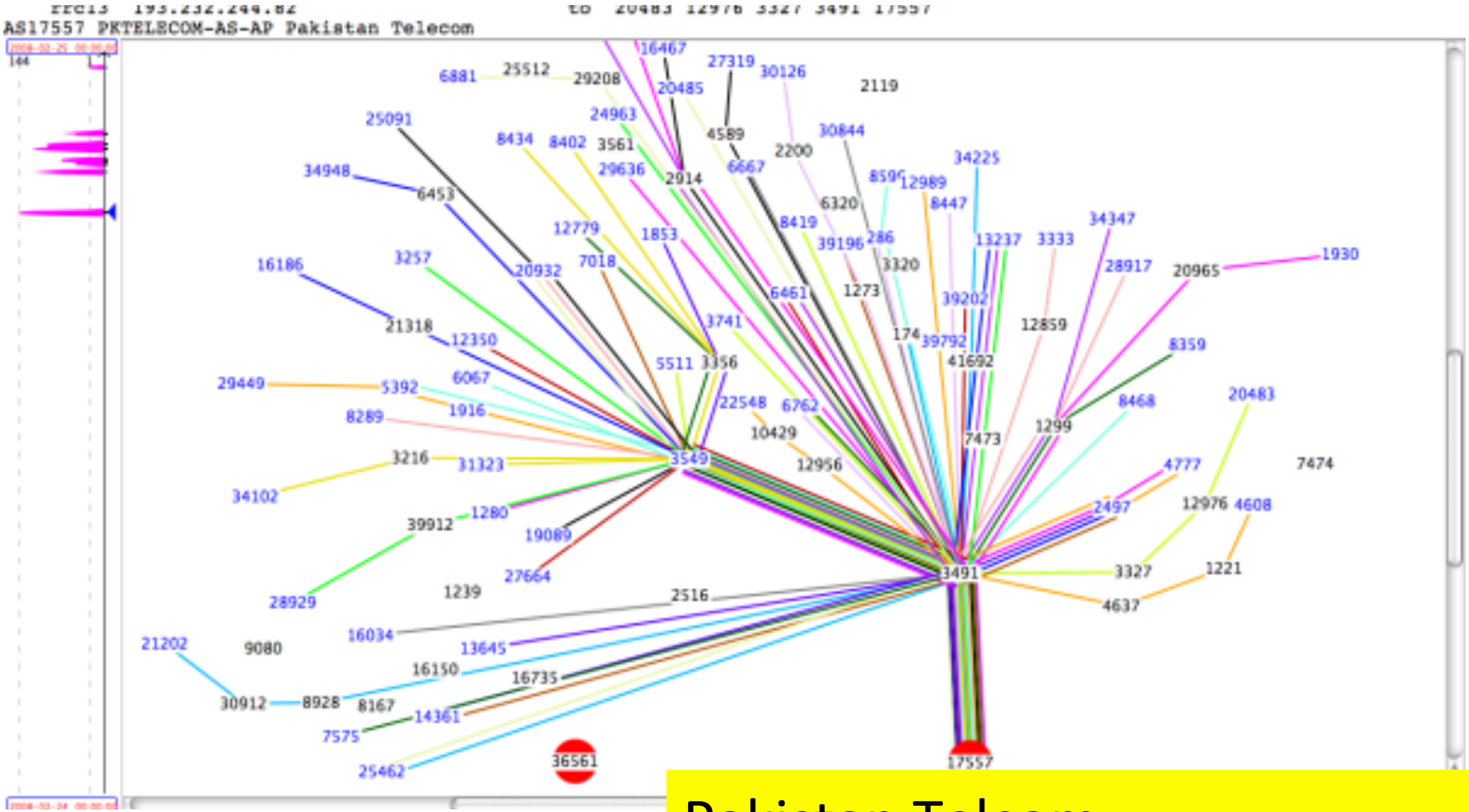


- Customer leaks provider 4’s route to provider 5, which causes a MITM



Song Li, Haixin Duan, Zhiliang Wang, and Xing Li, Route Leaks Identification by Detecting Routing Loops, SecureComm 2015

YouTube Hijacking by Pakistan Telecom, 2008



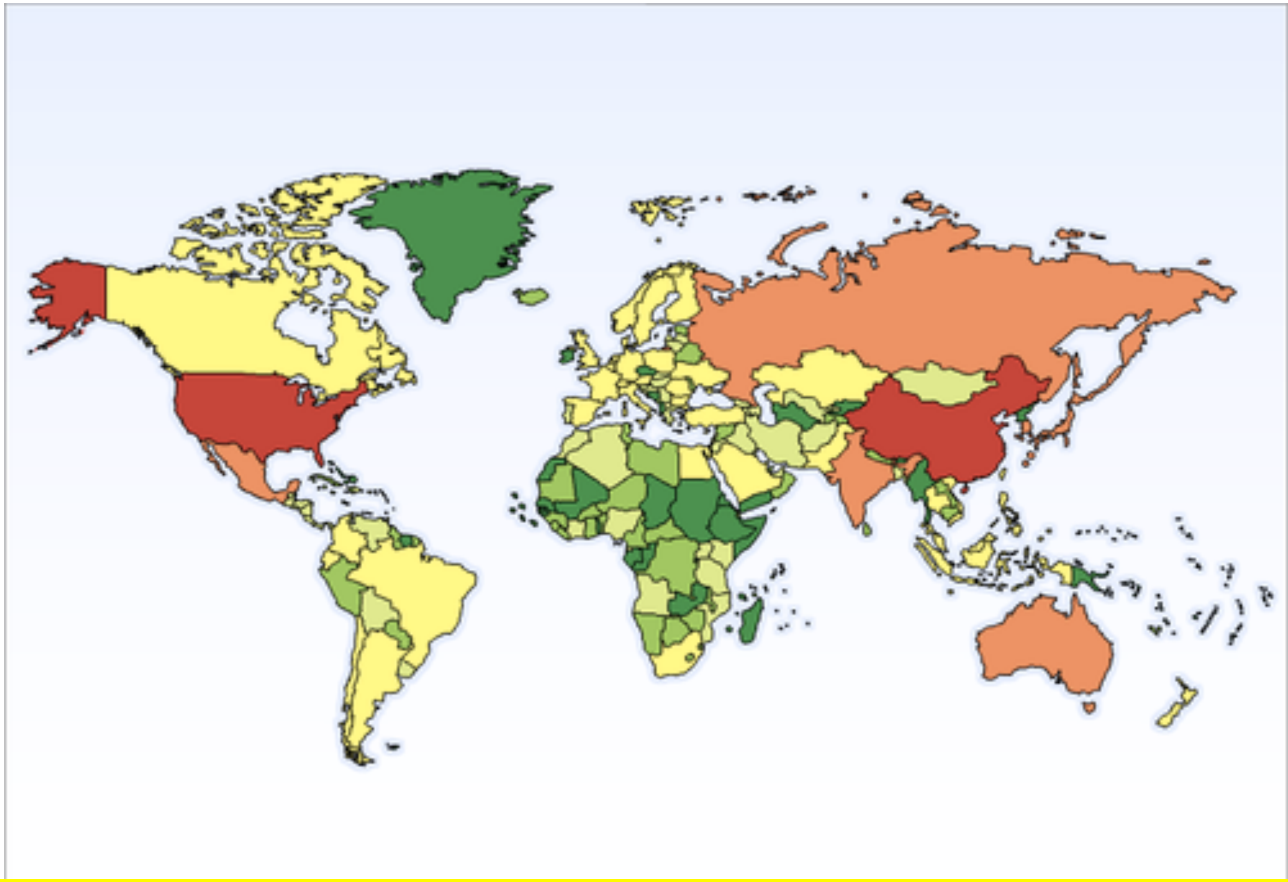
rrc13 193.232.244.82 to 20483 12976 3327 3491 17557
AS17557 PKTELECOM-AS-AP Pakistan Telecom

Youtube: 208.65.152.0/22

Pakistan Telcom: 208.65.152.0/24

中国某ISP路由劫持，2010年4月8日

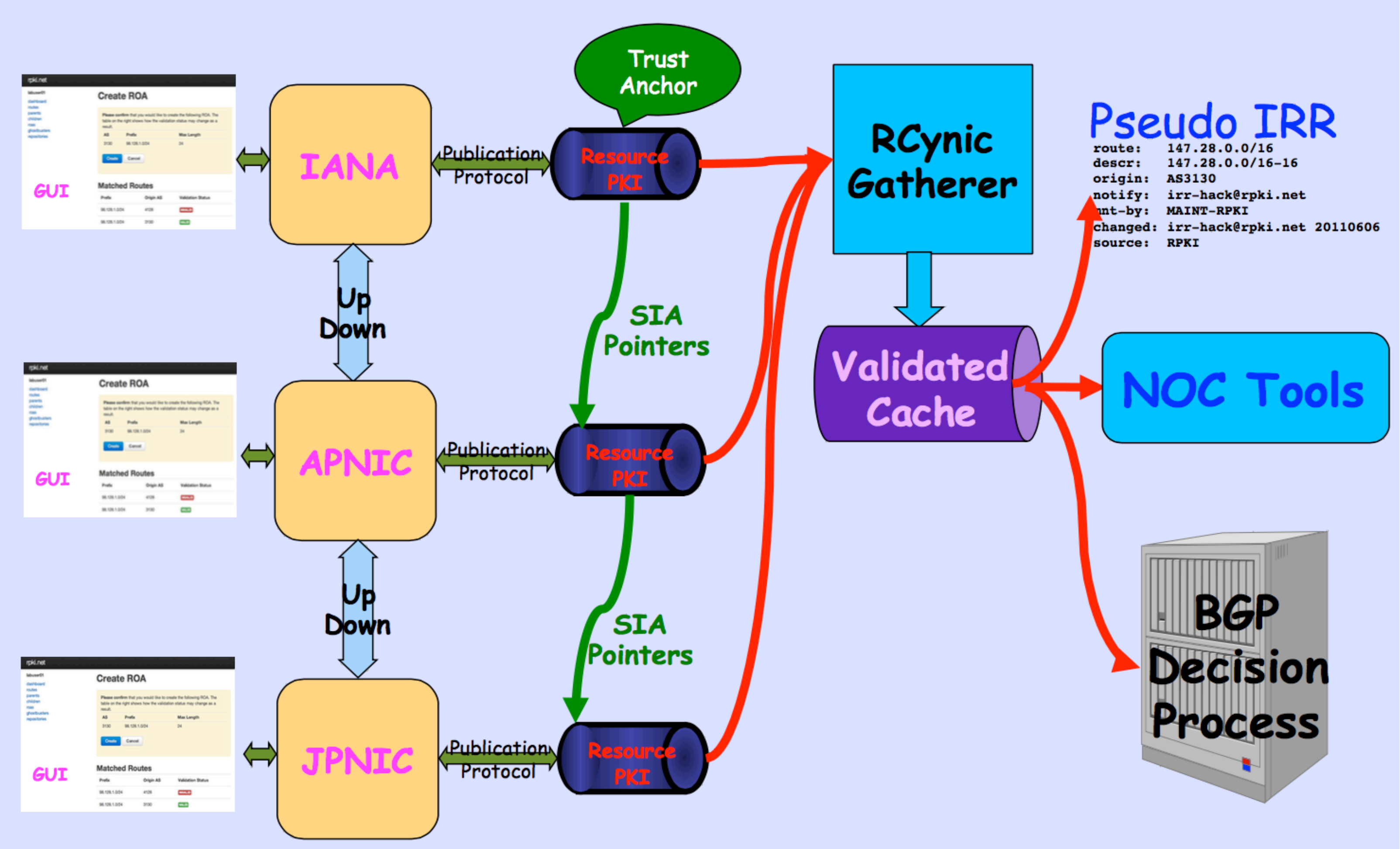
- 15%地址空间
- 170国家
- 持续18分钟



the scattershot nature of the hijack suggests a random mistake, not a deliberate attack on anyone in particular

http://www.renesys.com/2010/11/chinas-18-minute-mystery/

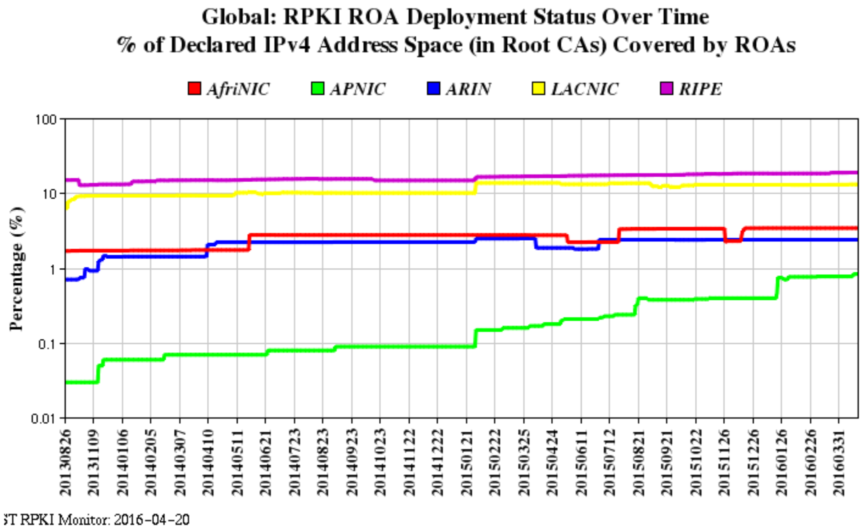
RPKI and BGPSec



```
route:   147.28.0.0/16
descr:   147.28.0.0/16-16
origin:  AS3130
notify:  irr-hack@rpki.net
mnt-by:  MAINT-RPKI
changed: irr-hack@rpki.net 20110606
source:  RPKI
```

An Infrastructure to Support Secure Internet Routing, RFC 6480, 2012

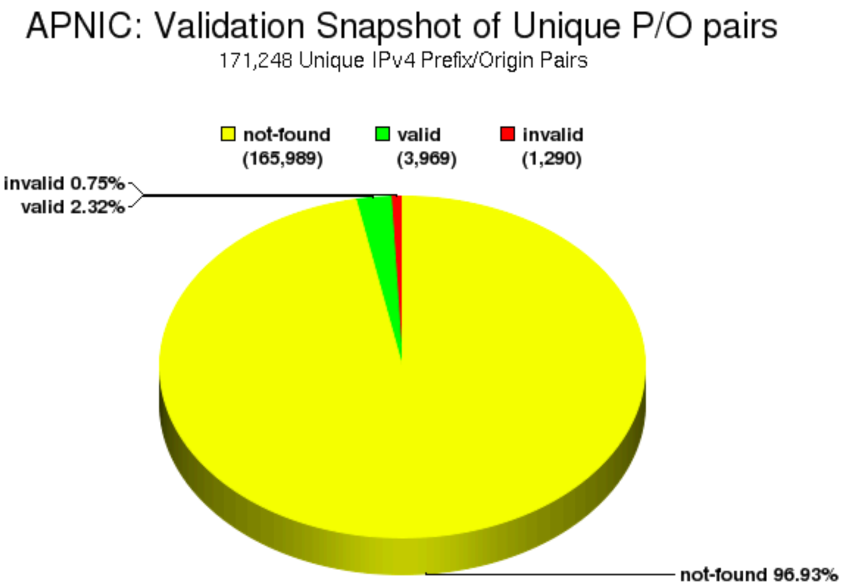
Deployment of RPKI



Global: RPKI ROA Deployment Status Over Time
% of Declared IPv4 Address Space (in Root CAs) Covered by ROAs

ST RPKI Monitor: 2016-04-20

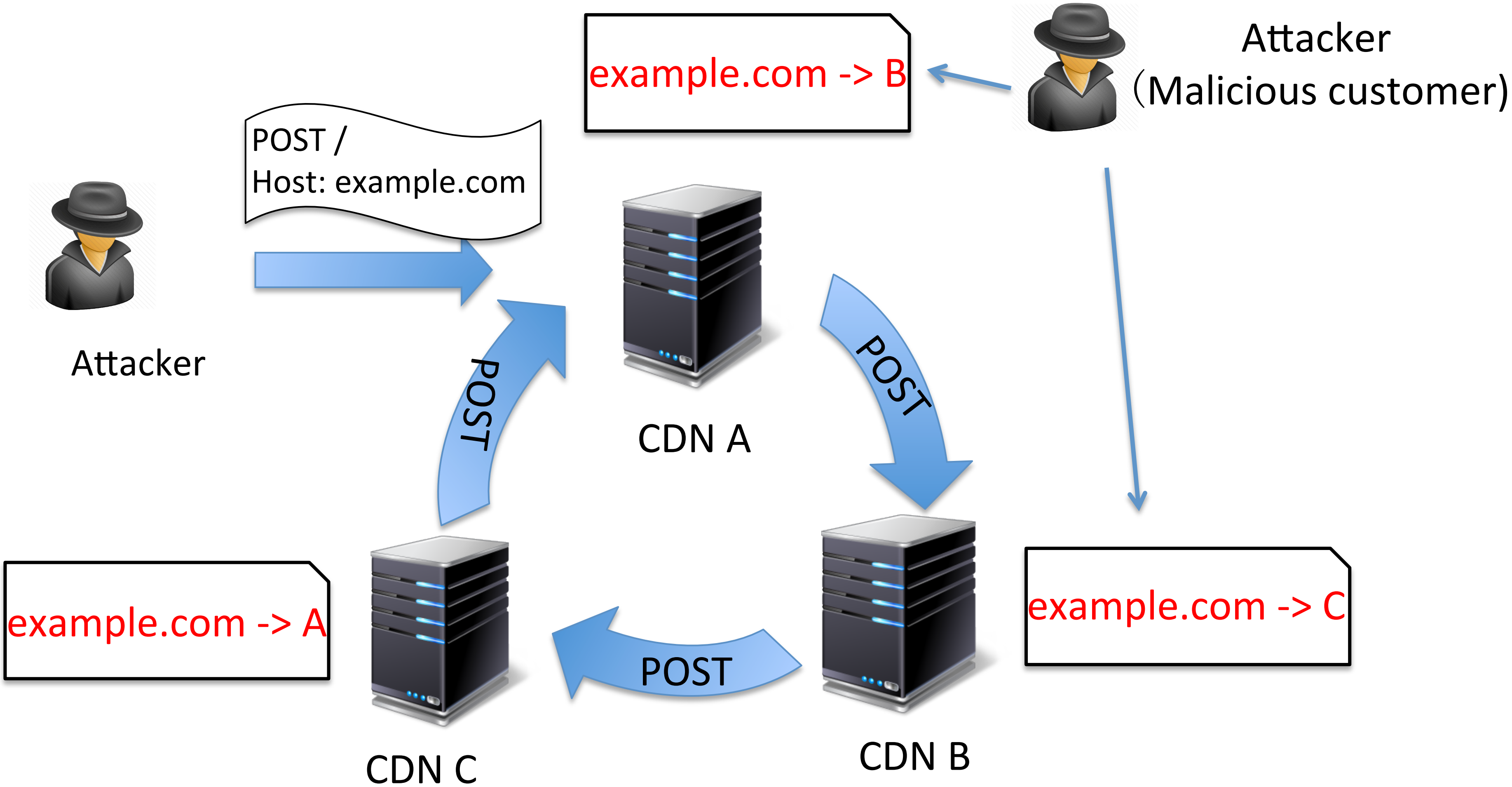
http://rpki-monitor.antd.nist.gov/?p=0&s=1



