互联网基础设施信任模型与威胁
Trust Model and Threats of Internet Infrastructure

段海新

duanhx@tsinghua.edu.cn

Tsinghua University
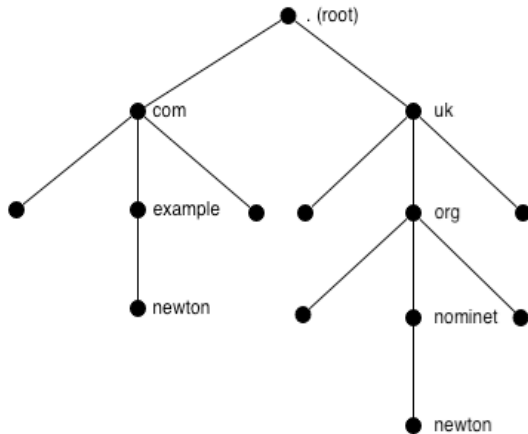
2014年10月，中国网络安全大会

提纲

◆ 基础设施的信任模型
- BGP路由劫持和 RPKI
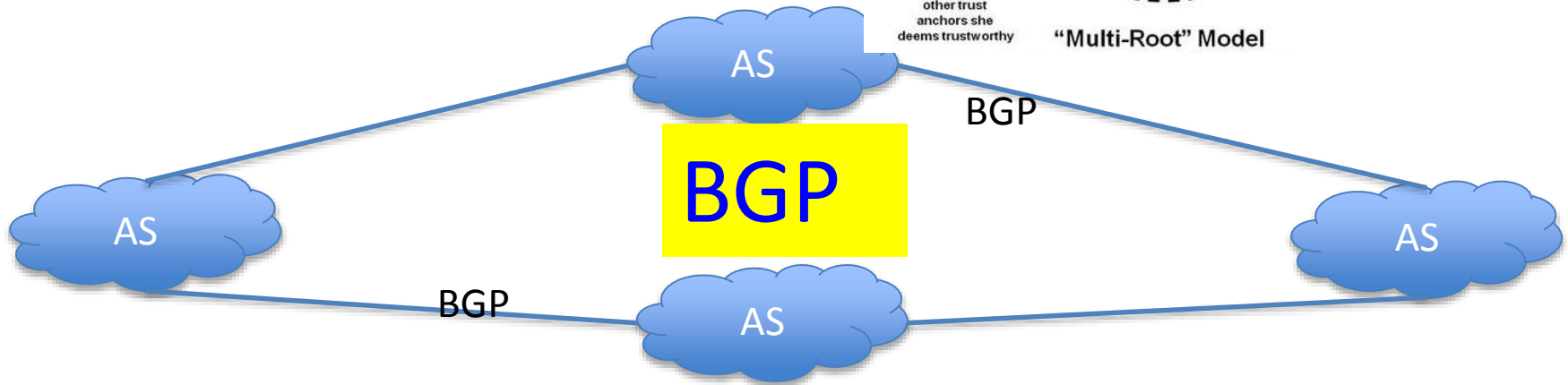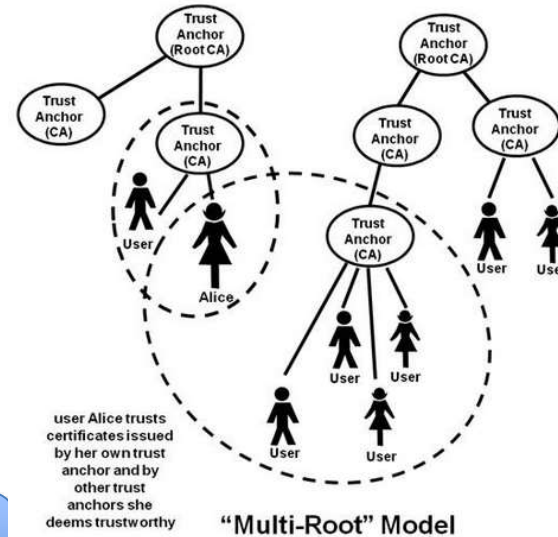- DNS 污染和 DNSSEC
- PKI 问题和建议
- 总结

互联网安全基础设施

Applications

DNS

PKI

"Multi-Root" Model

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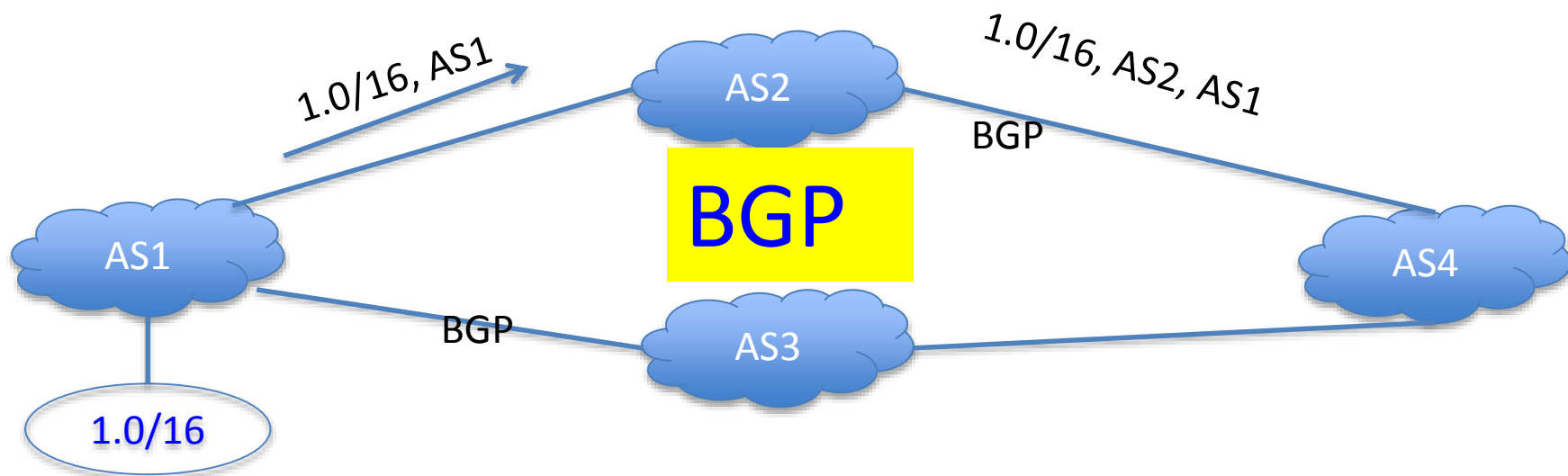anchors she
deems trustworthy
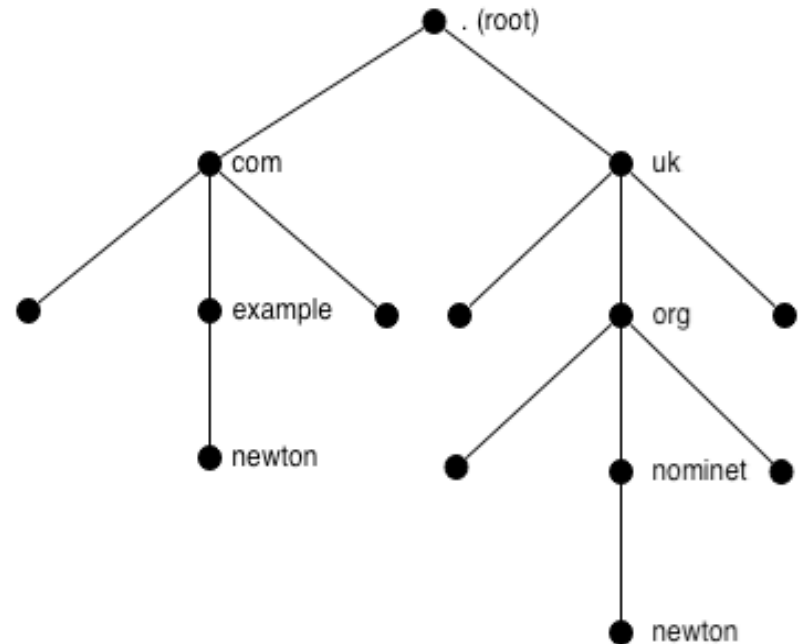
AS

BGP

BGP

AS

AS

BGP

AS

BGP的信任模型：Peer-Peer

- 目前的BGP-4对路由公告无密码机制验证
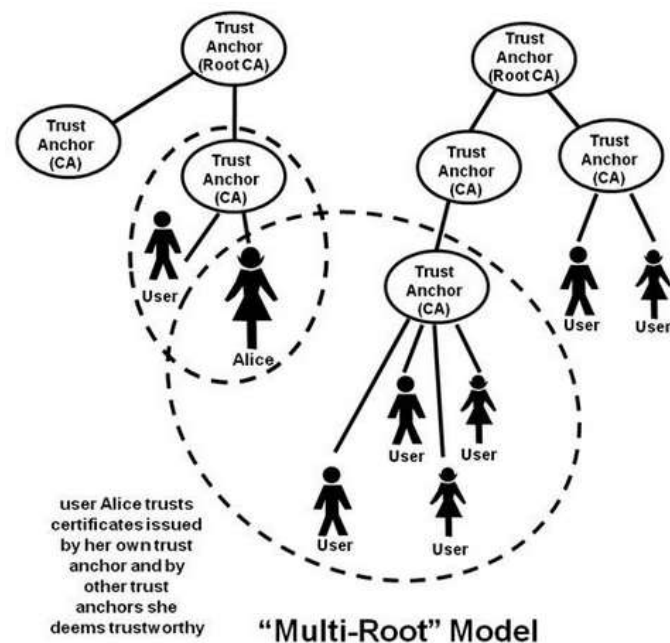- 对等实体之间相互信任（**Peer-Peer**）
- 没有集中的信任权威，完全的分布式