APNIC: Validation Snapshot of Unique P/O pairs
171,248 Unique IPv4 Prefix/Origin Pairs

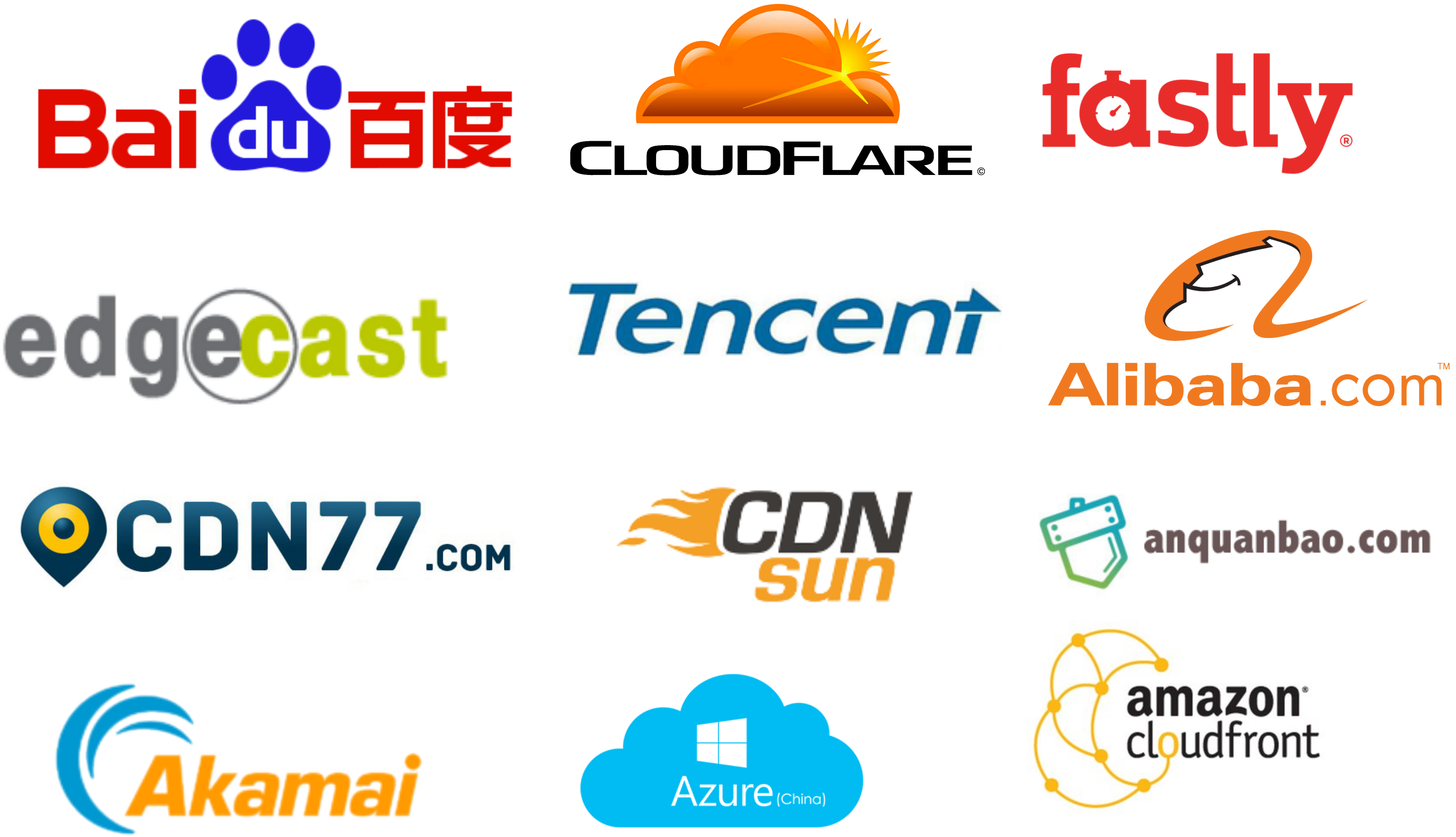
完美之路，遥遥无期。
不过，互联网的运转基本正常
大规模劫持必须向世界宣告一条非法路由
 谁愿意公开地与世界为敌？

Content routing: Forwarding-loop attack in CDN



Jianjun Chen, Jian Jiang, Xiaofeng Zheng, Haixin Duan, Jinjin Liang, Tao Wan, Kang Li, Vern Paxson, Forwarding-Loop Attacks in Content Delivery Networks, NDSS 2016 （Distinguished Paper Award）

Vulnerable CDN vendors(acknowledged)



Loop-Detection Headers are different

CDN Provider	Loop Detection Header	CDN Provider	Loop Detection Header
Akamai	Akamai-Origin-Hop	**CloudFlare**	X-Forwarded-For CF-Connecting-IP
Alibaba	Via	**CloudFront**	Via
Azure(China)		**Fastly**	Fastly-FF
Baidu	X-Forwarded-For CF-Connecting-IP	**Incapsula**	Incap-Proxy-ID
CDN77		**KeyCDN**	
CDNlion		**Level3**	Via
CDN.net		**MaxCDN**	
CDNsun		**Tencent**	X-Daa-Tunnel

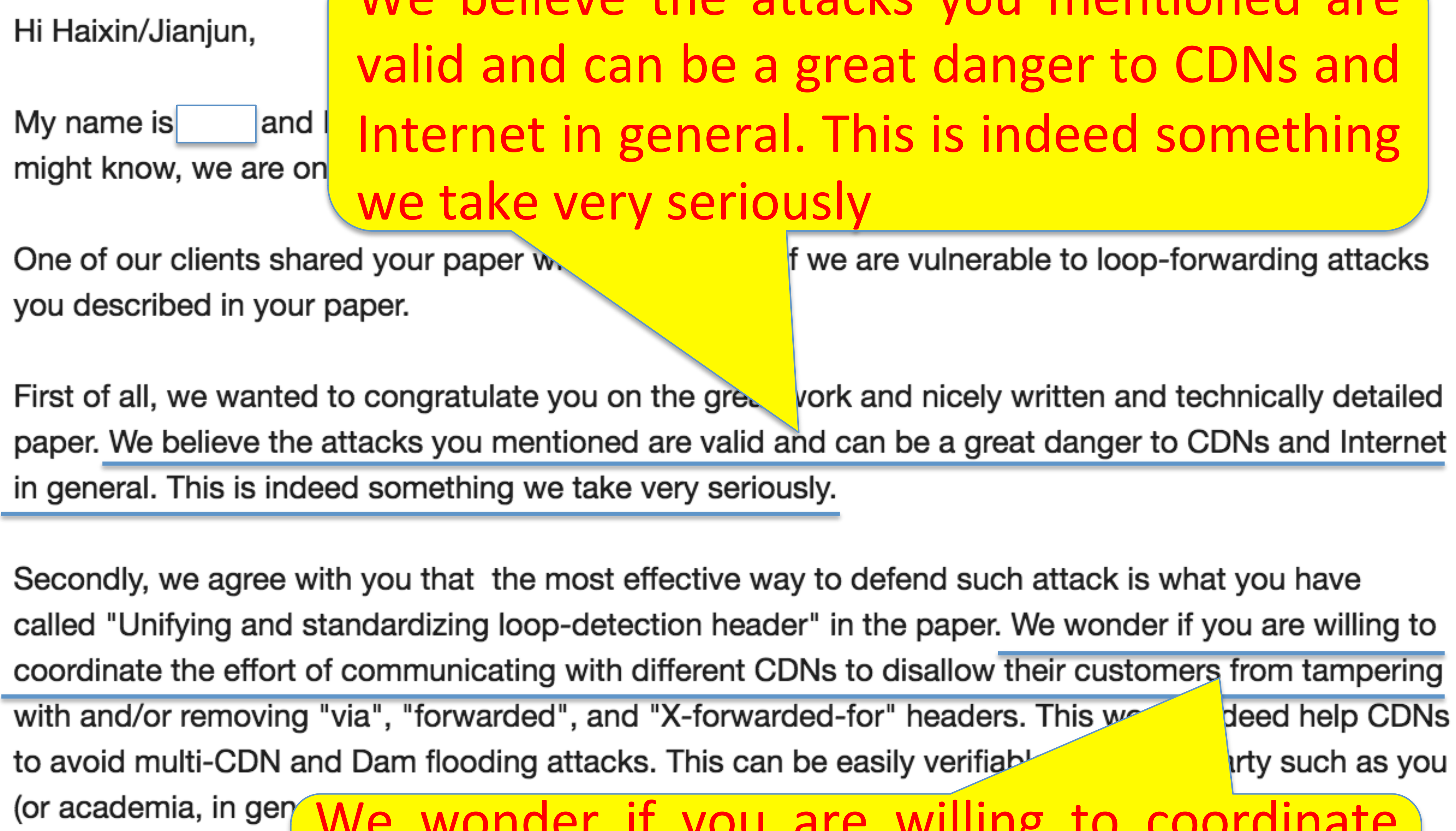
RFC 7230 recommends to use Via header for loop detection

Bypassing CDN defenses

- Chain loop-aware CDNs to other CDNs that can be abused to *disrupt* loop-detection headers
- Abusive features provided by CDNs:

CDN Provider	Reset	Filter
CDN77	Via	
CDNlion	Via	
CDN.net	Via	
CDNsun	Via	
Fastly		No-self-defined
MaxCDN		Any

We believe the attacks you mentioned are valid and can be a great danger to CDNs and Internet in general. This is indeed something we take very seriously



Hi Haixin/Jianjun,

My name is and I
might know, we are on

One of our clients shared your paper w f we are vulnerable to loop-forwarding attacks you described in your paper.

First of all, we wanted to congratulate you on the gre vork and nicely written and technically detailed paper. We believe the attacks you mentioned are valid and can be a great danger to CDNs and Internet in general. This is indeed something we take very seriously.

Secondly, we agree with you that the most effective way to defend such attack is what you have called "Unifying and standardizing loop-detection header" in the paper. We wonder if you are willing to coordinate the effort of communicating with different CDNs to disallow their customers from tampering with and/or removing "via", "forwarded", and "X-forwarded-for" headers. This w deed help CDNs to avoid multi-CDN and Dam flooding attacks. This can be easily verifiab rty such as you (or academia, in gen

We wonder if you are willing to coordinate the effort of communicating with different CDNs to…

A case, without centralized anchor…

- A case that highlights the danger of allowing cross-organization, user-controlled (untrusted) policies without centralized administration
- How to enforce standard compliance, especially when global coordination is needed

- Who is responsible for compliance of IETF standards?

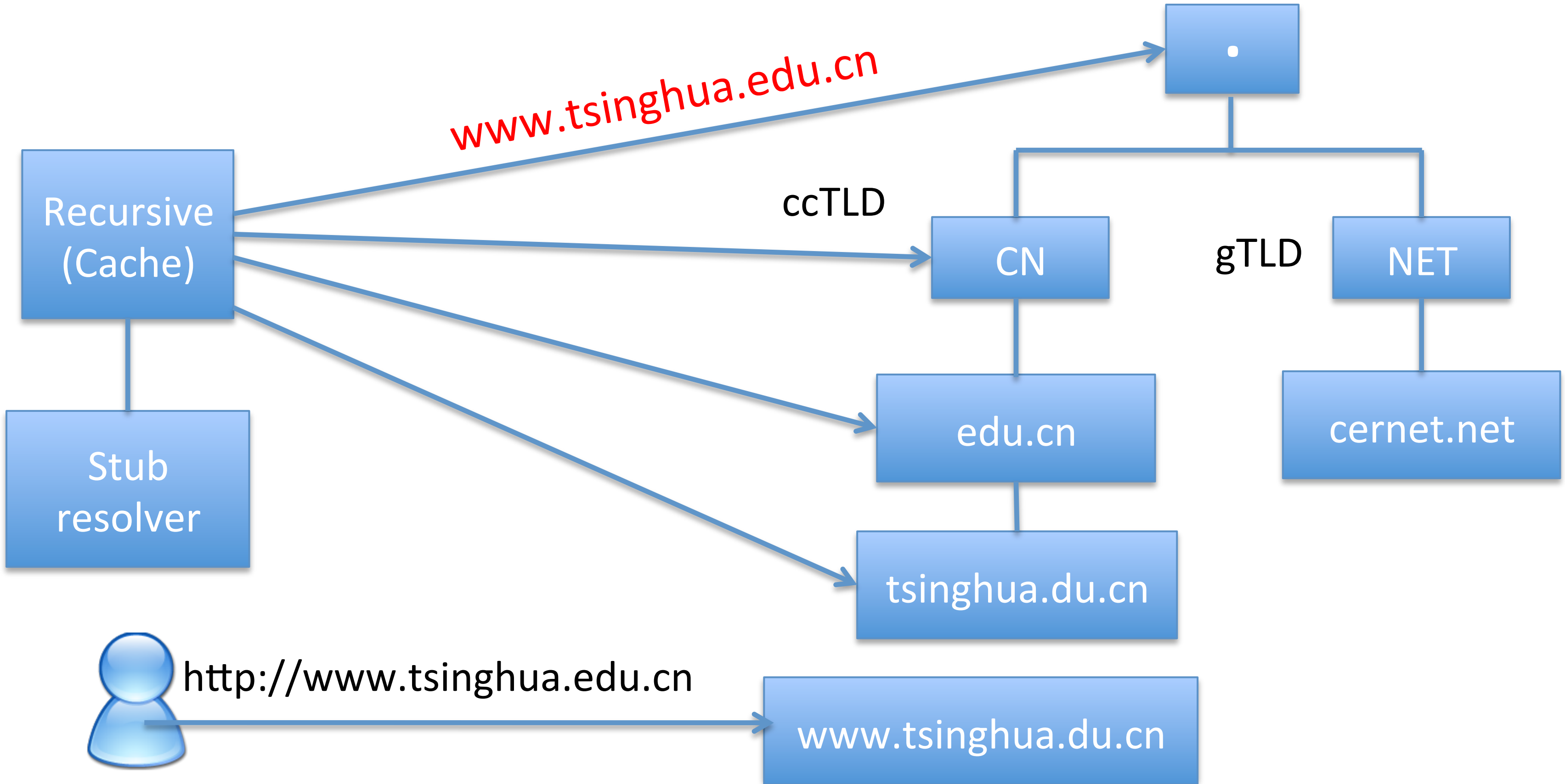
In DNS we Trust

Trust Anchors: Only Root?