DNS的信任模型：树形结构

- 树形、层次授权，唯一信任权威（root）
- 子域名在授权空间中比父节点更有权威
- 目前DNS没有密码机制保护
  信息的真实和完整性

PKI/CA的信任模型：森林状结构

- 浏览器预置上百个可信Root CA，相互独立
  - VeriSign，CNNIC, Google, Apple…
- 每个Root CA可签二级CA证书，形成信任树
- 每个CA可以为任何网站
  签发证书，都被认为是
  可信的

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

"Multi-Root" Model

提纲

- 基础设施的信任模型
  ◆ BGP路由劫持和 RPKI
- DNS 污染和 DNSSEC
- PKI 问题和建议
- 总结

BGP prefix Hijacking incidents

- April 1997: The "AS 7007 incident"
- December 24, 2004: TTNet in Turkey hijacks the Internet
- May 7, 2005: Google's May 2005 Outage
- January 22, 2006: Con-Edison hijacks big chunk of the Internet
- February 24, 2008: Pakistan's attempt to block YouTube
- November 11, 2008: The Brazilian ISP CTBC route leaked
- April 8, 2010: Chinese ISP hijacks the Internet
- February, 2014: Canadian ISP used to redirect data

YouTube Hijacked by Pakistan Telecom

Youtube: 208.65.152.0/22

Pakistan Telecom
Announce 208.65.153.0/24

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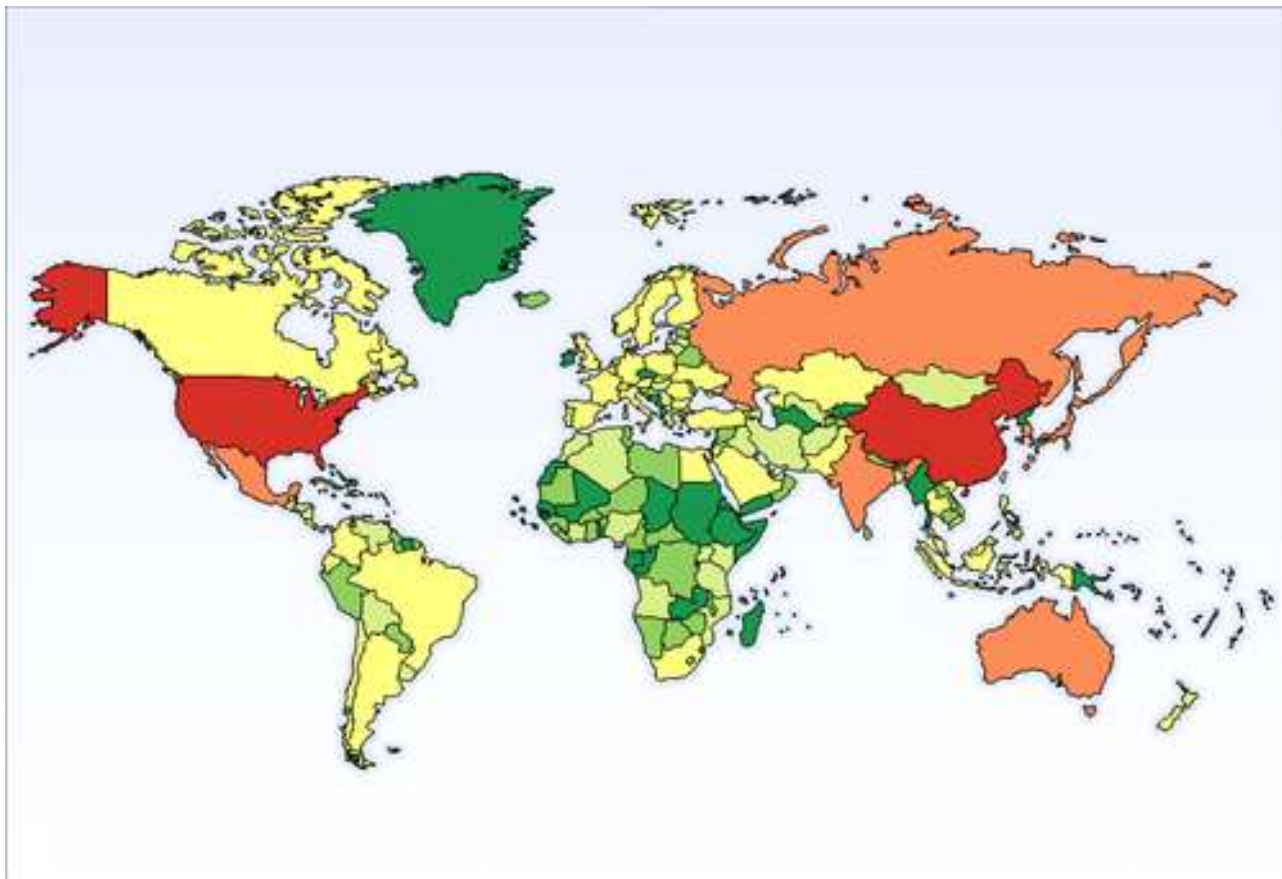
the scattershot nature of the hijack suggests a random mistake, not a deliberate attack on anyone in particular

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

通过路由劫持实现中间人攻击

The New Threat: Targeted Internet Traffic Misdirection

Traceroute Path 1: from **Guadalajara**, Mexico to **Washington**, D.C. via *Belarus*

http://www.renesys.com/2013/11/mitm-internet-hijacking/

RPKI(Resource PKI) and BGPSEC

- 通过密码技术实现路由前缀-来源的验证，防止路由劫持的攻击
  - X.509 certificate with RFC3779 extensions for IP resources (IP Address and ASN)
  - Route Origin Attestation (ROA) signed object
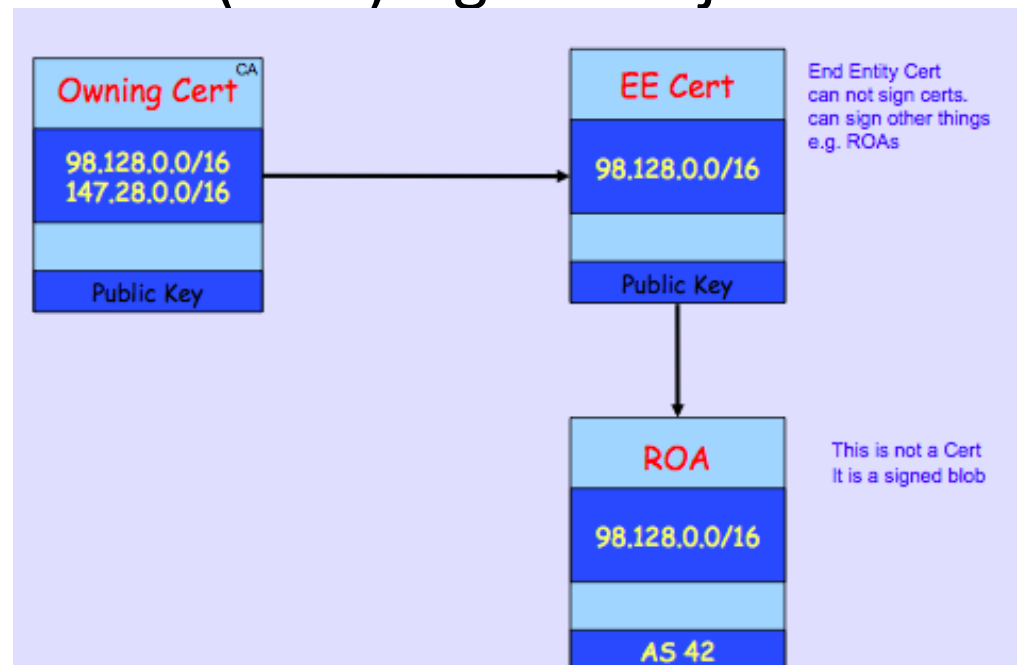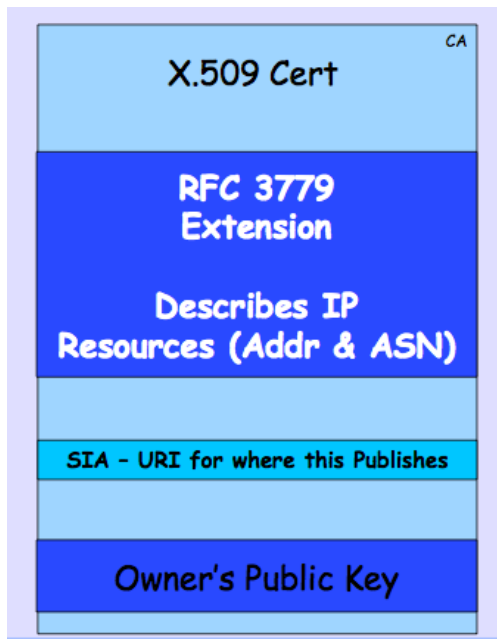
RPKI and BGPSEC Hierarchy