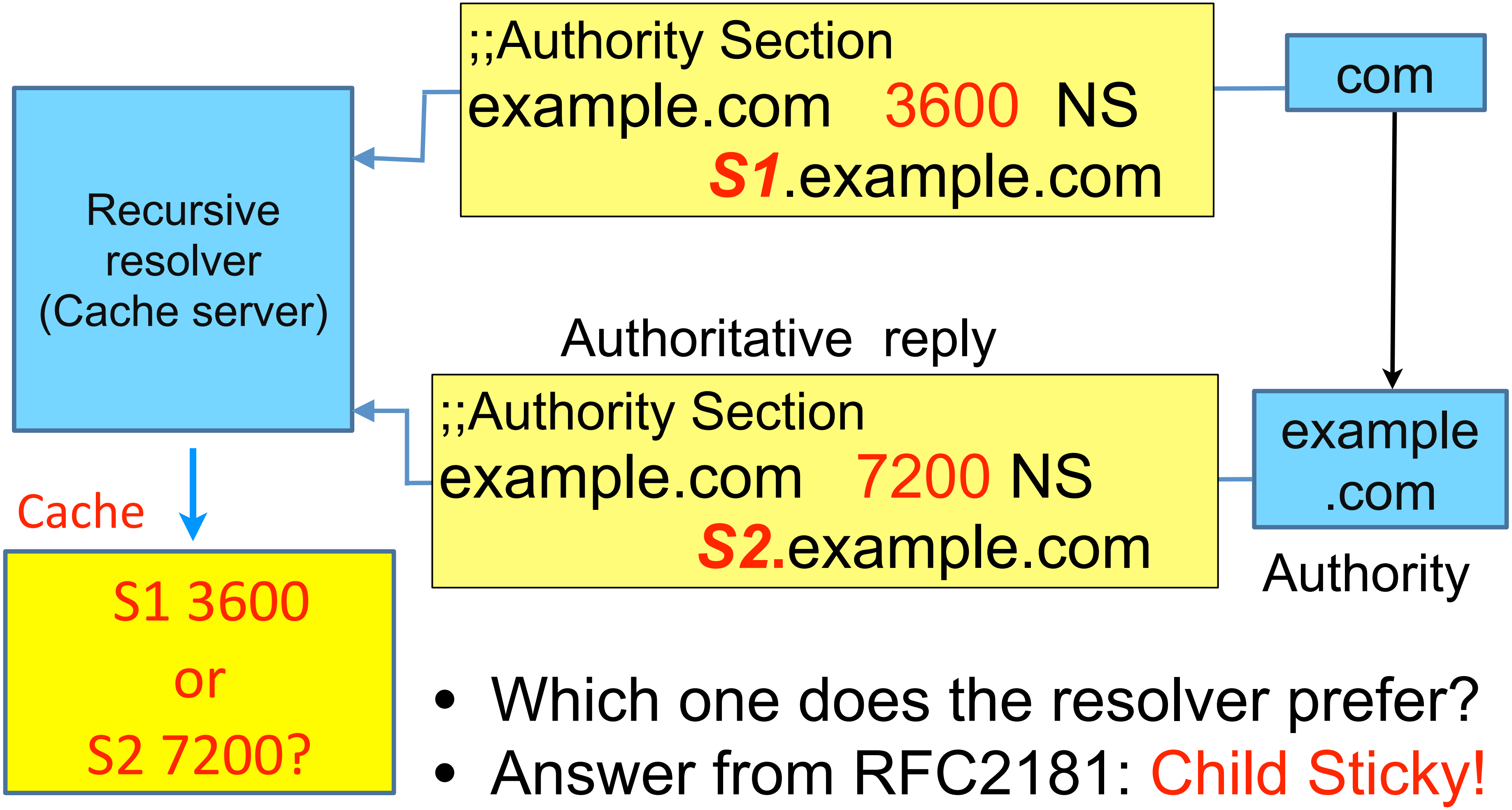
客户端：递归/缓存
- Cache, Recursive

UDP

权威服务器（Authoritative），Root, TLD, …



Problem:
“Parent-Sticky” or “Child-Sticky” ?



```
;;Authority Section
example.com   3600  NS
            S1.example.com
```

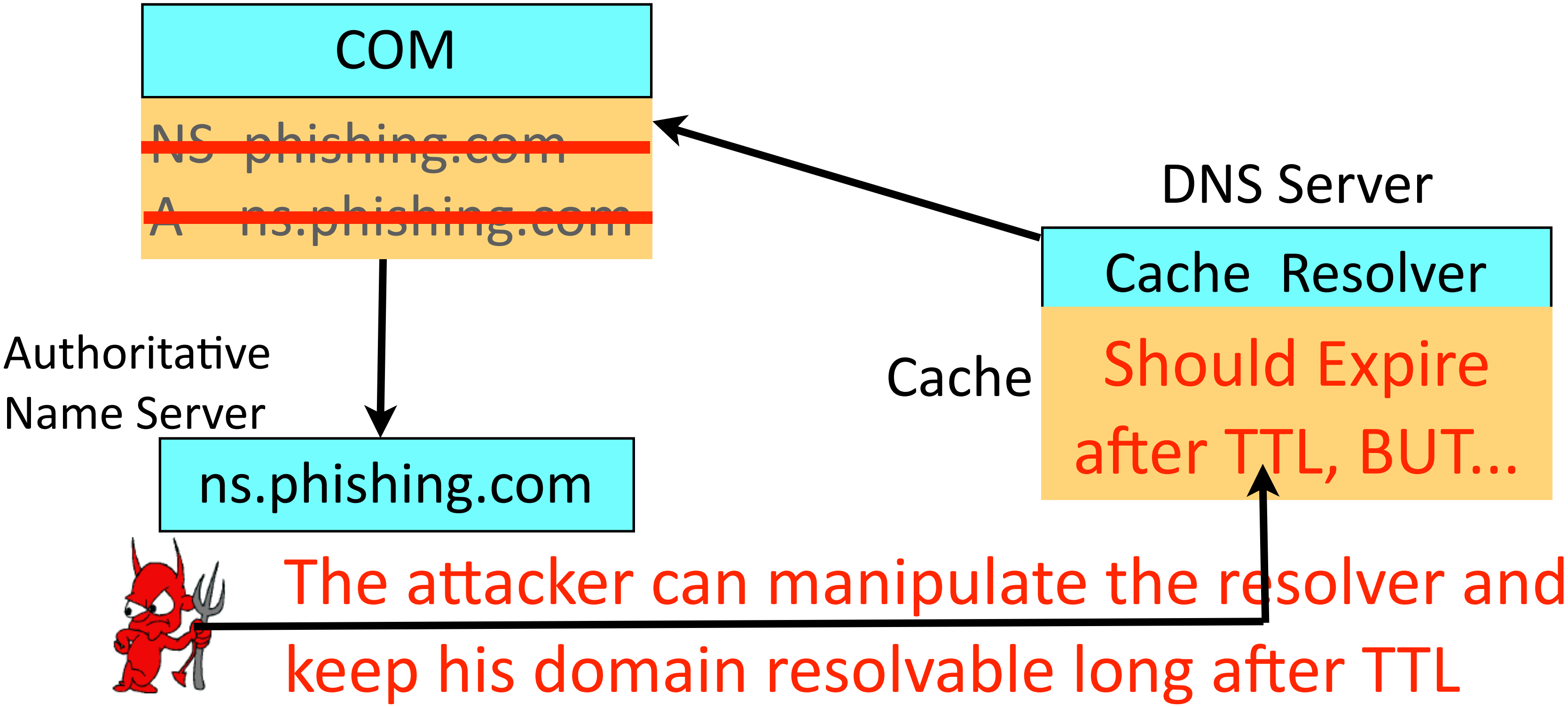
```
;;Authority Section
example.com   7200 NS
            S2.example.com
```

S1 3600
or
S2 7200?

- Which one does the resolver prefer?
- Answer from RFC2181: Child Sticky!
- Child-Sticky enables self-update !

Ghost Domain, CVE-2012-1033, 2012

- Attacker registers domain name for various attacks
- Current practice is to revoke domain from registrar
- But a domain could be resolvable long after that...



COM

~~NS phishing.com~~

~~A ns.phishing.com~~

Authoritative Name Server

ns.phishing.com

DNS Server

Cache Resolver

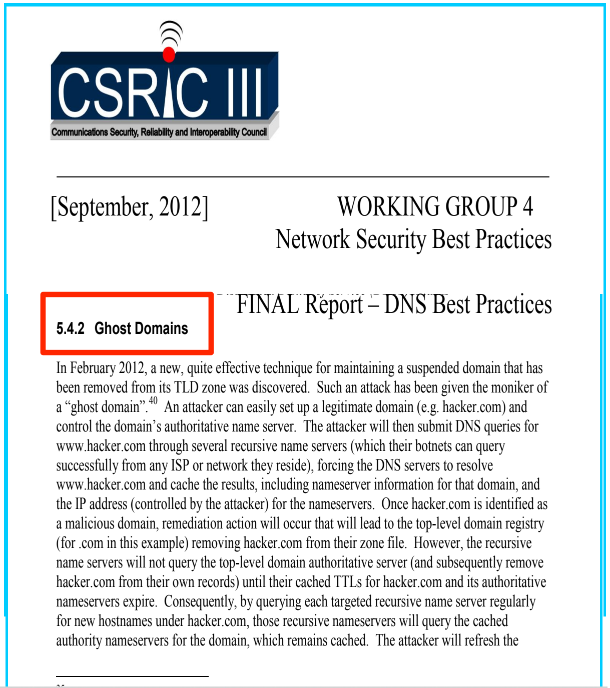
Cache

Should Expire after TTL, BUT...

The attacker can manipulate the resolver and keep his domain resolvable long after TTL

幽灵域名对工业界和学术界的影响

- 论文发表在网络安全顶级学术会议NDSS 2012
- 美国国家漏洞库收录，10个DNS软件厂商为自己的软件发布补丁
- 美国联邦通讯局（FCC）安全工作组将Ghost domain写入2012年安全最佳实践（Best Practice）报告



CSRIC III
Communications Security, Reliability and Interoperability Council

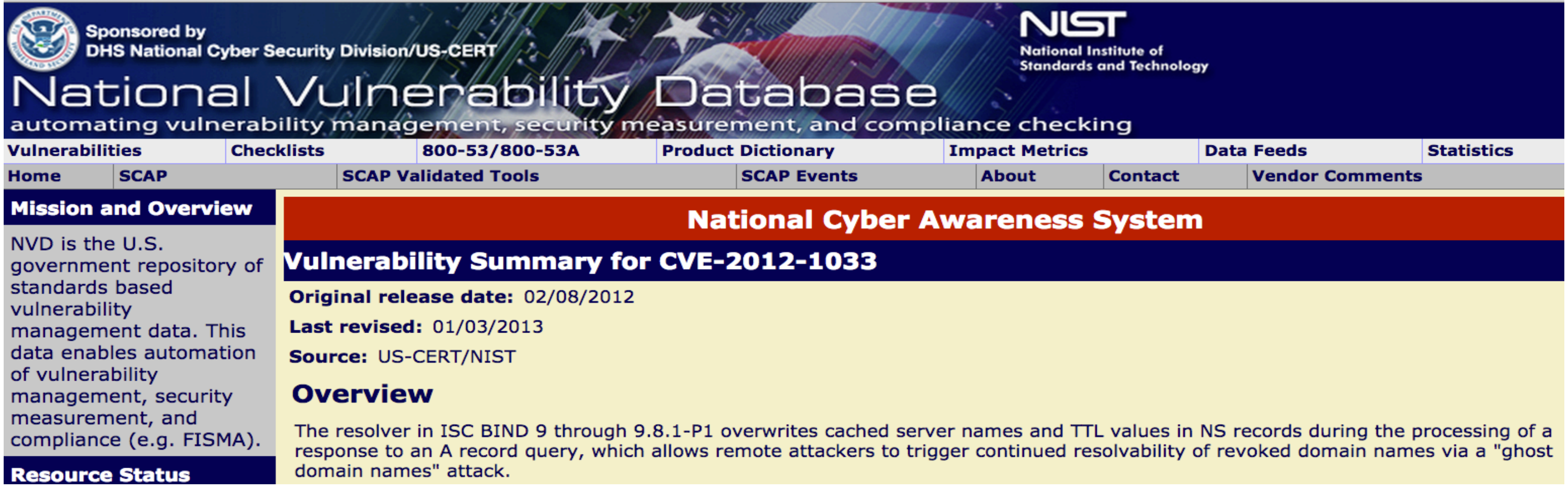
[September, 2012]

WORKING GROUP 4
Network Security Best Practices

FINAL Report – DNS Best Practices

5.4.2 Ghost Domains

In February 2012, a new, quite effective technique for maintaining a suspended domain that has been removed from its TLD zone was discovered. Such an attack has been given the moniker of a "ghost domain".[40] An attacker can easily set up a legitimate domain (e.g. hacker.com) and control the domain's authoritative name server. The attacker will then submit DNS queries for www.hacker.com through several recursive name servers (which their botnets can query successfully from any ISP or network they reside), forcing the DNS servers to resolve www.hacker.com and cache the results, including nameserver information for that domain, and the IP address (controlled by the attacker) for the nameservers. Once hacker.com is identified as a malicious domain, remediation action will occur that will lead to the top-level domain registry (for .com in this example) removing hacker.com from their zone file. However, the recursive name servers will not query the top-level domain authoritative server (and subsequently remove hacker.com from their own records) until their cached TTLs for hacker.com and its authoritative nameservers expire. Consequently, by querying each targeted recursive name server regularly for new hostnames under hacker.com, those recursive nameservers will query the cached authority nameservers for the domain, which remains cached. The attacker will refresh the



Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

National Cyber Awareness System

Vulnerability Summary for CVE-2012-1033

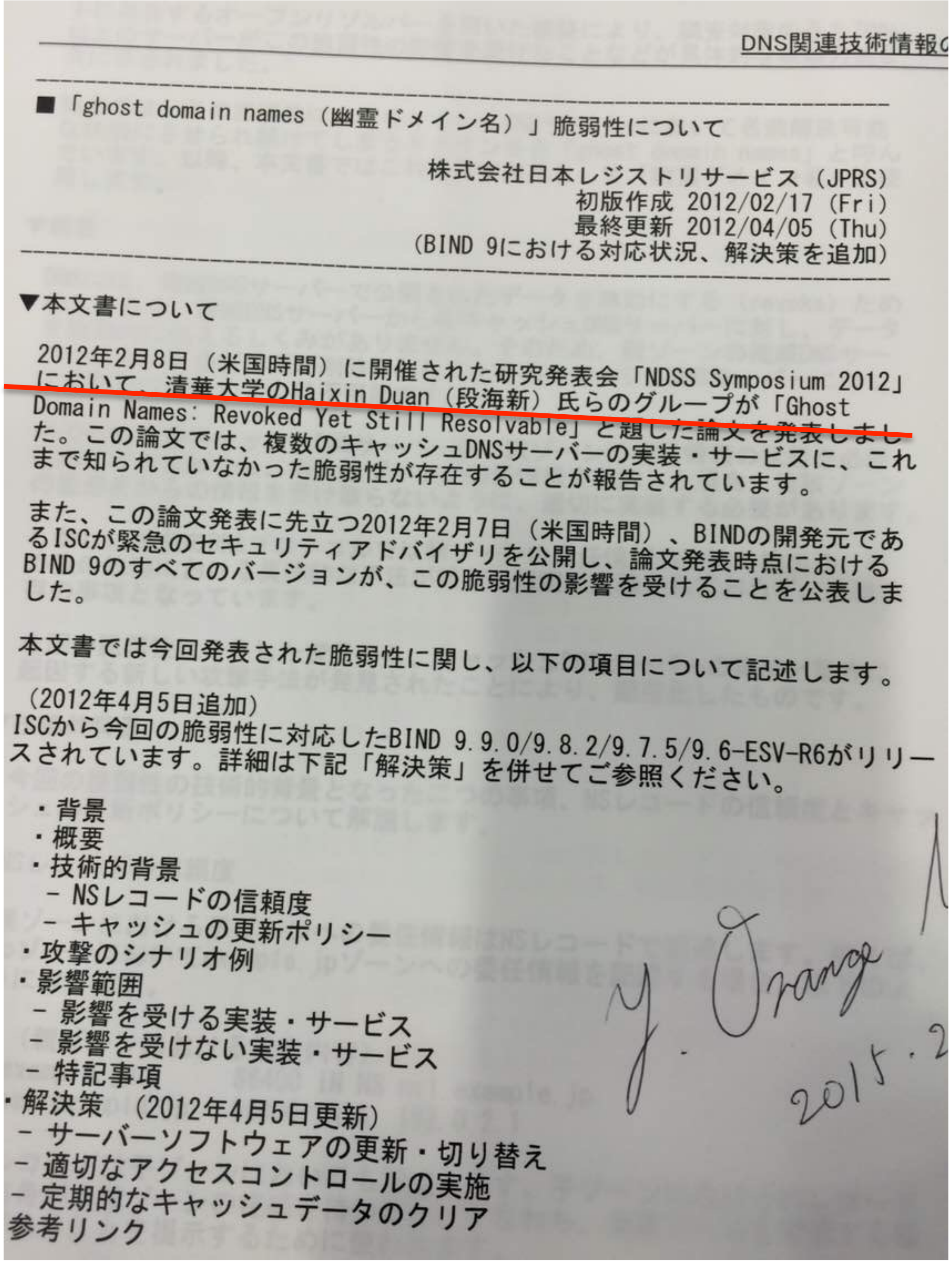
Original release date: 02/08/2012
Last revised: 01/03/2013
Source: US-CERT/NIST

Overview

The resolver in ISC BIND 9 through 9.8.1-P1 overwrites cached server names and TTL values in NS records during the processing of a response to an A record query, which allows remote attackers to trigger continued resolvability of revoked domain names via a "ghost domain names" attack.