提纲
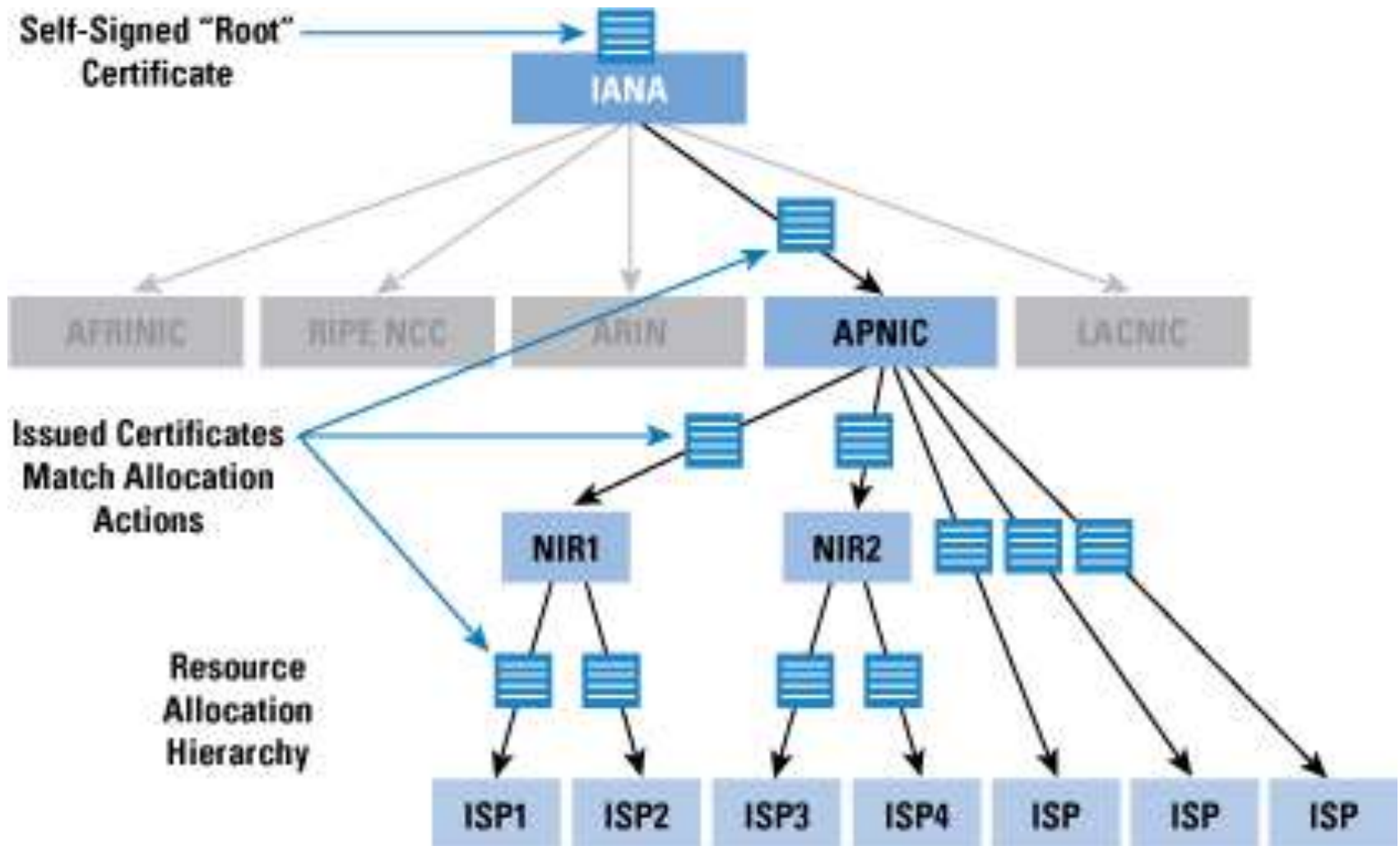
- 基础设施的信任模型
- BGP路由劫持和 RPKI
- DNS 污染和 DNSSEC
- PKI 问题和建议
- 总结

Incidents related to DNS

- 1990: Steven Bellovin Cache Poisoning
- 2002,2007: DDoS attacks against Root DNS
- 2008: Dan Kaminsky Bug
- 2009: 5/19 DNSPod&暴风影音导致大规模断网
- 2010: Baidu.com DNS hijack
- 2011: Massive DNS poisoning attacks in Brazil
- 2013: DDoS attack against Spamhaus
- 2013: 8/25 .CN DNS 大规模DDoS攻击
- 2014: 1/21 DNS Hijacking in China

Brazillian ISP's DNS cache poisoned 2011

"To access the new Google.com you need to install Google Defence"

Cache Poisoning: Kaminsky Bug,2008

srcPort, TXID

Q: Noexistent.example.edu A?

ns.example.edu

Recursive Resolver

?

srcPort, TXID
A: www.example.edu A 1.2.3.4
Authority: example.edu ns.example.edu
Additional: ns.example.edu 4.3.2.1

Ns.attacker.com

Noexistent.example.edu
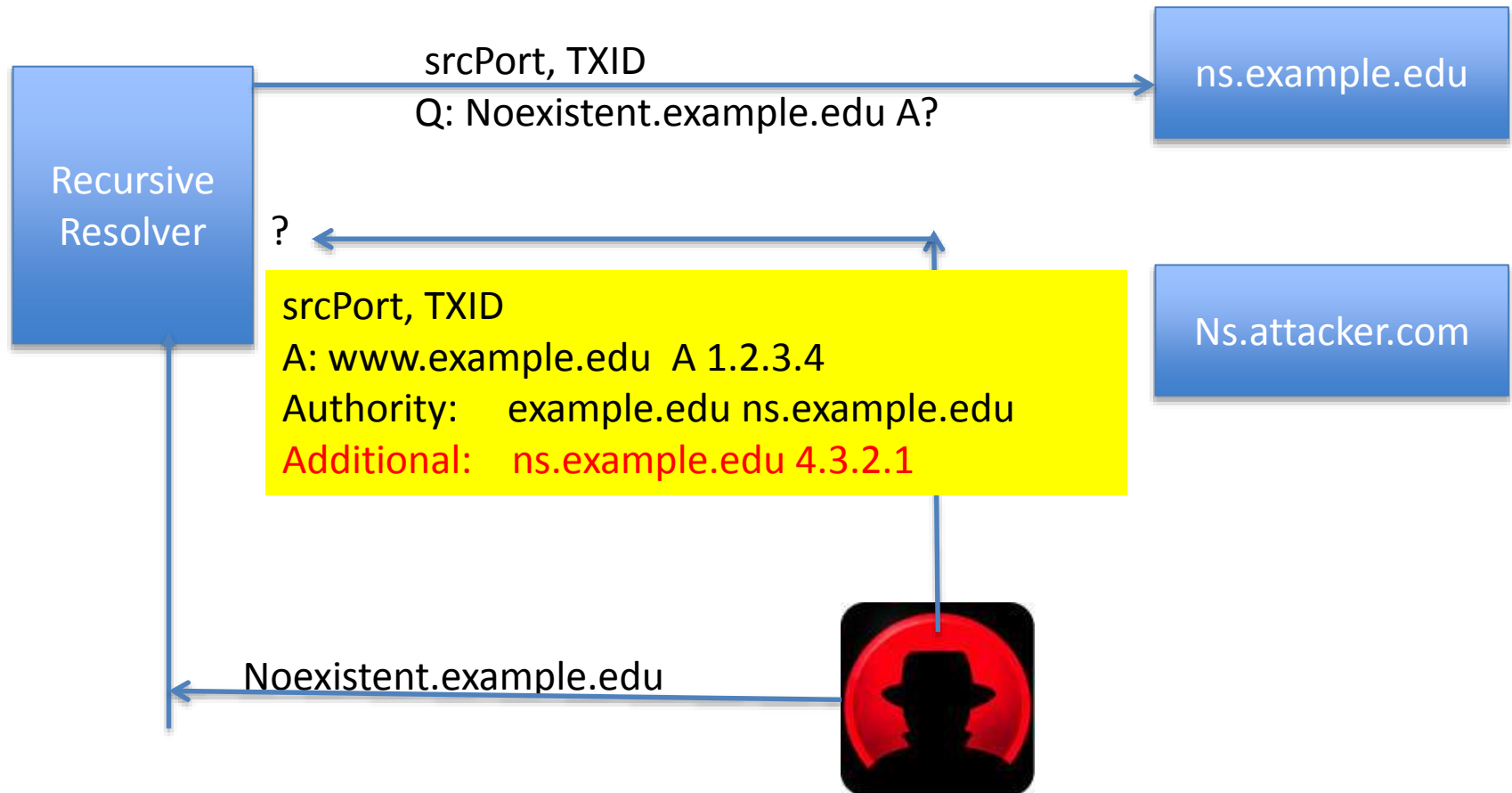
- In additional section, to poison a domain instead of an A record
- ith a predicted TXID, flood forged DNS replies with guessed srcPort (1/2^16) in a TTL
- How to improve the attack?