Ghost Domain 被翻译成日文在日本互联网届产生重要影响

2015年2月，我访问日本时，译者送我的签名拷贝



DNS関連技術情報の

■「ghost domain names（幽霊ドメイン名）」脆弱性について

株式会社日本レジストリサービス（JPRS）
初版作成 2012/02/17（Fri）
最終更新 2012/04/05（Thu）
（BIND 9における対応状況、解決策を追加）

▼本文書について

2012年2月8日（米国時間）に開催された研究発表会「NDSS Symposium 2012」において、清華大学のHaixin Duan（段海新）氏らのグループが「Ghost Domain Names: Revoked Yet Still Resolvable」と題した論文を発表しました。この論文では、複数のキャッシュDNSサーバーの実装・サービスに、これまで知られていなかった脆弱性が存在することが報告されています。

また、この論文発表に先立つ2012年2月7日（米国時間）、BINDの開発元であるISCが緊急のセキュリティアドバイザリを公開し、論文発表時点におけるBIND 9のすべてのバージョンが、この脆弱性の影響を受けることを公表しました。

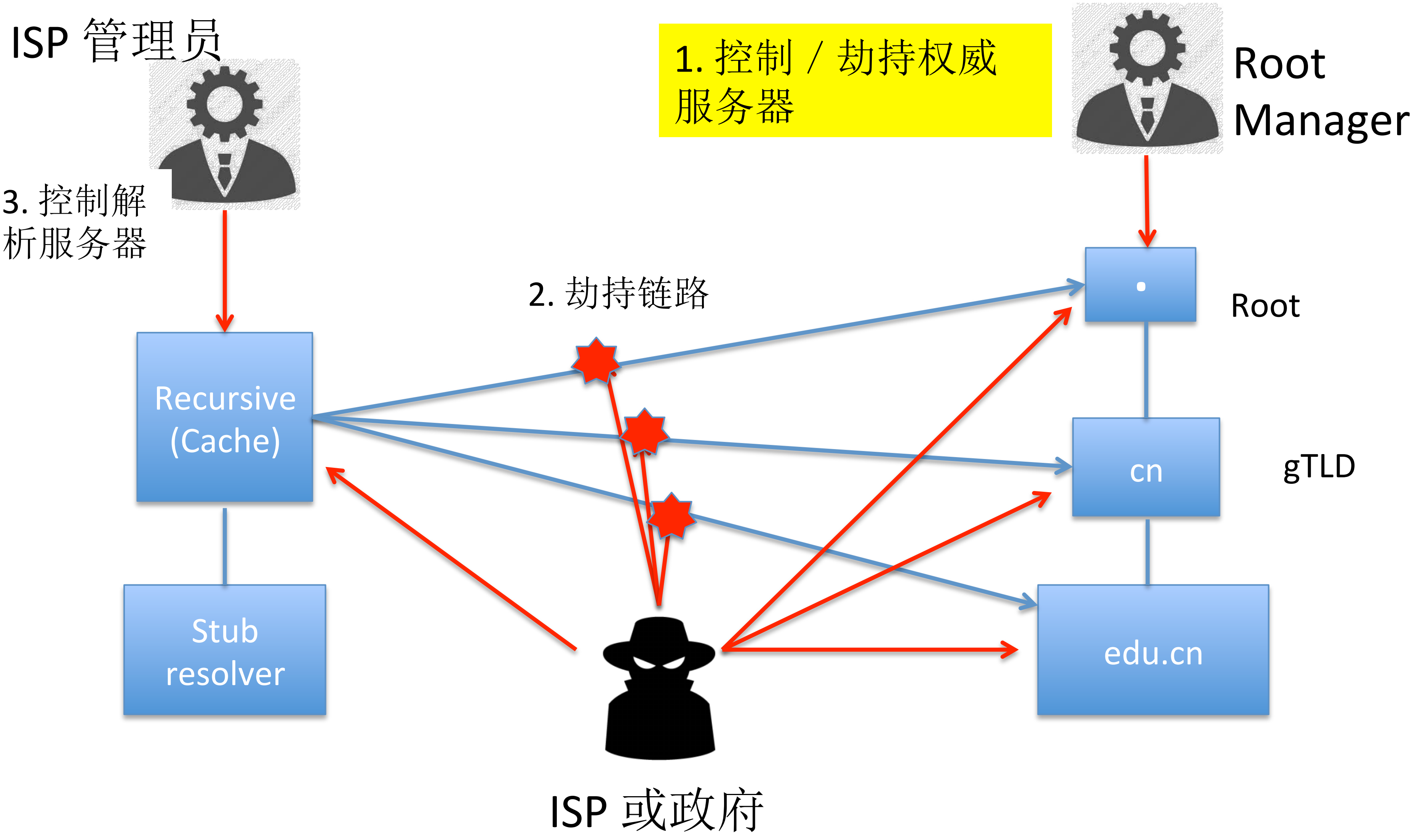
本文書では今回発表された脆弱性に関し、以下の項目について記述します。

（2012年4月5日追加）
ISCから今回の脆弱性に対応したBIND 9.9.0/9.8.2/9.7.5/9.6-ESV-R6がリリースされています。詳細は下記「解決策」を併せてご参照ください。

・背景
・概要
・技術的背景
　- NSレコードの信頼度
　- キャッシュの更新ポリシー
・攻撃のシナリオ例
・影響範囲
　- 影響を受ける実装・サービス
　- 影響を受けない実装・サービス
　- 特記事項
・解決策　（2012年4月5日更新）
　- サーバーソフトウェアの更新・切り替え
　- 適切なアクセスコントロールの実施
　- 定期的なキャッシュデータのクリア
参考リンク

Y. Orange
2015.2

We trust: Root, Link and local resolver



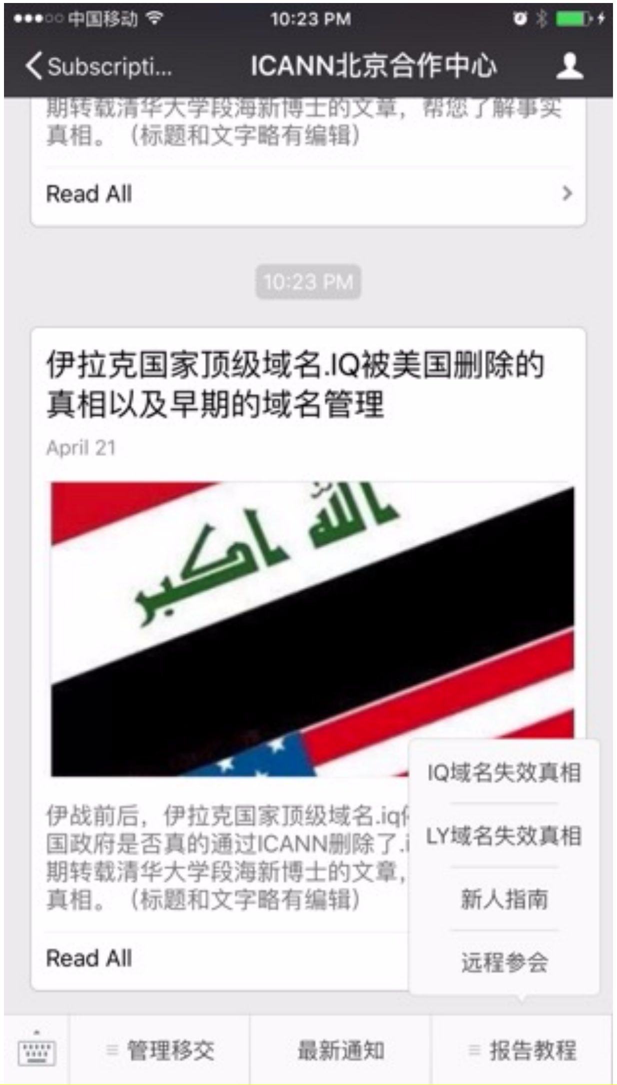
Root Manipulations/Hijacking?

- Hijacking of Root by Jon Postel, 1998
  - 邮件通知8个root管理员同步IANA而非NSI
- 2014/6/24《人民日报》：在美国政府授意下，伊拉克顶级域名“.iq”的申请和解析工作被终止，所有网址以“.iq”为后缀的网站从互联网蒸发
- 《信息安全与通信保密》2014年第10期：美国终止了利比亚的顶级域名. ly的解析服务，导致利比亚从网络中消失3天

真是这样的吗？证据来自哪里？

伊拉克域名IQ被美国删除的背后以及早期的根域名管理

段海新



期转载清华大学段海新博士的文章，帮您了解事实真相。（标题和文字略有编辑）

Read All

伊拉克国家顶级域名.IQ被美国删除的真相以及早期的域名管理

April 21

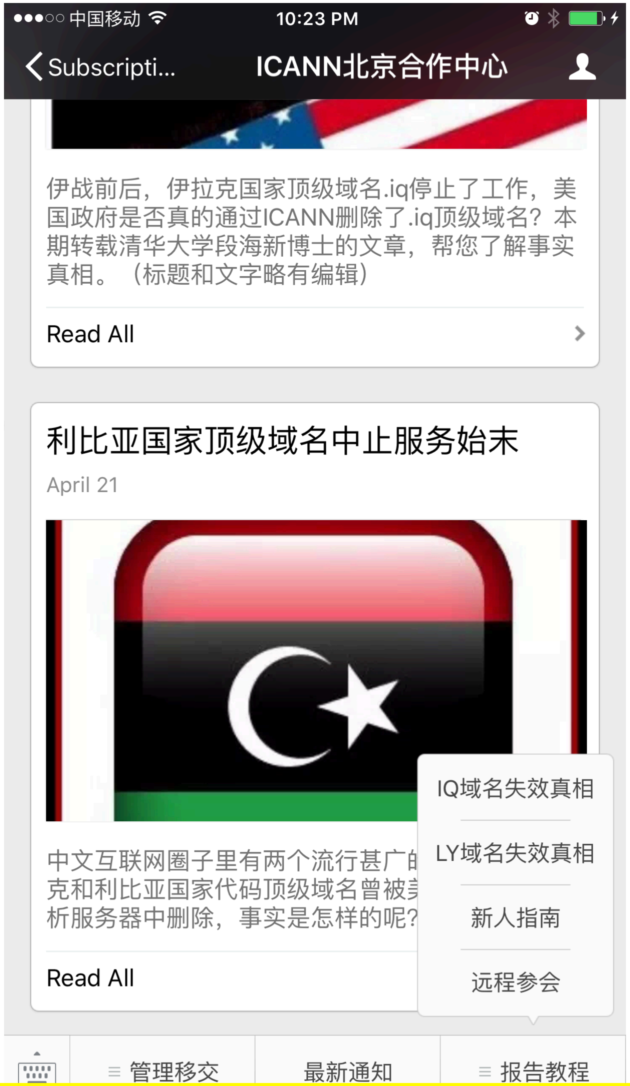
伊战前后，伊拉克国家顶级域名.iq
国政府是否真的通过ICANN删除了.i
期转载清华大学段海新博士的文章，
真相。（标题和文字略有编辑）

Read All

http://netsec.ccert.edu.cn/duanhx/?p=1850

美国真的删过“.IQ”和“.LY”吗？

（ICANN 首席技术官 David Conrad，ICANN 北京合作中心主任宋崝，域名工程中心高级研究员张建川）



伊战前后，伊拉克国家顶级域名.iq停止了工作，美国政府是否真的通过ICANN删除了.iq顶级域名？本期转载清华大学段海新博士的文章，帮您了解事实真相。（标题和文字略有编辑）

Read All

利比亚国家顶级域名中止服务始末

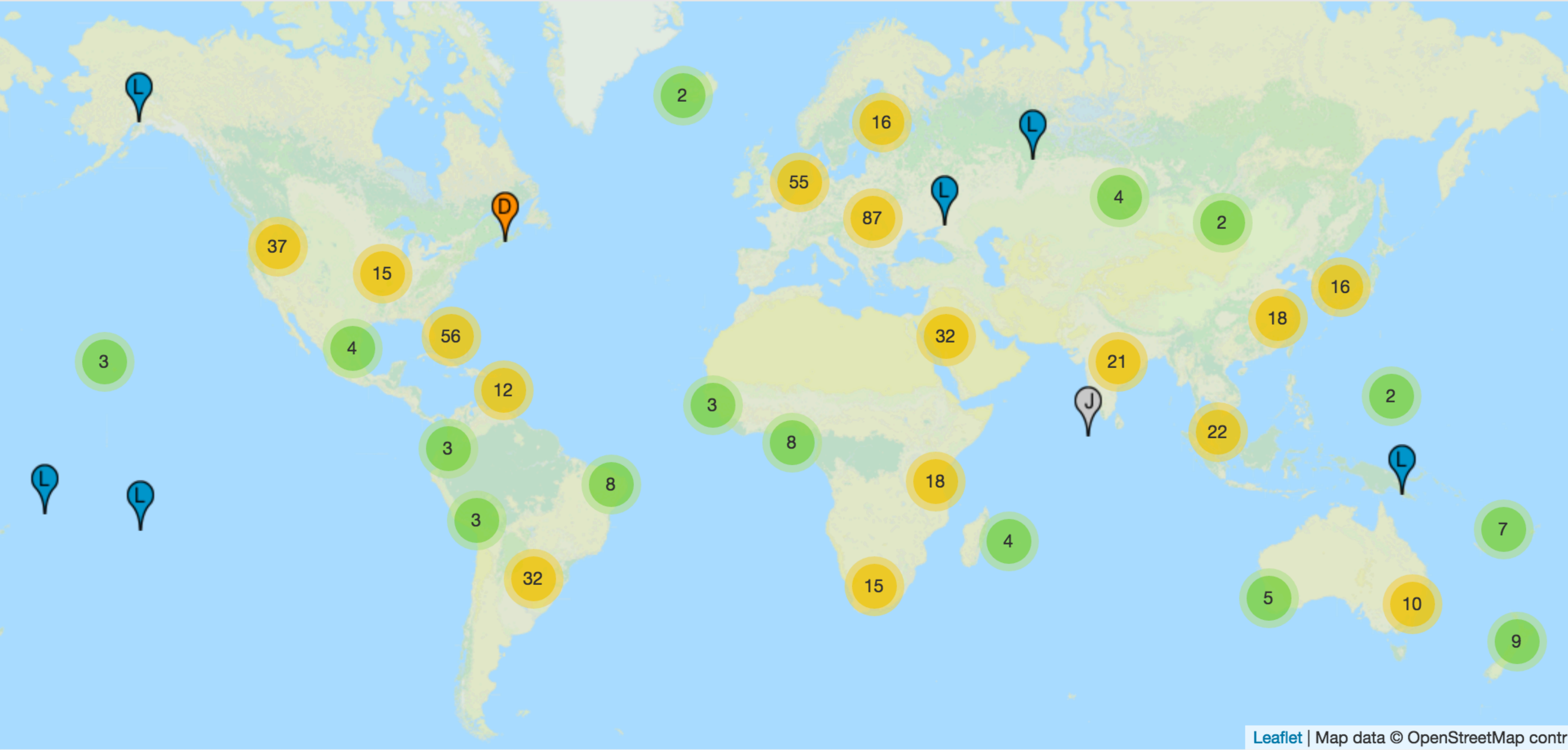
April 21

中文互联网圈子里有两个流行甚广的
克和利比亚国家代码顶级域名曾被美
析服务器中删除，事实是怎样的呢？

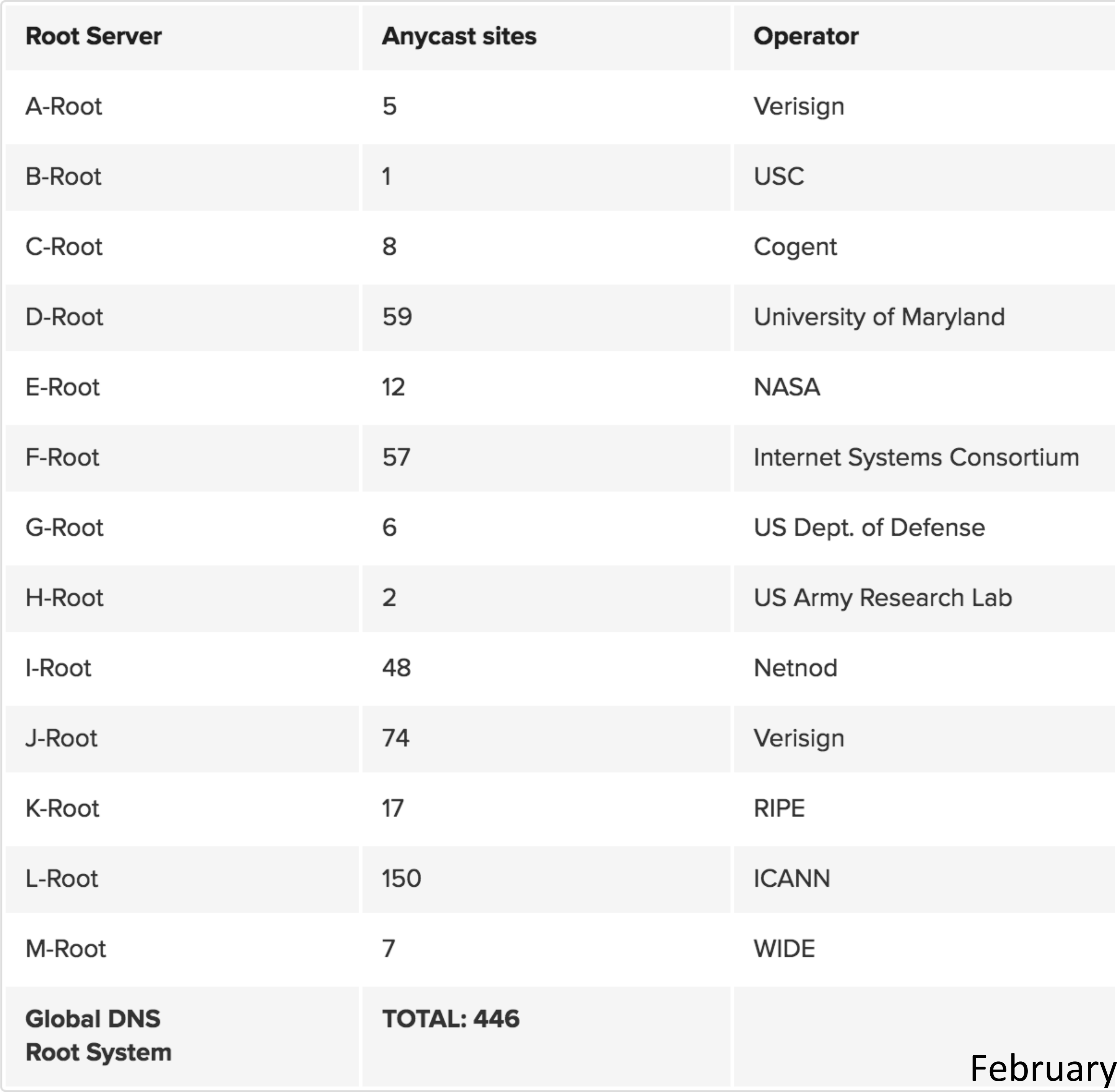
Read All

http://www.inforsec.org/wp/?p=86

Root-Servers



http://www.root-servers.org/

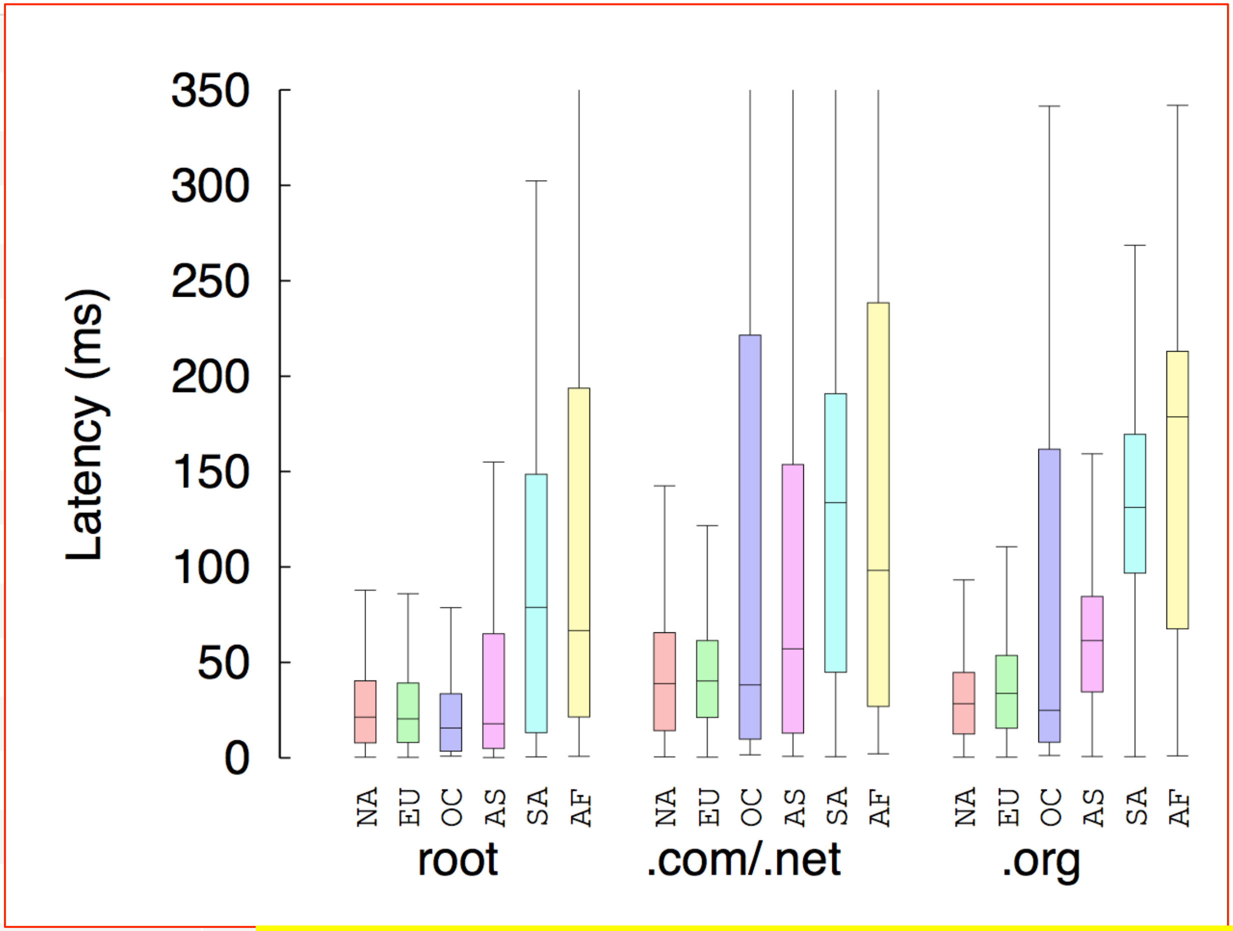


Root Server	Anycast sites	Operator
A-Root	5	Verisign
B-Root	1	USC
C-Root	8	Cogent
D-Root	59	University of Maryland
E-Root	12	NASA
F-Root	57	Internet Systems Consortium
G-Root	6	US Dept. of Defense
H-Root	2	US Army Research Lab
I-Root	48	Netnod
J-Root	74	Verisign
K-Root	17	RIPE
L-Root	150	ICANN
M-Root	7	WIDE
Global DNS Root System	**TOTAL: 446**	

February 2015

Measuring Roots, for performance and …

Country	Mean Latency (ms) to	
Bangladesh	57	
Brazil	51	
China	66	
Egypt	51	
France	23	
Germany	10	
India	38	
Indonesia	20	
Italy	46	
Iran	154	
Japan	15	
Mexico	55	
Pakistan	36	
Philippines	136	
Russia	35	
Thailand	20	I-Ro
Turkey	94	A-R
United Kingdom	13	E-R
		-R
		-Root

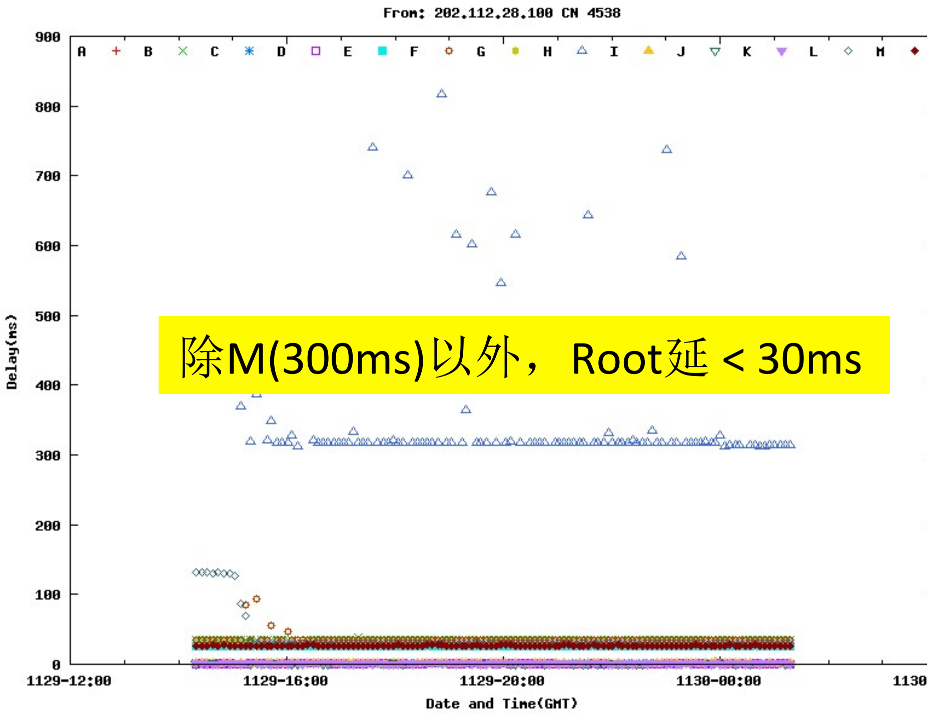


https://blog.thousandeyes.com/
comparing-dns-root-server-performance/

J. Liang, J. Jiang, H. Duan, K. Li, and J. Wu, "Measuring query latency of top level DNS servers," Passive and Active Measurement, March 2013.

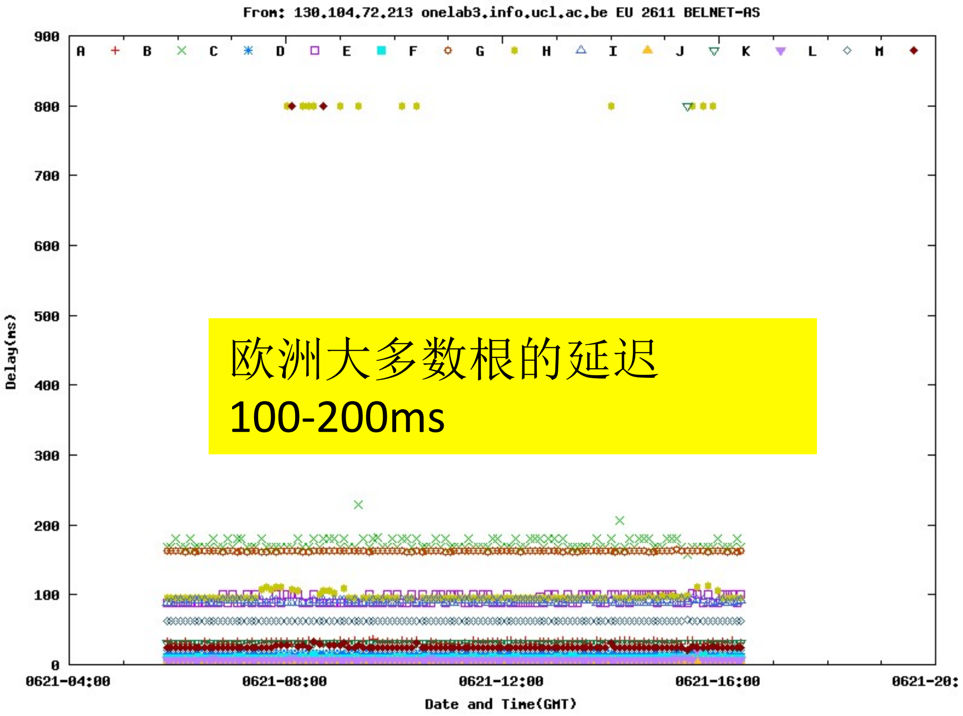
到Root的延迟： CERNET & Europe, 2012

- Root DNS delay in CERNET

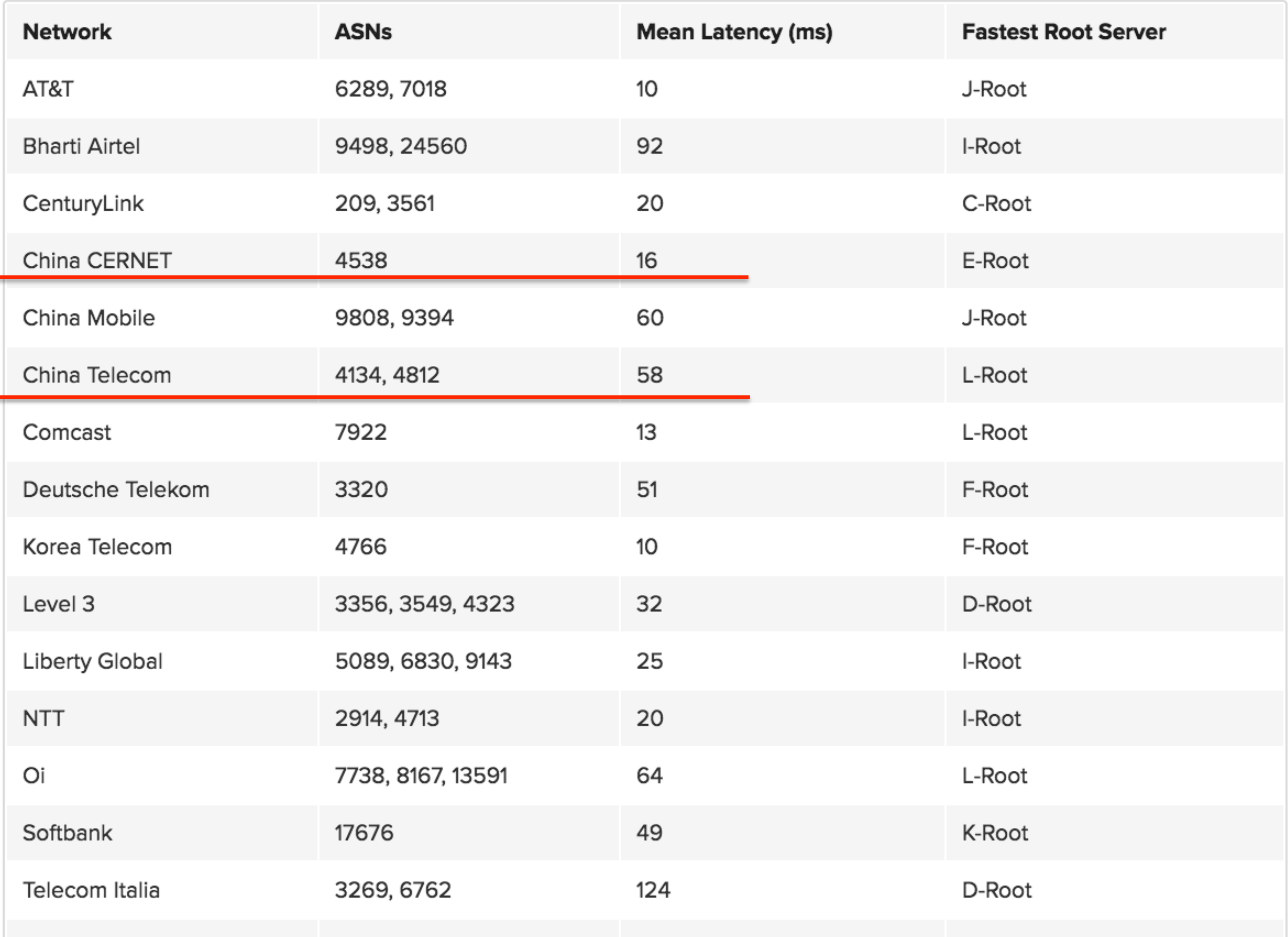


除M(300ms)以外，Root延 < 30ms

- Root Delay in Europe



欧洲大多数根的延迟
100-200ms



Network	ASNs	Mean Latency (ms)	Fastest Root Server
AT&T	6289, 7018	10	J-Root
Bharti Airtel	9498, 24560	92	I-Root
CenturyLink	209, 3561	20	C-Root
China CERNET	4538	16	E-Root
China Mobile	9808, 9394	60	J-Root
China Telecom	4134, 4812	58	L-Root
Comcast	7922	13	L-Root
Deutsche Telekom	3320	51	F-Root
Korea Telecom	4766	10	F-Root
Level 3	3356, 3549, 4323	32	D-Root
Liberty Global	5089, 6830, 9143	25	I-Root
NTT	2914, 4713	20	I-Root
Oi	7738, 8167, 13591	64	L-Root
Softbank	17676	49	K-Root
Telecom Italia	3269, 6762	124	D-Root

https://blog.thousandeyes.com/comparing-dns-root-server-performance/

Faked Roots in AS 4538, detected by

- J. Liang, J. Jiang, H. Duan, K. Li, and J. Wu, "Measuring query latency of top level DNS servers," Passive and Active Measurement, March 2013.
- Xun Fan, John Heidemann and Ramesh Govindan. Evaluating Anycast in the Domain Name System. IEEE Infocom , Apr. 2013
- Ben Jones, Nick Feamster, Vern Paxson, Nicholas Weaver, Mark Allman. Detecting DNS Root Manipulation. Passive and Active Measurement Conference, March 2016.

Alternative Root solutions

- Open Root Server Network (ORSN)
  - Synchronization with ICANN.
  - to avoid the technical possibility of global "Internet shutdown" by one party.
  - Paul Vixie, is a proponent of the ORSN.
- eDNS (Enhanced Domain Name Service)
- Open RSC(Root Service Confederation)

ICANN: One world, One Internet

ONE WORLD. ONE INTERNET.