对DNS 解析的劫持可在多个环节
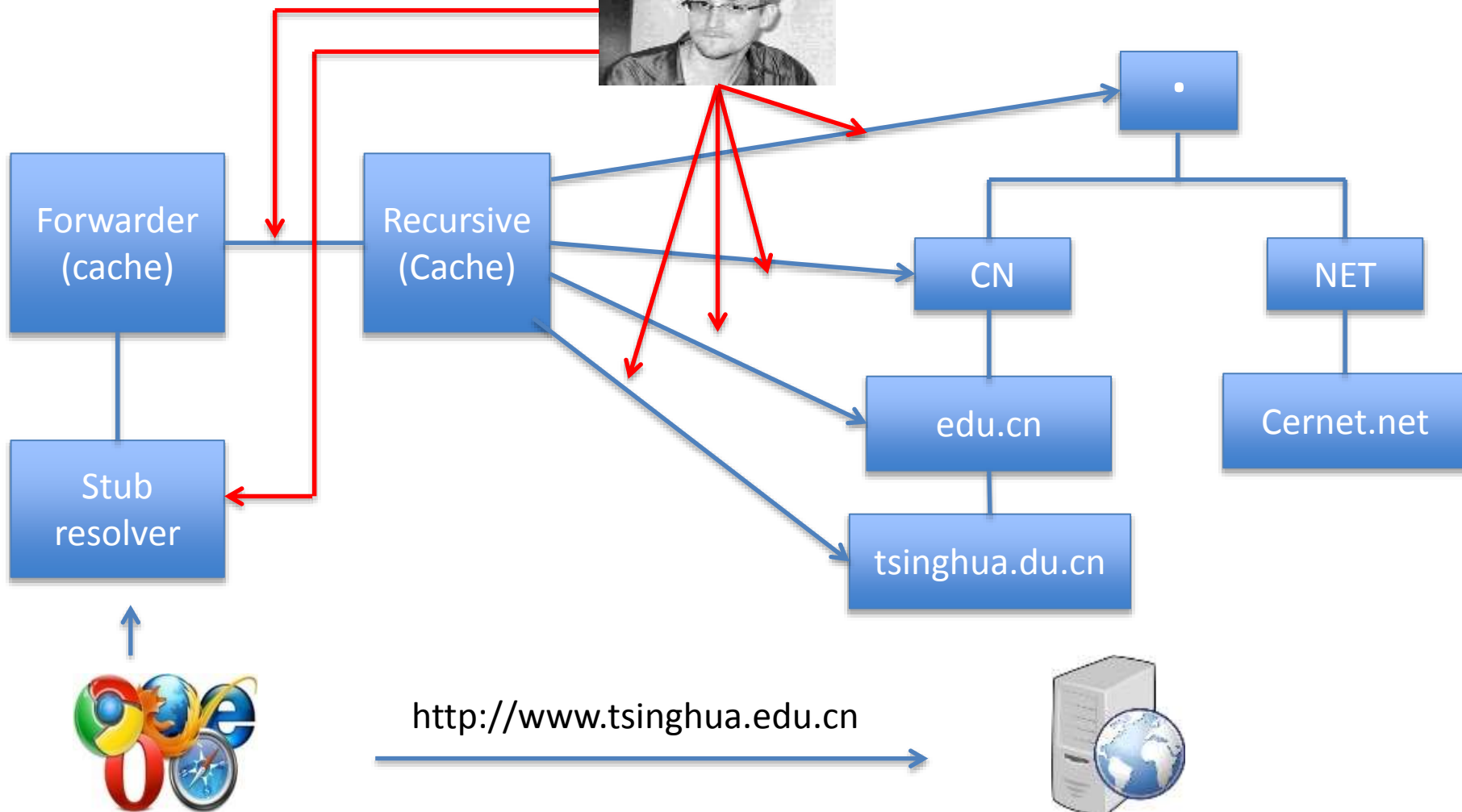
对DNS 解析的劫持可在多条路径
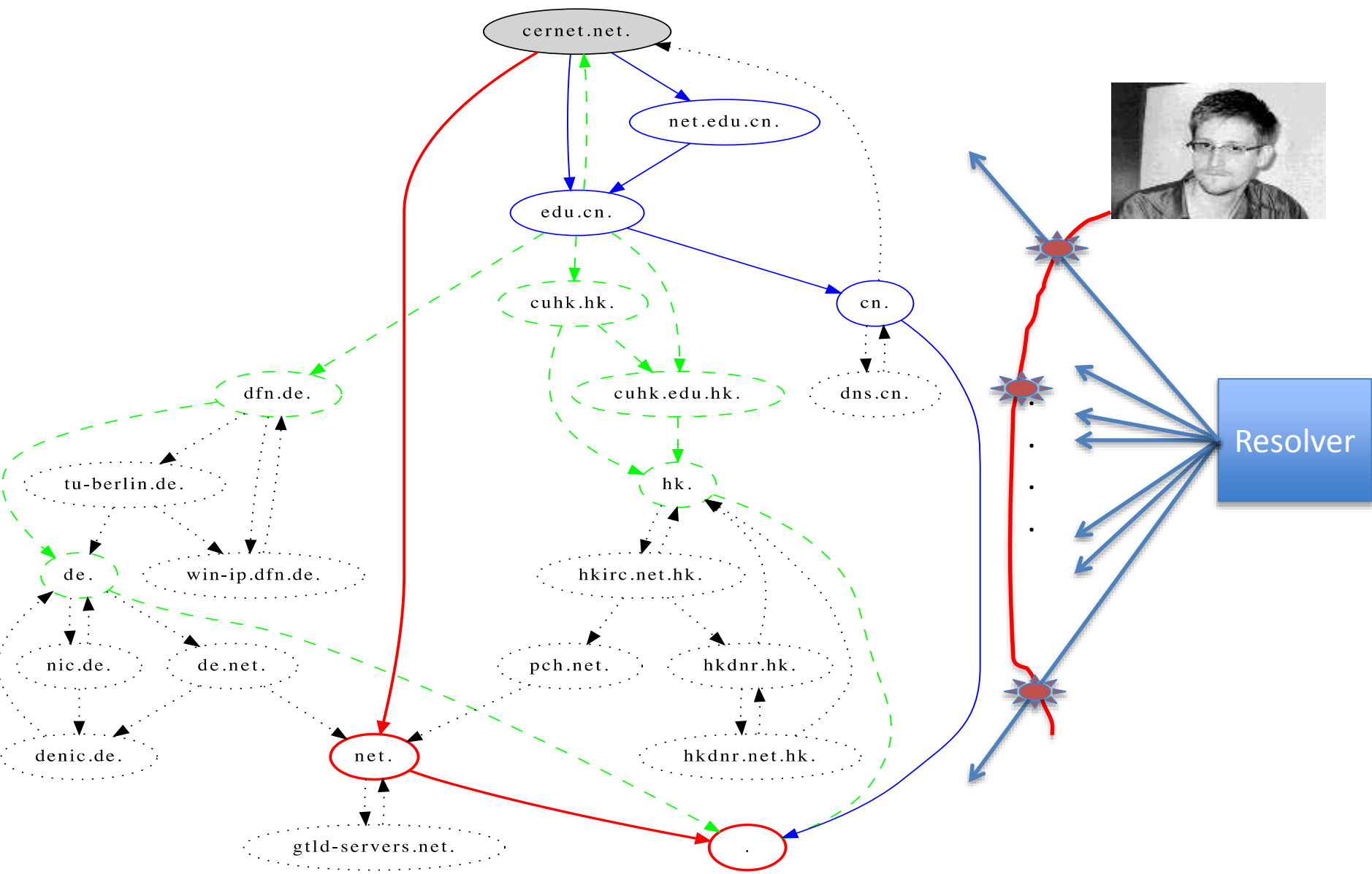
每个依赖的域名解析过程都可被劫持

- 域名A依赖B，**即**解析A可能需要先解析B
- 我们对100万最热门域名依赖性进行了分析
- 平均依赖46，最多依赖117
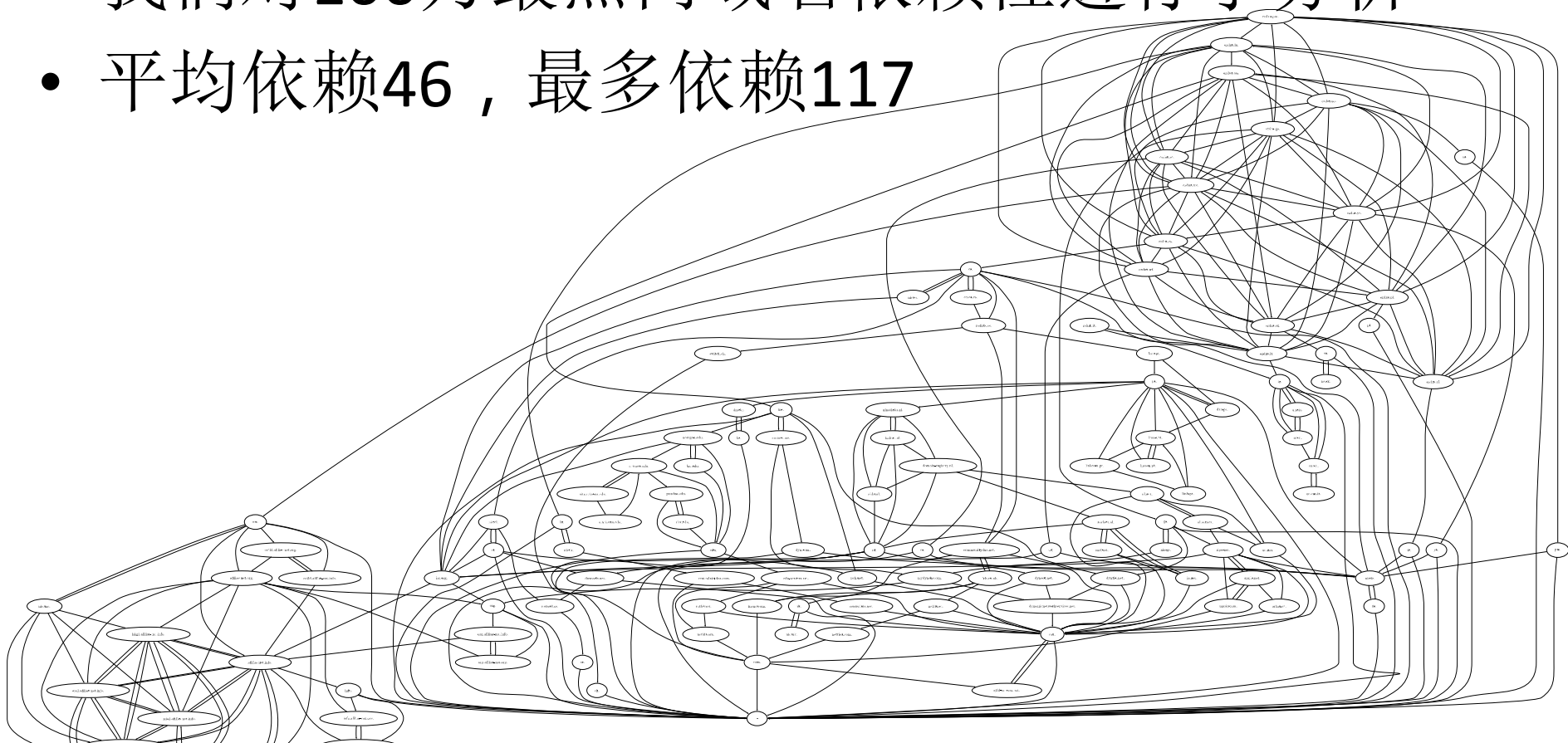
根域名服务器的世界分布
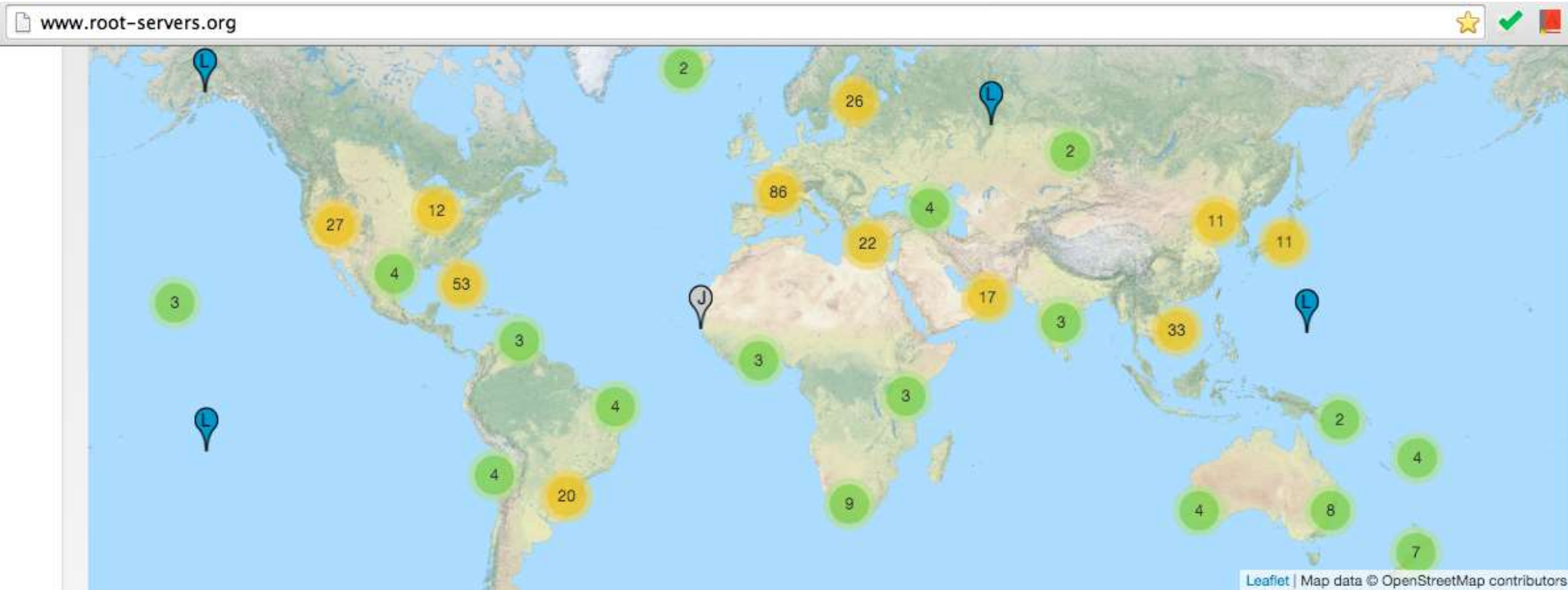
由于AnyCast，你的DNS请求去往那个ROOT并不确定