ICANN

2010
ANNUAL
REPORT

Network Working Group   Internet Architecture Board
Request for Comments: 2826   May 2000
Category: Informational

IAB Technical Comment on the Unique DNS Root

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

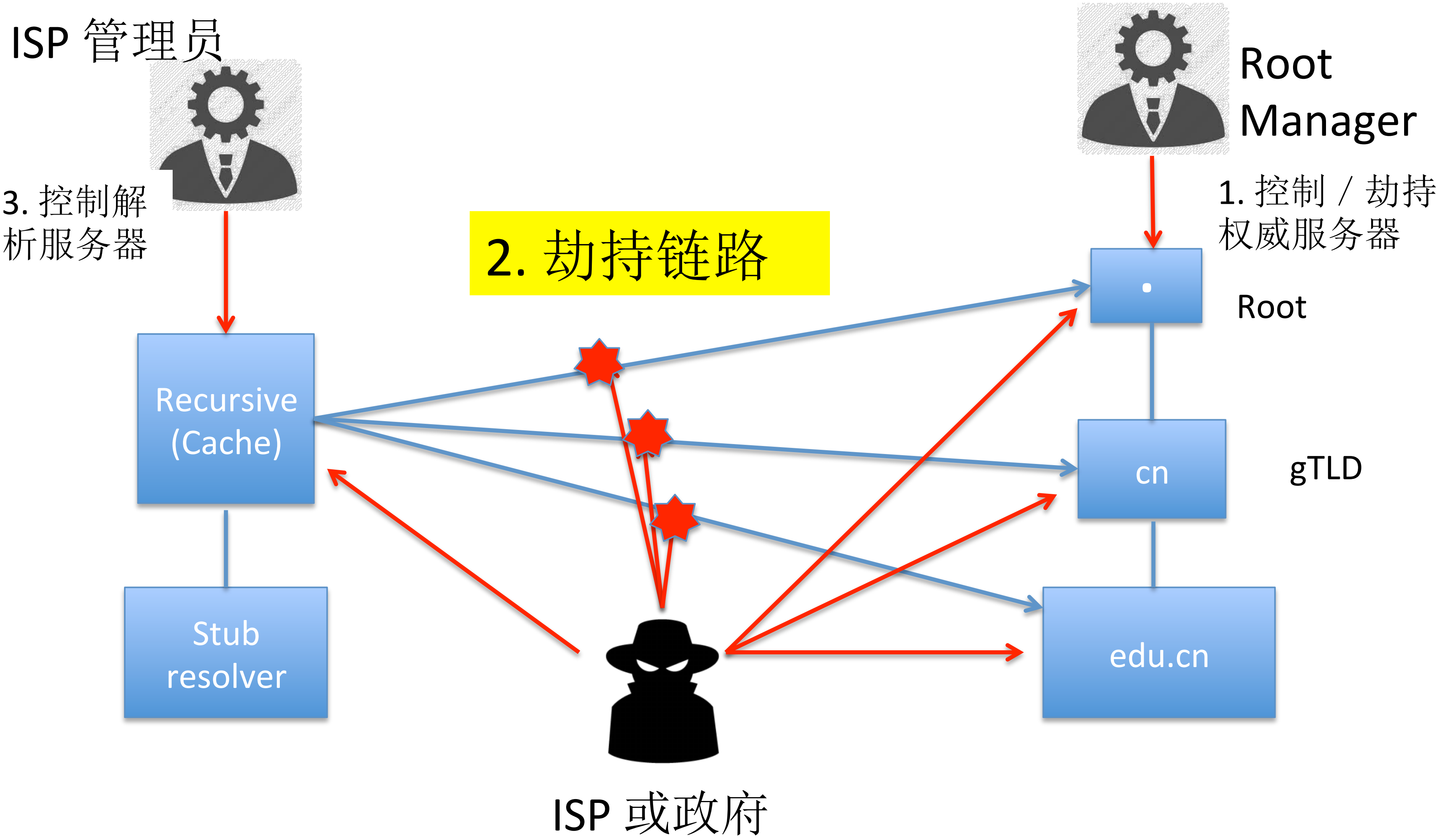
Copyright Notice

Summary

To remain a global network, the Internet requires the existence of a globally unique public name space. The DNS name space is a hierarchical name space derived from a single, globally unique root. This is a technical constraint inherent in the design of the DNS. Therefore it is not technically feasible for there to be more than one root in the public DNS. That one root must be supported by a set of coordinated root servers administered by a unique naming authority.

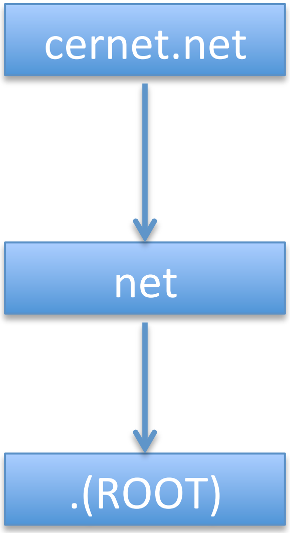
Put simply, deploying multiple public DNS roots would raise a very strong possibility that users of different ISPs who click on the same link on a web page could end up at different destinations, against the will of the web page designers.

We trust: Root, Link and local resolver



DNS Hijacking: 多少链路可以劫持?

为解析cernet.net，假设递归解析服务器的缓存是空的，看似只需知道ROOT, NET的IP地址：

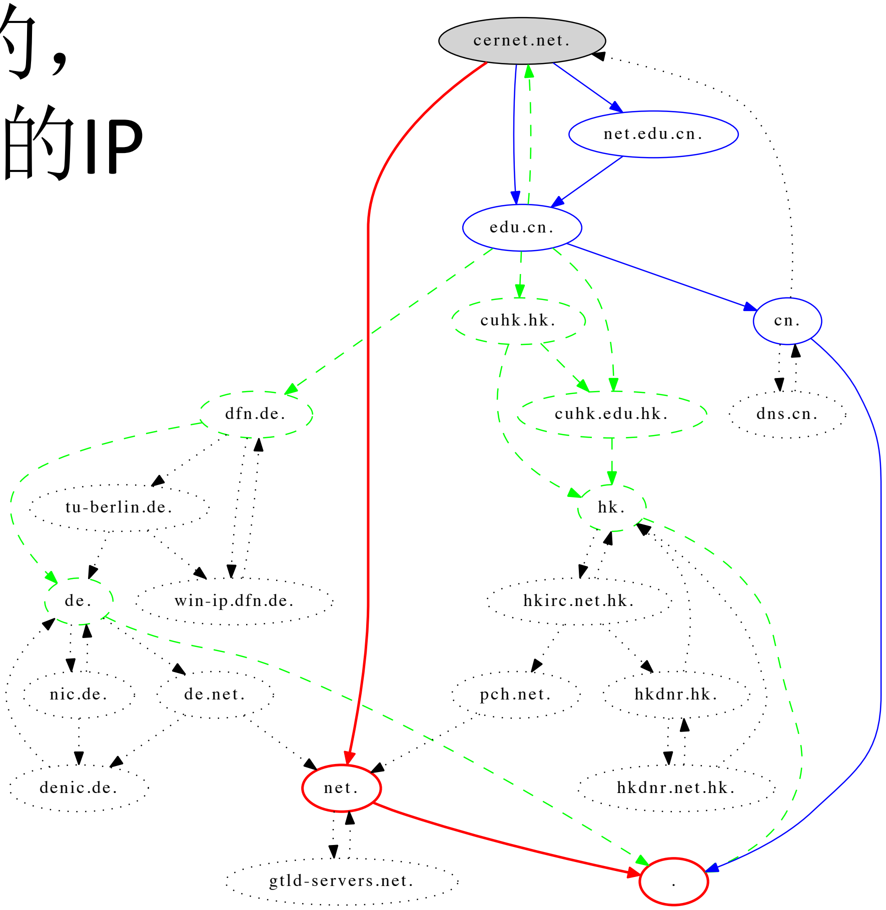


cernet.net

net

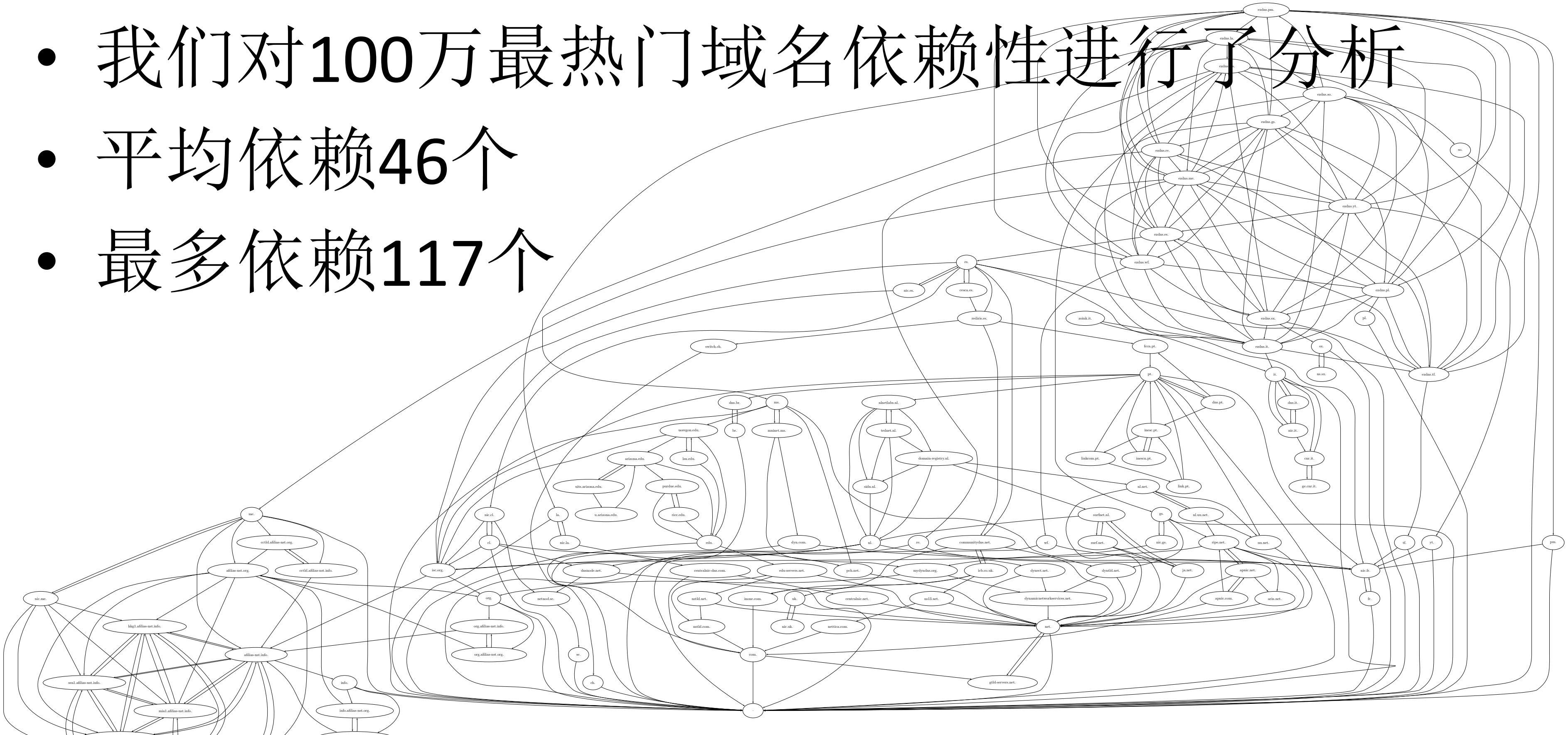
.(ROOT)

实际情况：



每个所依赖域名的解析路径被劫持，都会达到劫持的效果

- 域名A依赖B，表示解析A之前可能需要首先解析B
- 我们对100万最热门域名依赖性进行了分析
- 平均依赖46个
- 最多依赖117个



[dns-operations] Odd behaviour on one node in I root-server (facebook, youtube & twitter)

Hi there! A local ISP has told us that there's some strange behavior with at least one node in i.root-servers.net (traceroute shows mostly China) It seems that when you ask A records for facebook, youtube or twitter, you get an IP and not the referral for .com

It doesn't happen every time, but we have confirmed this on 4 different connectivity places (3 in Chile, one in California)

This problem has been reported to Autonomica/Netnod but I don't know if anyone else is seeing this issue.

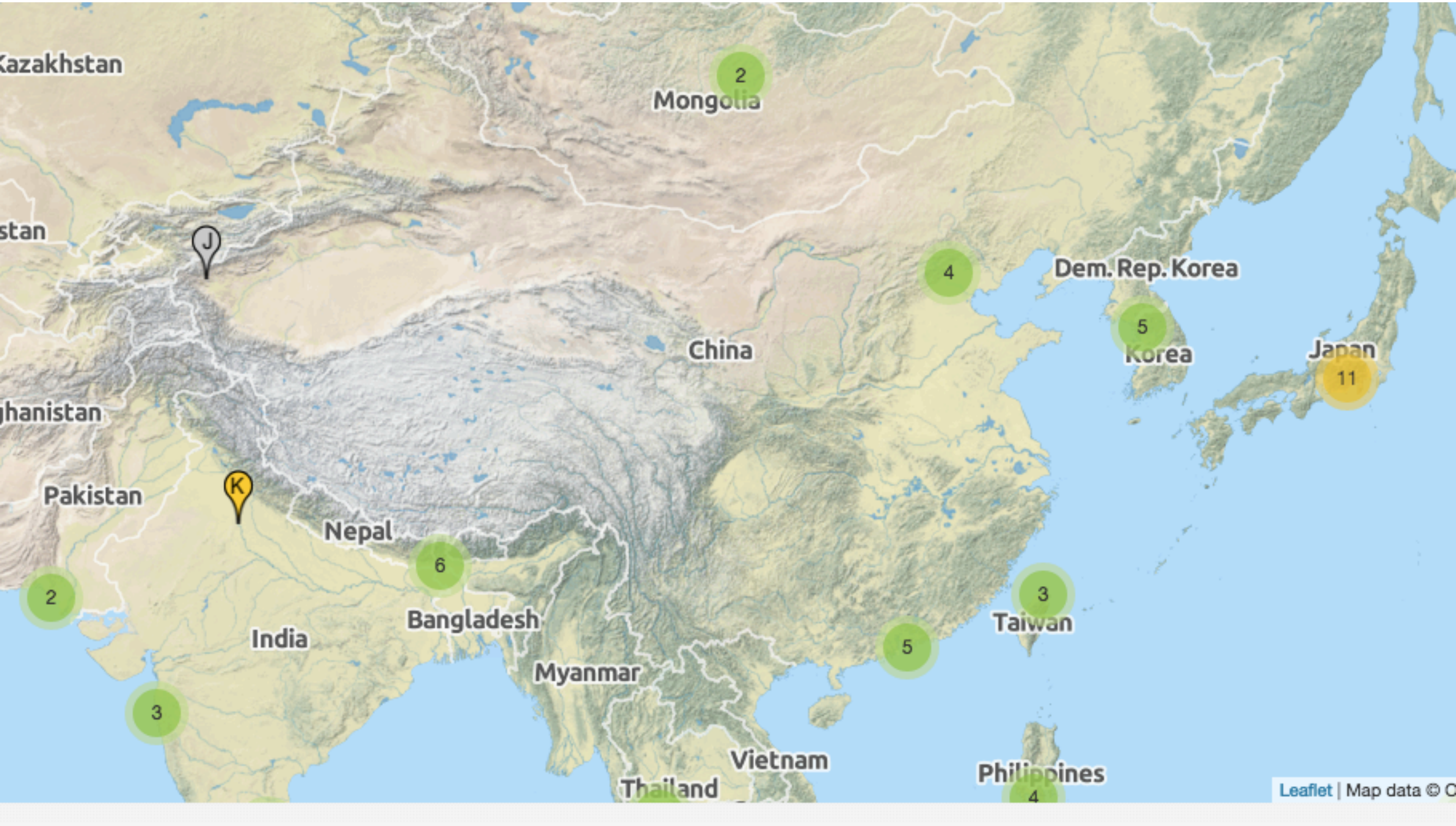
This is an example of what are we seeing:

```
$ dig @i.root-servers.net  www.facebook.com  A ;
….
ANSWER SECTION: www.facebook.com. 86400 IN A 8.7.198.45
```

Mauricio Vergara Ereche
Santiago CHILE

https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005260.html

Root Servers in China



2013: 4(BJ) + 5(HK) + 3(TW) = 12

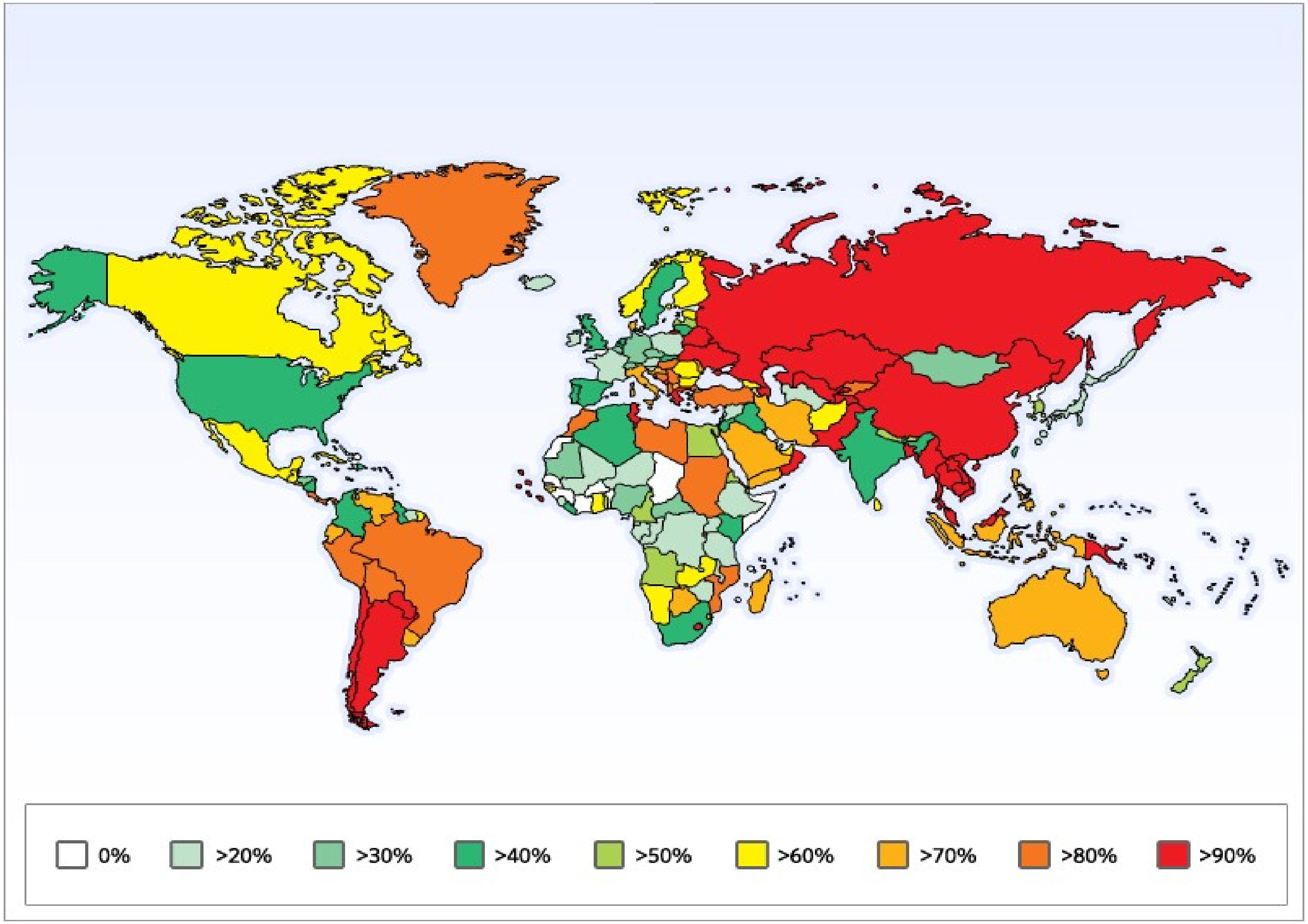
2013: 4(BJ) + 5(HK) + 3(TW) = 12

Explanation

- The global advertisements for 192.36.148.0/24 include AS 29216 (I-root) and AS 8674 and then traversed several Chinese ASNs (in red).
- Inbound packets on this path would traverse AS 10026 (PacNet), AS 7497 (Computer Network Information Center), AS 24151 (CNNIC) before reaching AS 29216 and 8674:
  - […] 10026 7497 7497 24151 8674 29216
- Peers selecting this path would clearly be sending their queries to the Beijing node.
- The results reported by Mauricio Vergara Ereche on the dns-operations mailing list are consistent with GFW behavior.