Root Servers

A   B   C   D   E   **F**   G   H   I   J   K   L   M

Operator: Internet Systems Consortium, Inc.   ⌂ Homepage   👥 Peering Policy   ✉ Contact Email

Locations: **Sites: 57**

📍 Amsterdam, NL   📍 Atlanta, US   📍 Auckland, NZ   📍 Barcelona, ES   📍 Beijing, CN   📍 Brisbane, AU   📍 Buenos Aires, AR   📍 Cairo, EG   📍 Caracas, VE

📍 Chennai, IN   📍 Chicago, US   📍 Dar es Salaam, TZ   📍 Dhaka, BD   📍 Dubai, AE   📍 Frankfurt, DE   📍 Hong Kong, HK   📍 Jakarta, ID   📍 Johannesburg, ZA

📍 Karachi, PK   📍 Kuala Lumpur, MY   📍 Kyiv, UA   📍 Lagos, NG   📍 Lisbon, PT   📍 London, UK   📍 Los Angeles, US   📍 Madrid, ES   📍 Monterrey, MX

解决方案：DNSSEC

- 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

.

NET

examle.net

example.net NS a.iana-servers.net.

example.net RRSIG bFhV….0Y3NI

Stub resolver
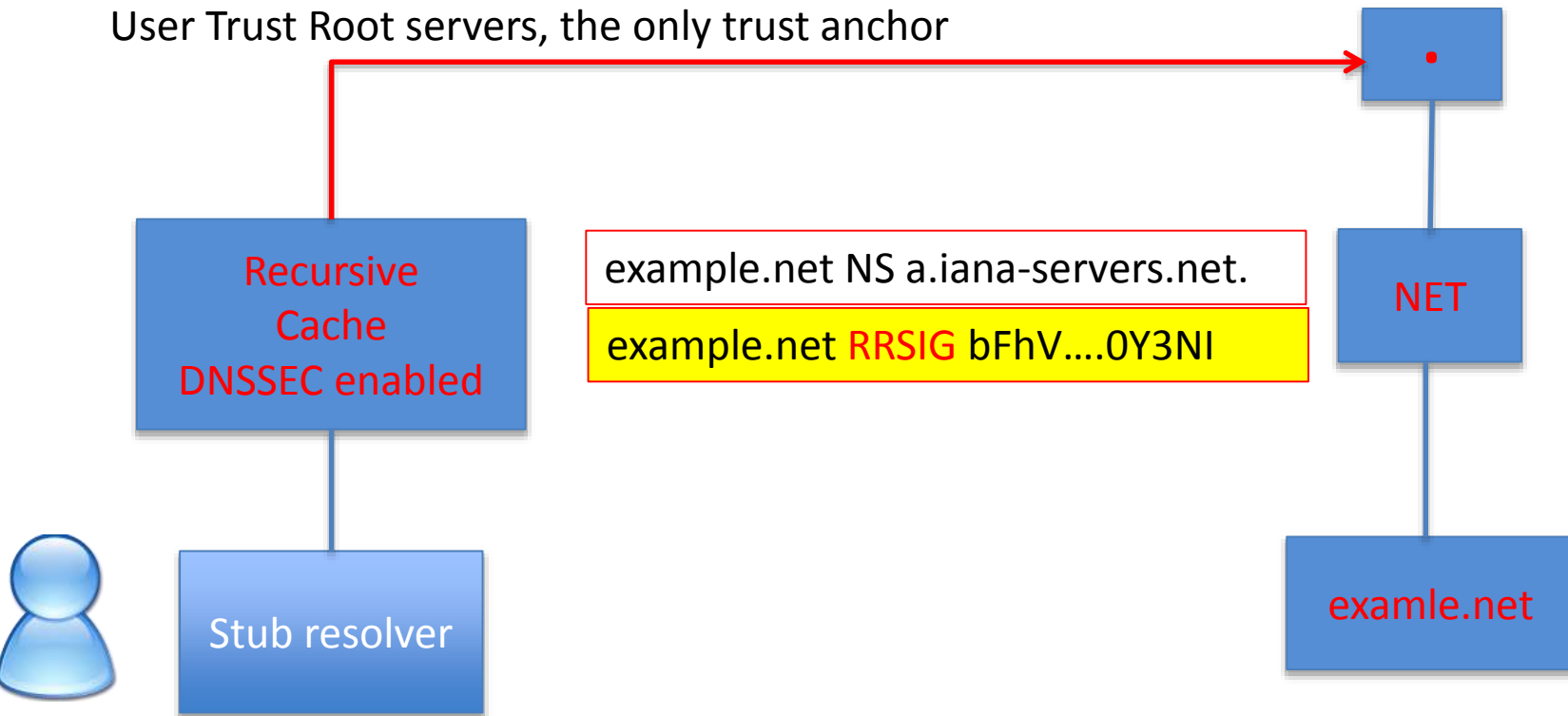
Current Status of DNSSEC

- Client Validation
  - DNSSEC enabled Resolver:

  < 5%

- Server : Signature
  - Almost ready

ccTLD DNSSEC Status on 2013-04-05

- Uncertain (2)
- Experimental (9
- Announced (10)
- Partial (5)
- DS in Root (17)
- Operational (53)

oot-dnssec.org/tcr/selection-2010/
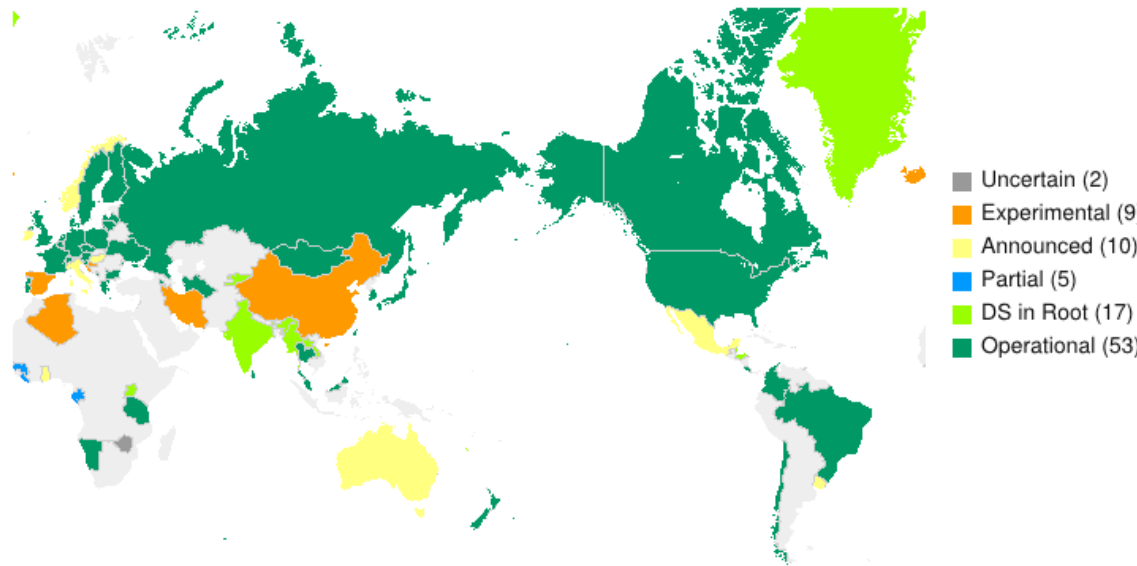
» Subramanian Moonesamy, MU

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

Backup Crypto Officers

» Christopher Griffiths, US

guardian.com/technology/2014/feb/28/seven-people-keys-worldwide-internet-security-web

News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environn

News > Technology > Internet

Meet the seven people who hold the keys to worldwide internet security

Share

Tweet

nternet governance: multi stakeholder model
rust Community, Not Government

提纲

- 基础设施的信任模型
- BGP路由劫持和 RPKI
- DNS 污染和 DNSSEC
- PKI 问题和建议
- 结论

Problems of trust model of Web PKI

- 浏览器/OS厂商预置了数百个CA 的根证书
- 每个CA都可签发所有网站证书，被视为合法
- 一个CA被攻破，则所有商务应用可能被颠覆

VeriSign

Google

Cert. of Gmail.com,
Issued by Google

Cert. of Gmail.com,
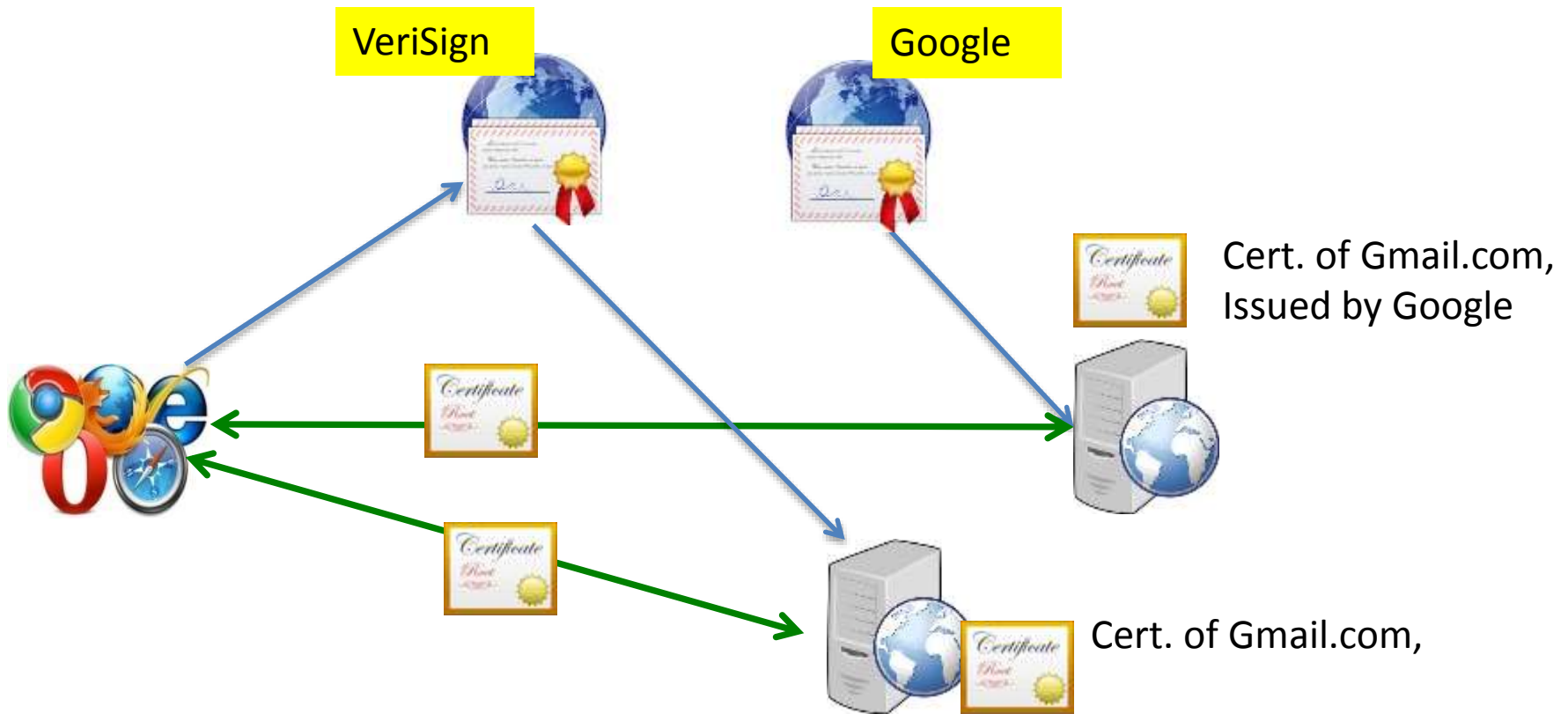
Man in the Middle attack with faked certificate

Man-in-the-Middle

ServerHello

ServerHello
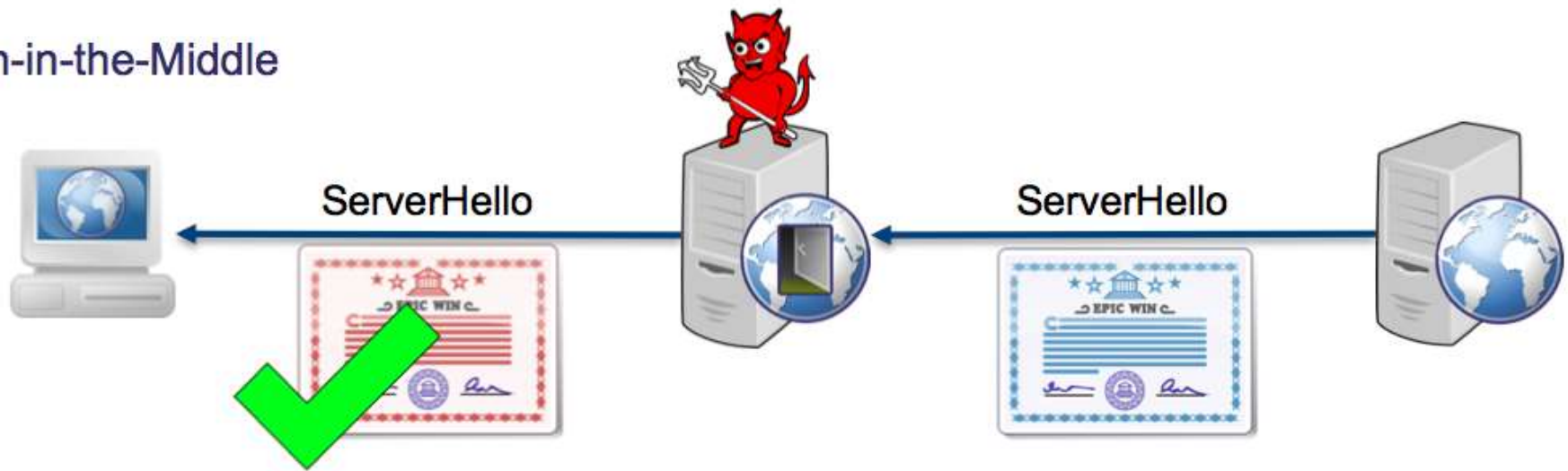
The (fake) certificate is…
- Not expired or revoked
- Validates with one of the many CA's
- Has a matching common name

Report of incident on 15-MAR-2011

An RA suffered an attack that resulted in a breach of one user account of that specific RA.
This RA account was then used fraudulently to issue 9 certificates (across 7 different domains).
All of these certificates were revoked immediately on discovery.
Monitoring of OCSP responder traffic has not detected any attempted use of these certificates after their revocation.

Fraudulently issued certificates

9 certificates were issued as follows:
Domain: mail.google.com [NOT seen live on the internet]
Serial: 047ECBE9FCA55F7BD09EAE36E10CAE1E

Domain: www.google.com [NOT seen live on the internet]
Serial: 00F5C86AF36162F13A64F54F6DC9587C06

Domain: login.yahoo.com [Seen live on the internet]
Serial: 00D7558FDAF5F1105BB213282B707729A3

Domain: login.yahoo.com [NOT seen live on the internet]
Serial: 392A434F0E07DF1F8AA305DE34E0C229

Domain: login.yahoo.com [NOT seen live on the internet]
Serial: 3E75CED46B693021218830AE86A82A71

Domain: login.skype.com [NOT seen live on the internet]
Serial: 00E9028B9578E415DC1A710A2B88154447

Domain: addons.mozilla.org [NOT seen live on the internet]
Serial: 009239D5348F40D1695A745470E1F23F43

Domain: login.live.com [NOT seen live on the internet]
Serial: 00B0B7133ED096F9B56FAE91C874BD3AC0

Domain: global trustee [NOT seen live on the internet]
Serial: 00D8F35F4EB7872B2DAB0692E315382FB0

What didn't Happen

Our CA infrastructure was not compromised.
Our keys in our HSMs were not compromised.
No other RA was compromised. No other RA user accounts were compromised.