http://www.renesys.com/tech/presentations/pdf/DNS-Tampering-and-Root-Servers.pdf

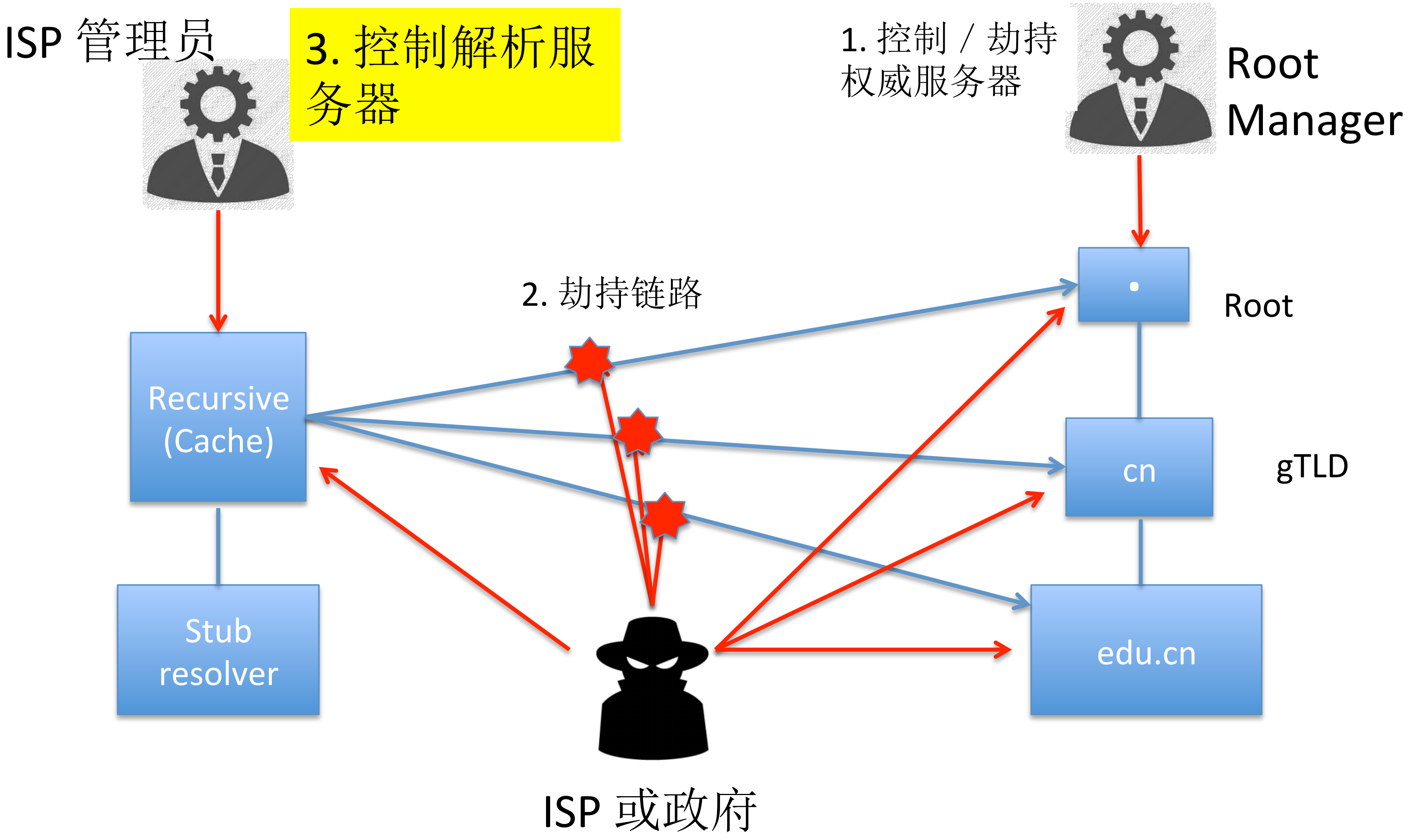
Who could have been affected?



Netnod serves Chinese market

- Netnod intends the Beijing node to be globally visible.
- Netnod employs TSIG and routinely checks serial numbers of the data at each of their root server instances against Verisign/IANA root zone data to ensure validity.
- The tampering of replies from the Beijing I-root was completely consistent with and almost irrefutably the GFW.
- Netnod withdrew their anycasted routes until their host (CNNIC) could secure assurances that the tampering would not recur.
- Netnod serves a large Internet user base in China and its Beijing node is one of its top 5 busiest instances.

We trust: Root, Link and local resolver



如果你可以控制解析服务器...

From:Paul A Vixie[SMTP:paul@vix.com]
Sent:Thursday, October 31, 1996 12:56 PM
To:newdom@vrx.net
Subject:requirements for participation

I have told the IANA and I have told InterNIC -- now I'll tell you kind folks.

If IANA's proposal stagnates past January 15, 1997, without obvious progress and actual registries being licensed or in the process of being licensed, I will declare the cause lost. At that point it will be up to a consortium of Internet providers, probably through CIX if I can convince them to take up this cause, to tell me what I ought to put into the "**root.cache**" file that I ship with BIND.

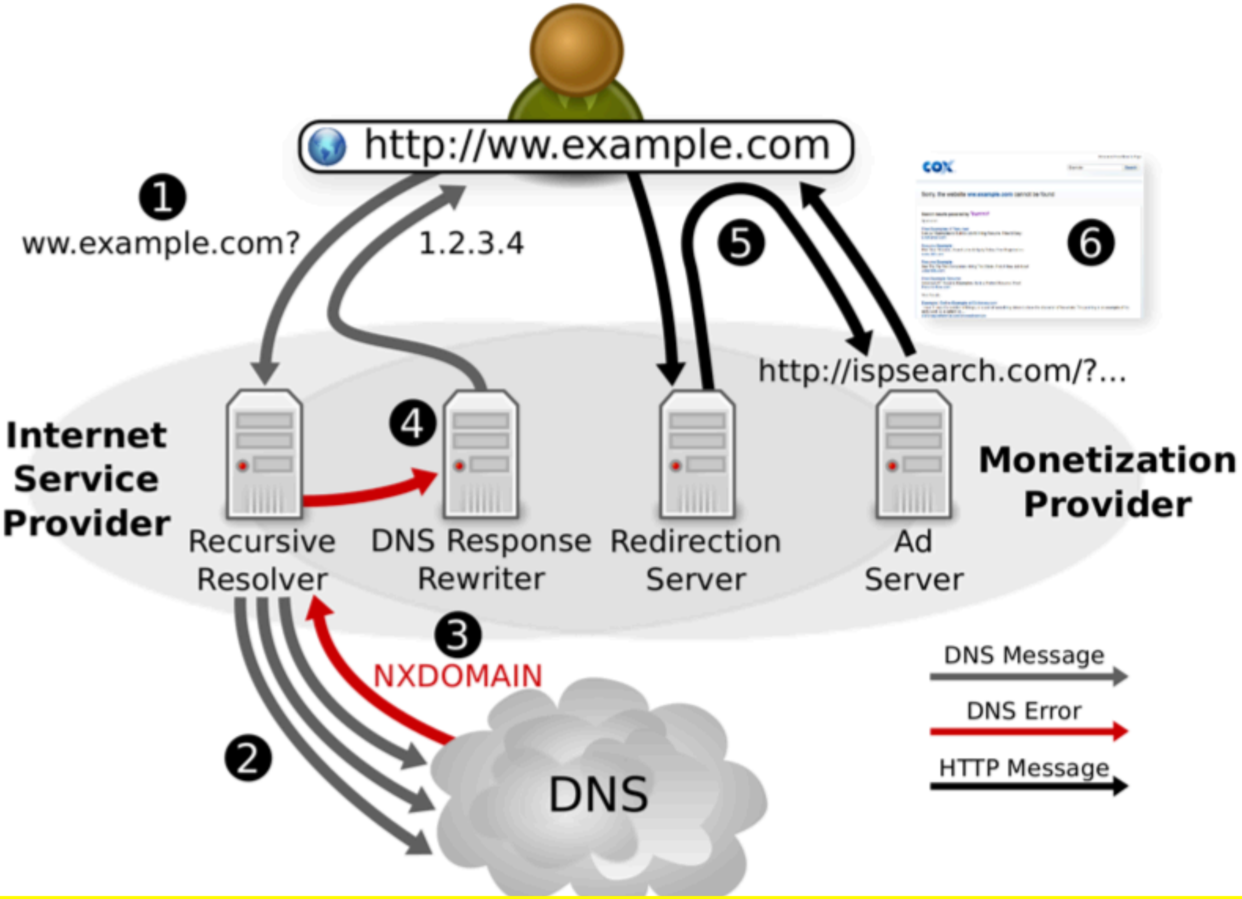
Paul Vixie
Author of BIND
Chair of SAC of ICANN

ORSN (2002-2008, 2013-)
(Open Root Server Network)

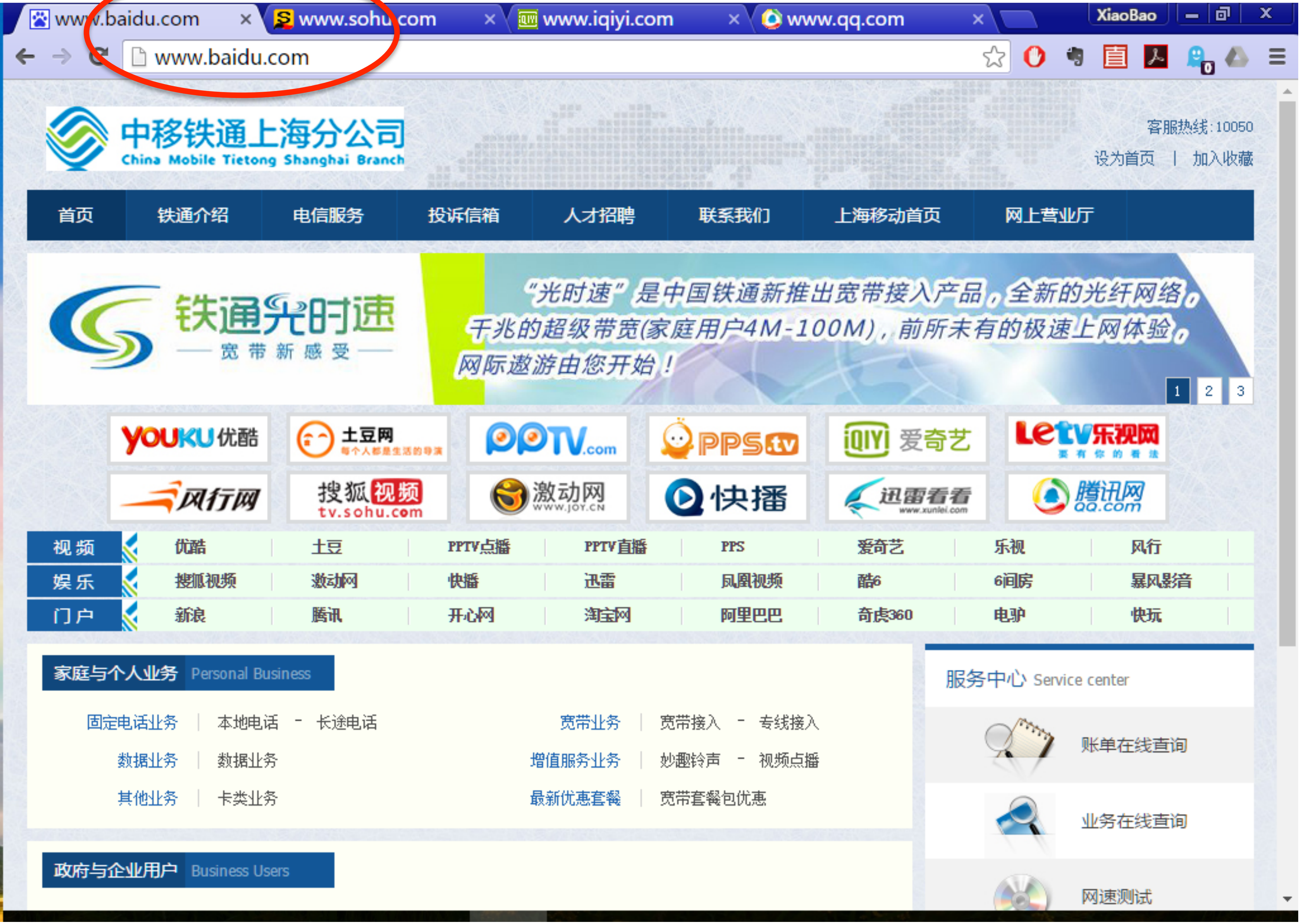
As a long time supporter of the universal namespace operated by IANA, it may come as a surprise that I have joined the Open Root Server Network project (ORSN). I'll try to explain what's going on and what it all means.

https://www.ietf.org/mail-archive/text/ietf/1996-11

有些ISP利用解析服务NXDOMAIN赚钱



N. Weaver, V. Paxson, and C. Kreibich, “Redirecting DNS for Ads and Profit,” presented at the Proceedings of the 20th USENIX Security Symposium“s Workshop on Free and Open Communications on the Internet (FOCI ”11), 2011.



中移铁通上海分公司
China Mobile Tietong Shanghai Branch

客服热线:10050
设为首页 | 加入收藏

首页 铁通介绍 电信服务 投诉信箱 人才招聘 联系我们 上海移动首页 网上营业厅

铁通光时速
— 宽带新感受 —

"光时速"是中国铁通新推出宽带接入产品，全新的光纤网络，千兆的超级带宽(家庭用户4M-100M)，前所未有的极速上网体验，网际遨游由您开始！

1 2 3

视 频	优酷	土豆	PPTV点播	PPTV直播	PPS	爱奇艺	乐视	风行
娱 乐	搜狐视频	激动网	快播	迅雷	凤凰视频	酷6	6间房	暴风影音
门 户	新浪	腾讯	开心网	淘宝网	阿里巴巴	奇虎360	电驴	快玩

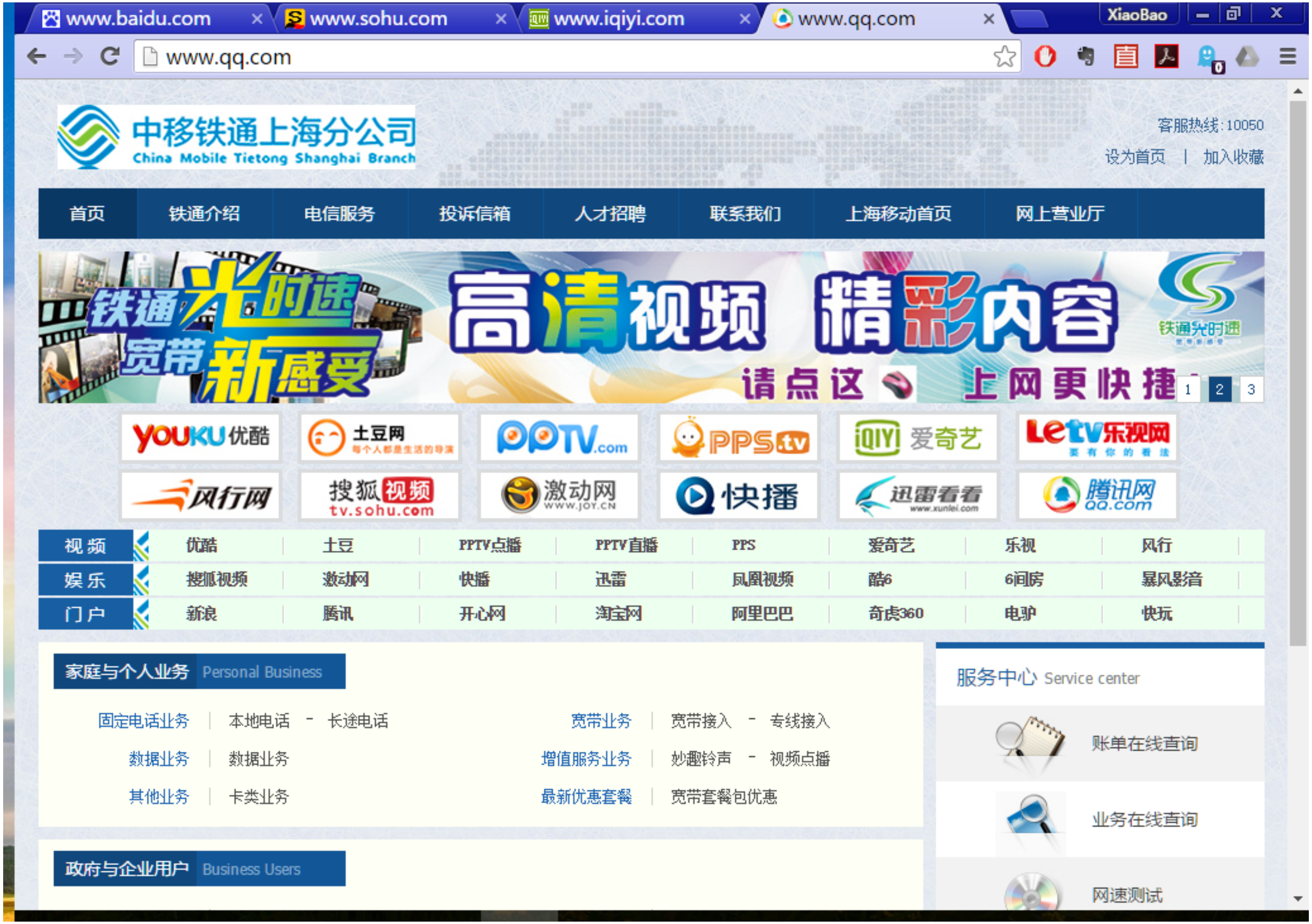
家庭与个人业务 Personal Business

固定电话业务 | 本地电话 - 长途电话
宽带业务 | 宽带接入 - 专线接入
数据业务 | 数据业务
增值服务业务 | 妙趣铃声 - 视频点播
其他业务 | 卡类业务
最新优惠套餐 | 宽带套餐包优惠