Comodo 世界排名前三的CA

2011年被发现系统被入侵，一个伪造的用户签发了9个服务器证书：Google, Yahoo!, Skype Mozilla, MS Live

荷兰的CA: DigiNotar, 被攻破以致破产

- CA , Root CA, issue commercial and gov cert.
- June,20, 2011, COO :"We believe that DigiNotar's certificates are among the most reliable in the field."
- July. 10, 2011, issued a certificate for *.google.com , used in multiple Iranian ISPs
- DigiNotar belatedly admitted dozens fraudulent certificates, including Yahoo!, Mozilla, Wordpress, and Tor
- DigiNotar detected intrusions, but did not disclose to browser vendors.
- Microsoft, Mozilla, Google, Apple and Opera browser revoke Root Certificate of DigiNotar

DANE and TLSA
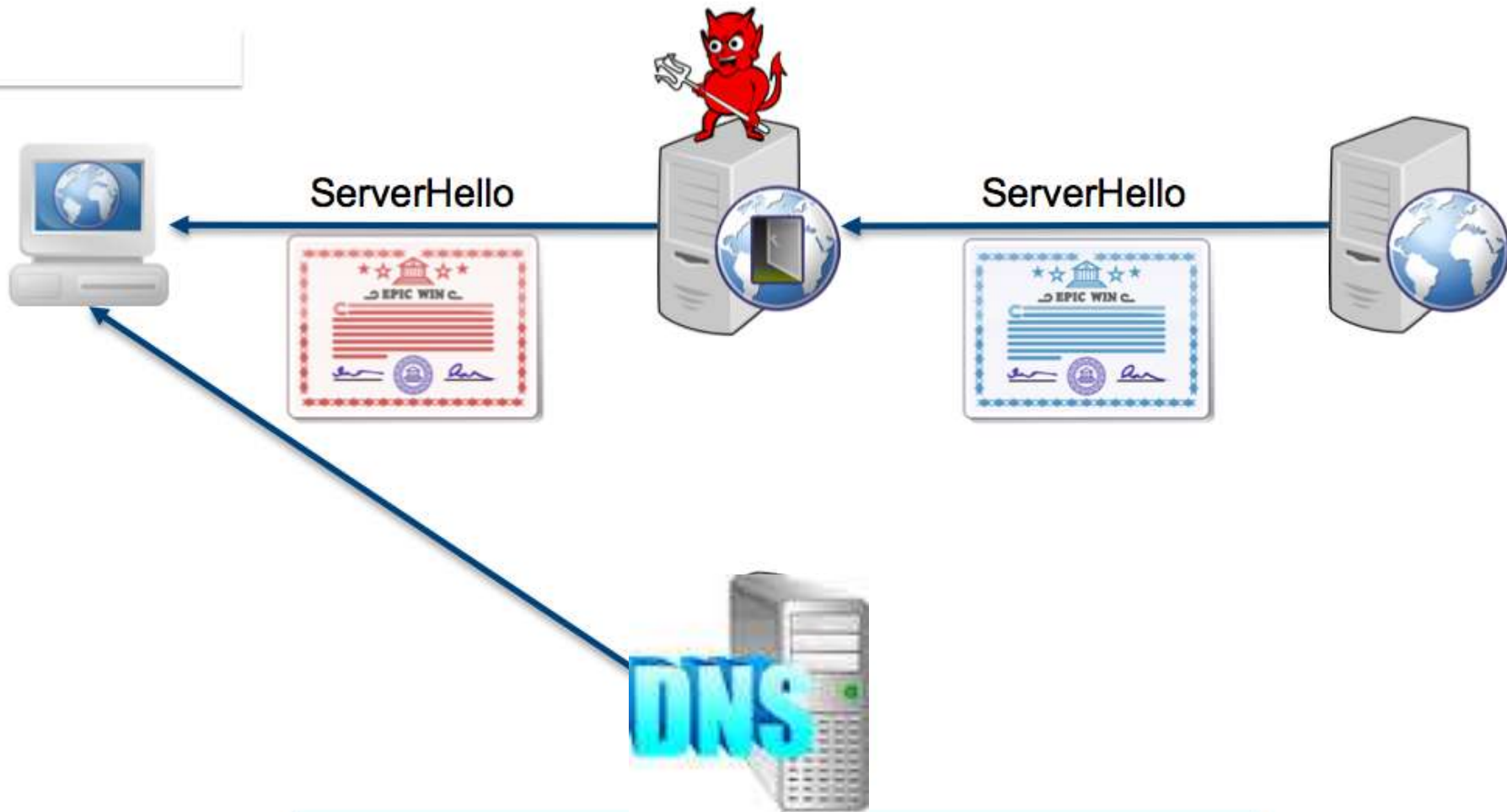

```
_443._tcp.www.example.nl. IN TLSA (
     1 0 1 d2abde240d7cd3ee6b4b28c54df034b9
          7983a1d16e8a410e4561cb106618e971 )
```

Hybird of CA and DNSSEC for Web

DNSSEC

PKI

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

"Multi-Root" Model
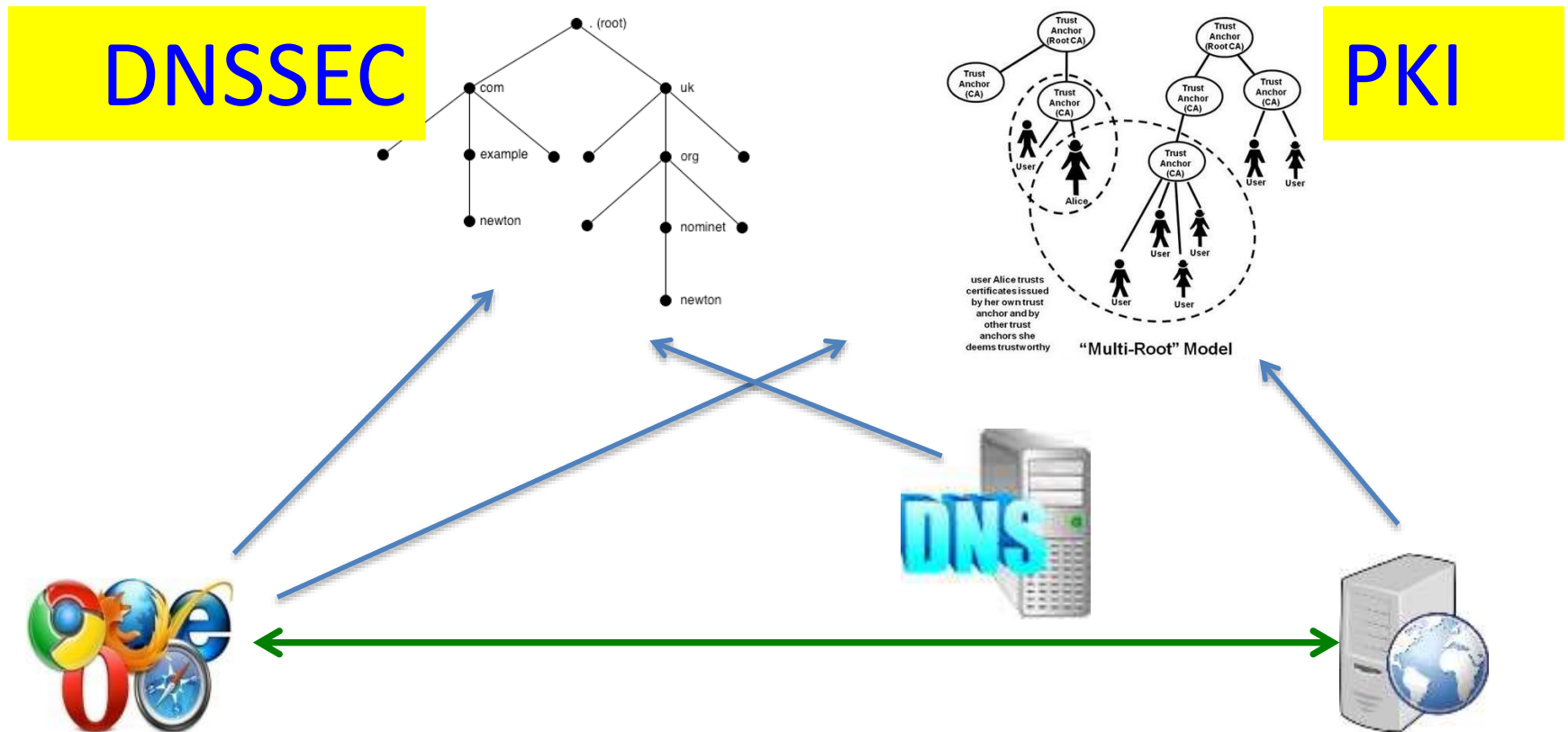
一个安全的应用建立在可靠的PKI和DNSSEC基础上

Cyber Trust 信任模型发展

- BGP -> BGPSEC: IANA，初步试验部署
  - 标准化已完成
  - Cisco, Juniper, 开源软件均支持
  - 少数ISP开始部署实验
- DNS -> DNSSEC:
  - ICANN，10+年, 开始大规模部署
  - 签名基本成熟，但验证部署率很低（5%）
- CA -> DANE/DNSSEC
  - 标准形成了
  - 少数DNS软件已支持（BIND）
  - 应用软件不支持

Concerns

- IETF将推进密码协议发展
  - Pervasive Monitoring Is an Attack(RFC7258, 2014)
  - The IETF will strive to produce specifications that mitigate   pervasive monitoring attacks
- 密码技术的大规模使用依赖PKI
- 集中到少数信任权威（Trust Anchor）似乎不可避免
- 不太可能打破国际现有的体制，自成为一个新的权威

Solutions：多点长期监测

- 互联网的安全机制（如**DNSSEC**）经过一点一滴的演进发展到今天，重新设计并让互联网接受很难

- 我们不能因为对权威的疑惑（比如**DNSSEC**）把自己隔离在互联网之外

- **接受权威并时刻保持质疑**，通过大规模的测量和监督手段，及时发现权威被滥用的情况、进而防止权威主动滥权

发现DNS协议设计问题：幽灵域名

Ghost Domain：恶意域名被父节点删掉，但攻击者可以操控解析服务器，使之永远存活

幽灵域名：**Ghost Domain**

COM
NS phishing.com
A ns.phishing.com

DNS Server
Cache Resolver
Cache | Should Expire after TTL, BUT...