政府与企业用户 Business Users

服务中心 Service center

账单在线查询
业务在线查询
网速测试



中移铁通上海分公司
China Mobile Tietong Shanghai Branch

客服热线：10050

设为首页 | 加入收藏

首页 铁通介绍 电信服务 投诉信箱 人才招聘 联系我们 上海移动首页 网上营业厅

视 频	优酷	土豆	PPTV点播	PPTV直播	PPS	爱奇艺	乐视	风行
娱 乐	搜狐视频	激动网	快播	迅雷	凤凰视频	酷6	6间房	暴风影音
门 户	新浪	腾讯	开心网	淘宝网	阿里巴巴	奇虎360	电驴	快玩

家庭与个人业务 Personal Business

固定电话业务	本地电话 - 长途电话	宽带业务	宽带接入 - 专线接入
数据业务	数据业务	增值服务业务	炒趣铃声 - 视频点播
其他业务	卡类业务	最新优惠套餐	宽带套餐包优惠

政府与企业用户 Business Users

服务中心 Service center

账单在线查询

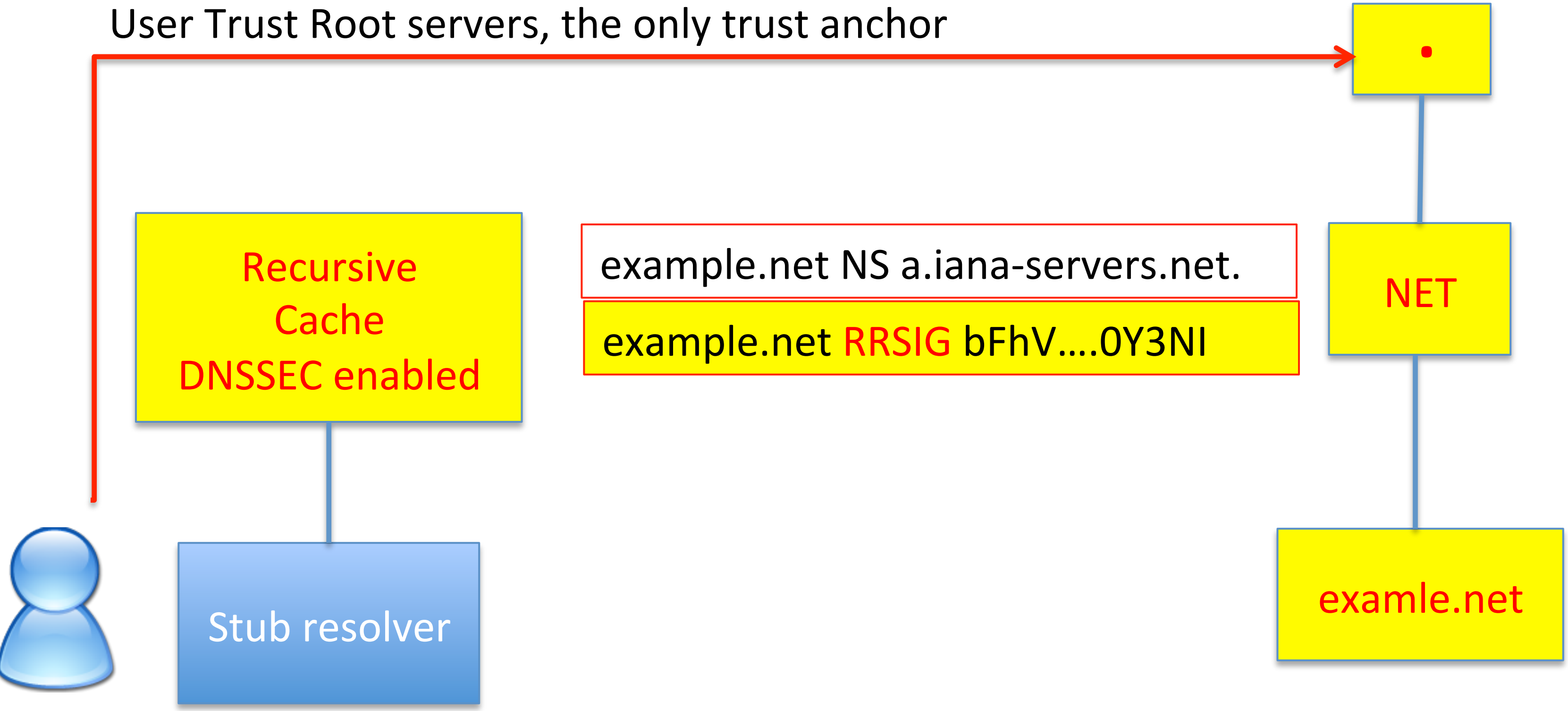
业务在线查询

网速测试

DNSSEC：防止链路劫持、缓存污染

- Clients(resolvers) validate the signature with their public keys

- Servers sign all the DNS records with their private Keys


User Trust Root servers, the only trust anchor
.
Recursive Cache DNSSEC enabled
example.net NS a.iana-servers.net.
example.net RRSIG bFhV....0Y3NI
NET
Stub resolver
examle.net

Paul Vixie, June 1995:

> This sounds simple but it has deep reaching consequences in both the protocol and the implementation—which is why it's taken more than a year to choose a security model and design a solution. We expect it to be another year before DNSSEC is in wide use on the leading edge, and at least a year after that before its use is commonplace on the Internet.

BIND 8.2 blurb, March 1999:

> [Top feature:] Preliminary DNSSEC.

BIND 9 blurb, September 2000:

> [Top feature:] DNSSEC.

Paul Vixie, November 2002:

> We are still doing basic research on what kind of data model will work for DNS security. After three or four times of saying "NOW we've got it, THIS TIME for sure" there's finally some humility in the picture . . . "Wonder if THIS'll work?" . . .
>
> It's impossible to know how many more flag days we'll have before it's safe to burn ROMs . . . It sure isn't plain old SIG+KEY, and it sure isn't DS as currently specified. When will it be? We don't know. . . .
>
> 2535 is already dead and buried. There is no installed base. We're starting from scratch.

DNSSEC
Trusted Community Representatives

Crypto Officers for the US East Coast Facility

- Alain Aina, BJ
- Anne-Marie Eklund Löwinder, SE
- Frederico Neves, BR
- Gaurab Upadhaya, NP
- Olaf Kolkman, NL
- Robert Seastrom, US
- Vinton Cerf, US

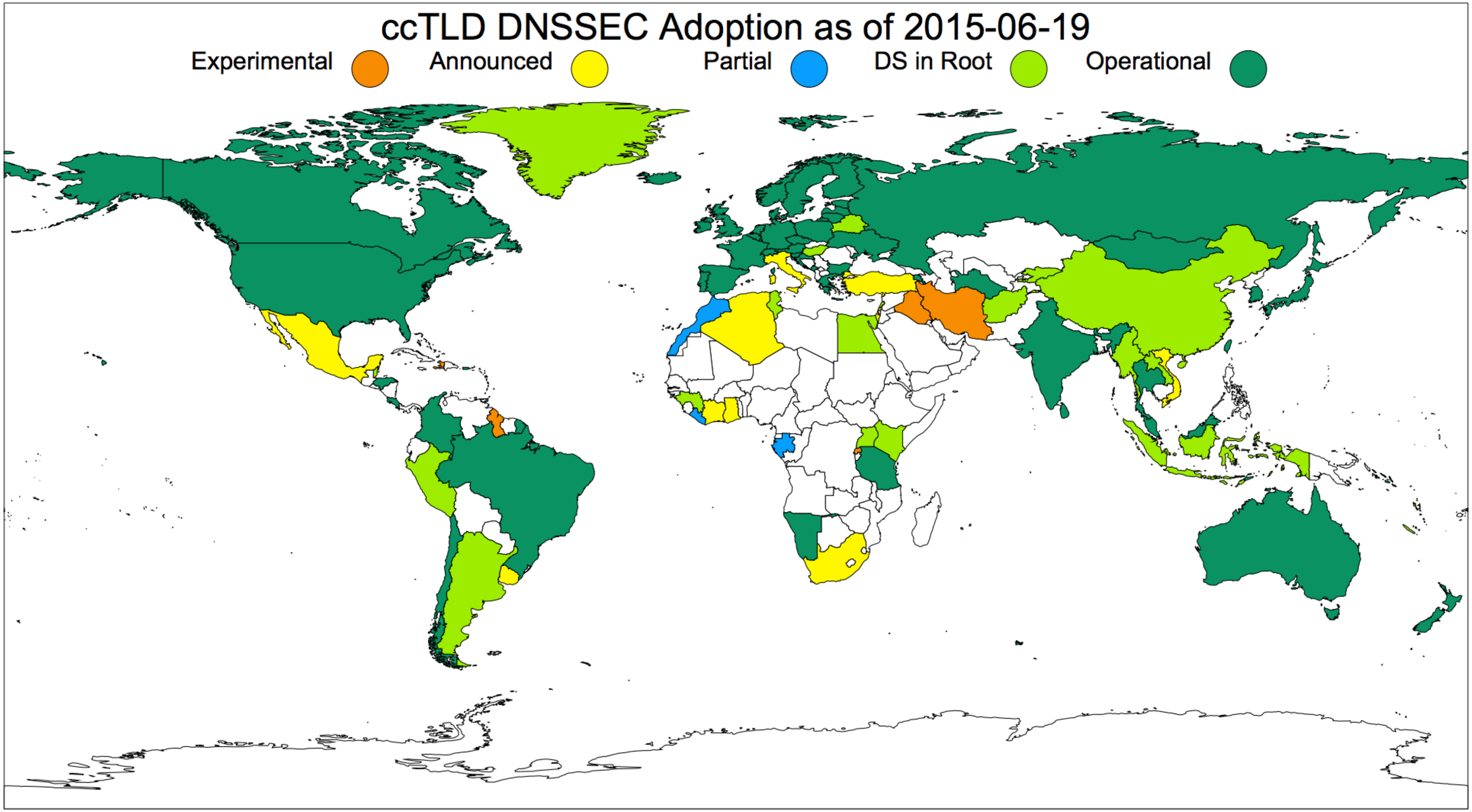
Crypto Officers for the US West Coast Facility

- Andy Linton, NZ
- Carlos Martinez, UY
- Dmitry Burkov, RU
- Edward Lewis, US
- João Luis Silva Damas, PT
- Masato Minda, JP
- Subramanian Moonesamy, MU

Recovery Key Share Holders

- Bevil Wooding, TT
- Dan Kaminsky, US
- Jiankang Yao, CN
- Moussa Guebre, BF
- Norm Ritchie, CA
- Ondřej Surý, CZ
- Paul Kane, UK

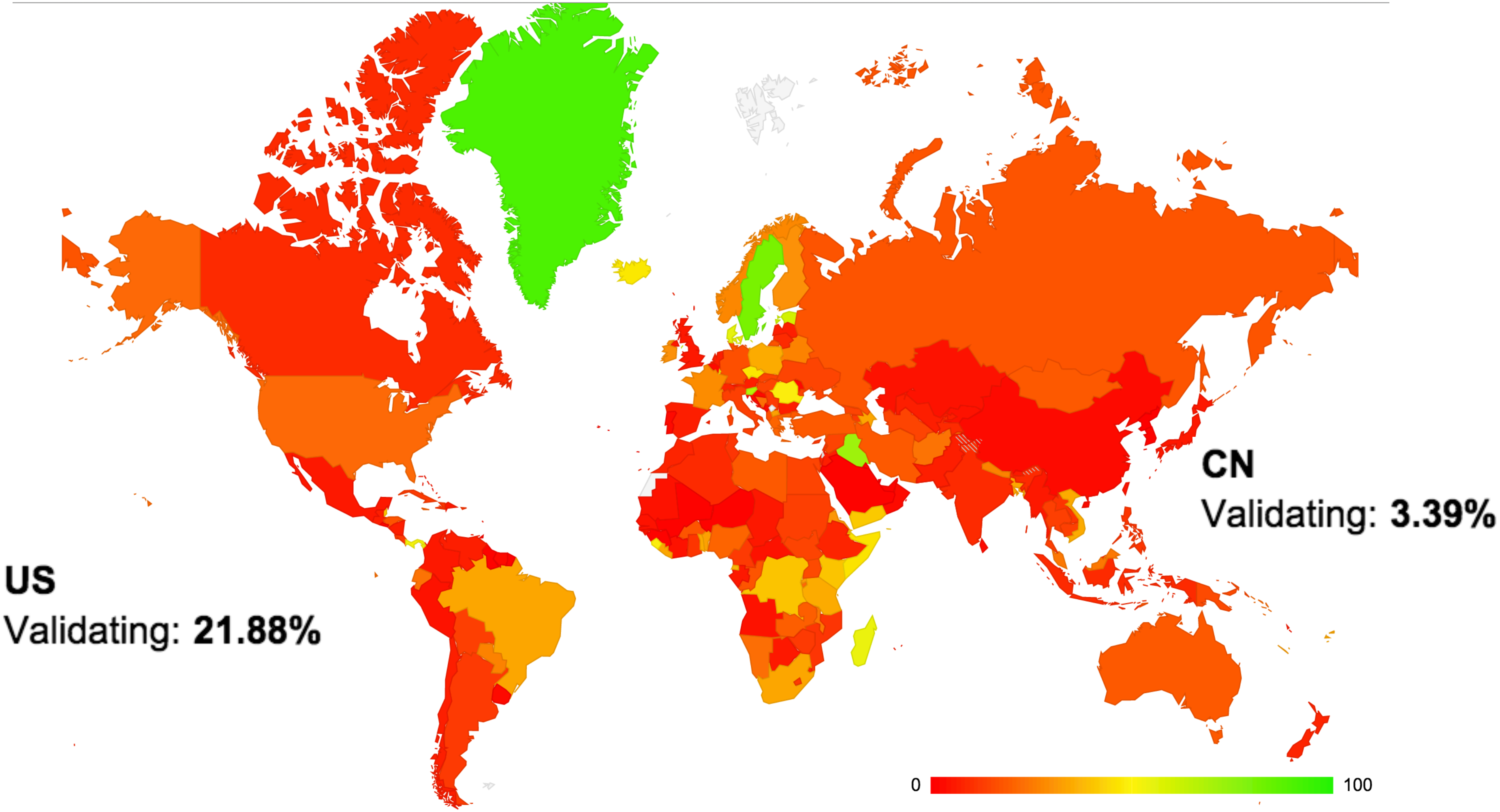
http://www.root-dnssec.org/index.html



ccTLD DNSSEC Adoption as of 2015-06-19

Experimental -- Internal experimentation announced or observed (9):	GY HK HT IQ IR MS MU RW TO
Announced -- Public commitment to deploy (11):	CI DZ GH IL IT MX SG TR UY VN ZA
Partial -- Zone is signed but not in operation (no DS in root) (4):	GA LR MA VC
DS in Root -- Zone is signed and its DS has been published (34):	AD AF AG AR AW BY BZ CC CN EG FO GD GI GL GN HU ID KE KG KI KY LA LB LC MM NC NU PE PW SJ TN TV UG VU
Operational -- Accepting signed delegations and DS in root (67):	AC AM AT AU BE BG BR CA CH CL CO CR CX CZ DE DK EE ES FI FR GR GS HN HR IE IN IO IS JP KR LI LK LT LU LV ME MN MY NA NF NL NO NZ PL PM PR PT RE RU SB SC SE SH SI SX TF TH TL TM TT TW TZ UA UK US WF YT

DNSSEC Validation Rate by country (%)



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

DNSSEC部署现状意味着什么？

- 尽管权威服务器.CN已经签名，但是绝大多数中国的解析服务器仍然不做验证
- 防止假冒的权威服务器、防止链路上的劫持、缓存污染攻击，还有漫长的路

- 你能指望劫持你DNS的ISP部署DNSSEC验证吗？
- 在终端上做DNS解析、验证？

Outline

- Trust models and trust anchors
- In Routing, We Trust…
- In DNS, We Trust …
- In Web PKI, We Trust（西安交大, 4/26， 直播http://inforsec.org)

In WHAT, we TRUST ?

Q & A

duanhx@tsinghua.edu.cn