Authoritative Name Server
ns.phishing.com

The attacker can manipulate the resolver and keep his domain resolvable long after TTL
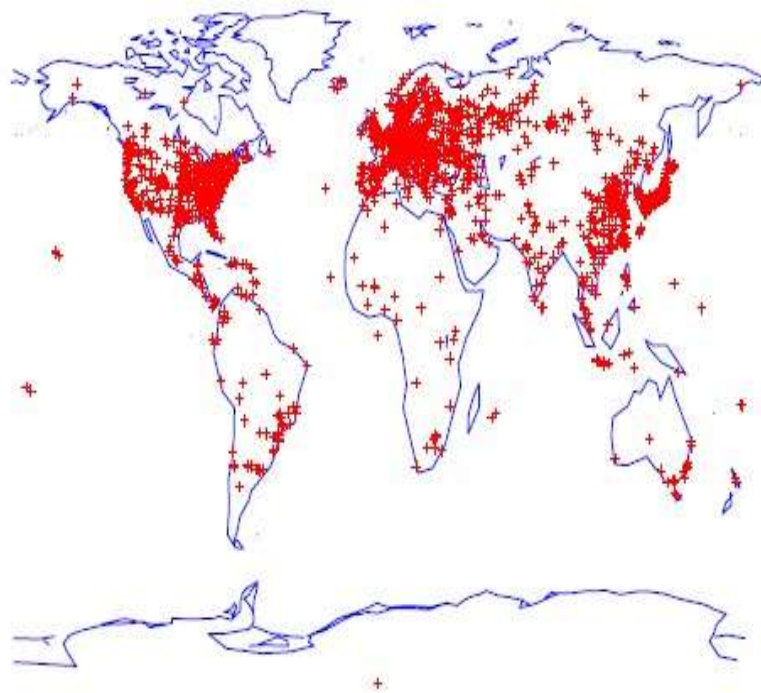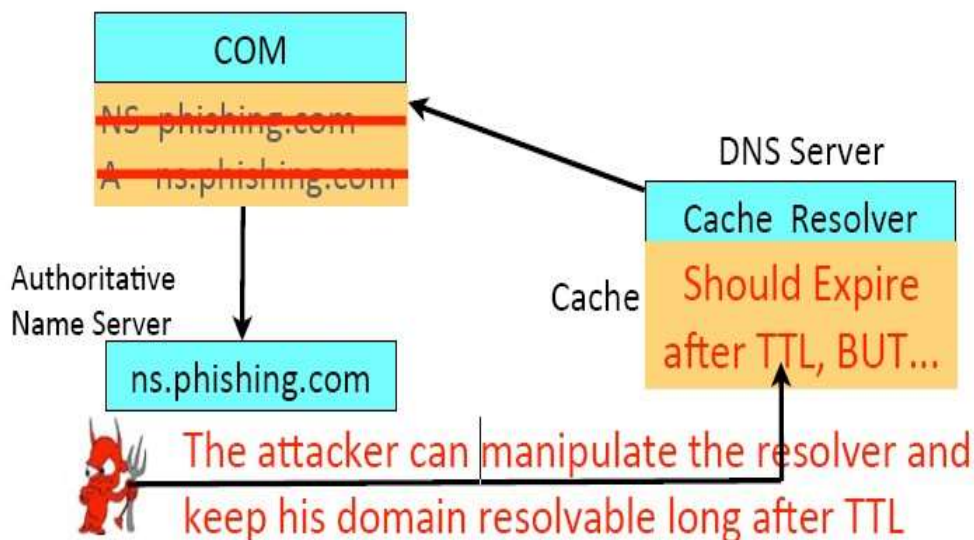
(b) Geographic view of open DNS resolvers that are still haunted by ghost domain names one week later.

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 Réport – 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

| Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics | Data Feeds | Statistics |
| Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments |

National Cyber Awareness System

Vulnerability Summary for CVE-2012-1033

Mission and Overview

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).

Resource Status

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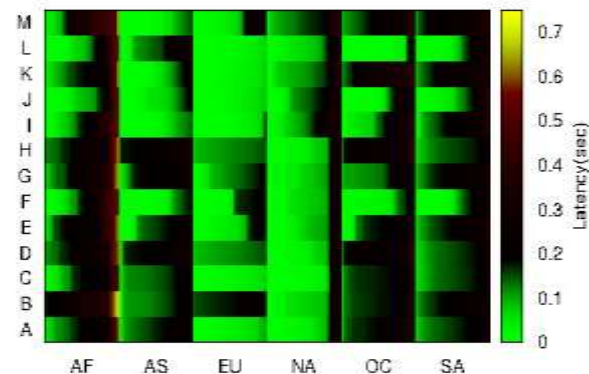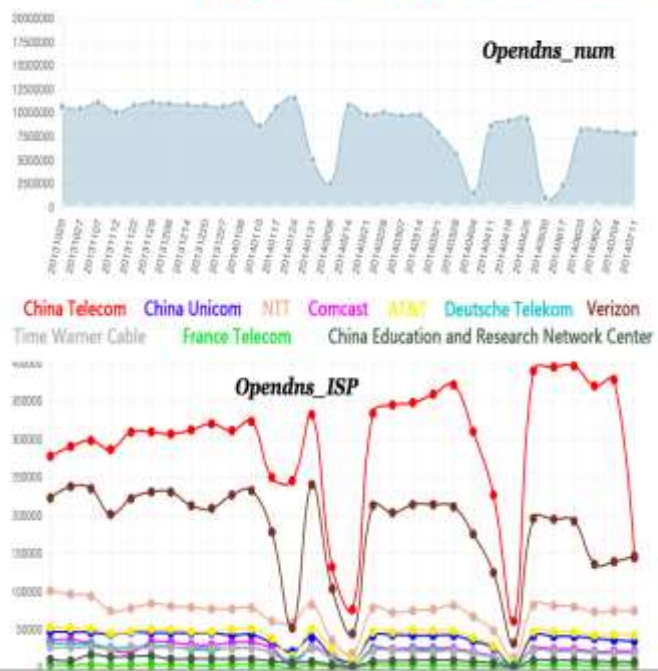**Source:** US-CERT/NIST

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.
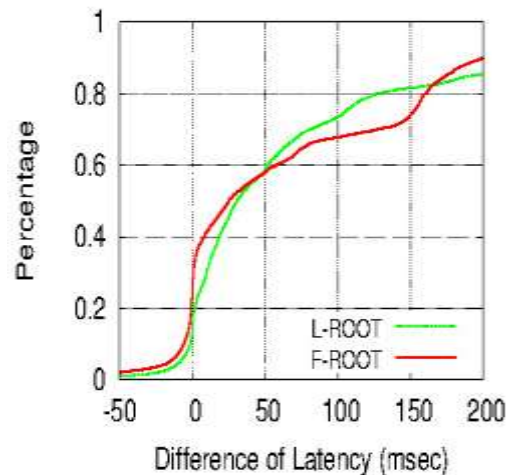
全球DNS安全和测量平台

基于安全实验室和CERNET部署分布式测量平台，对全球DNS服务行为进行了综合分析和安全测试

OpenDNS-Project and Interent measurement

Opendns_num

China Telecom China Unicom NTT Comcast AT&T Deutsche Telekom Verizon
Time Warner Cable France Telecom China Education and Research Network Center

Opendns_ISP

Country_pie

CN
US
JP
DE
FR
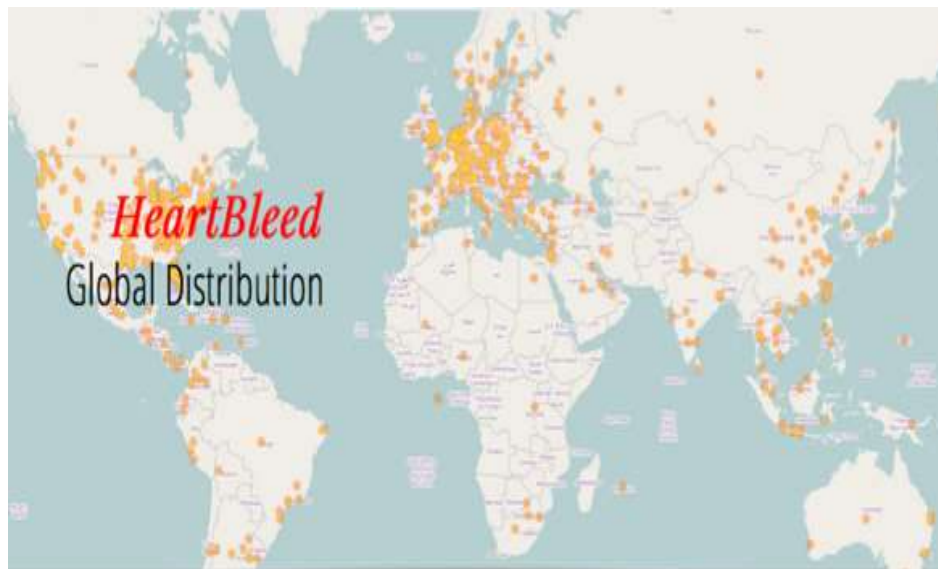GB
RU
IT
BR
IN

13个根域名服务器在各大洲的延迟测量

超过40%的服务器没有访问到最优根节点

2014/01/21: DNS Hijacking in China

全球公钥证书和PKI安全监测平台

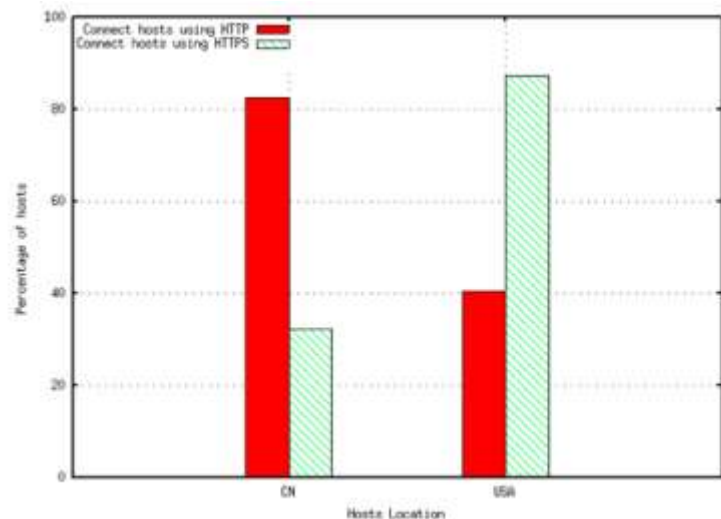全球HeartBleed漏洞服务器安全监测

世界各国使用有效公钥证书的比例，中国仅9%
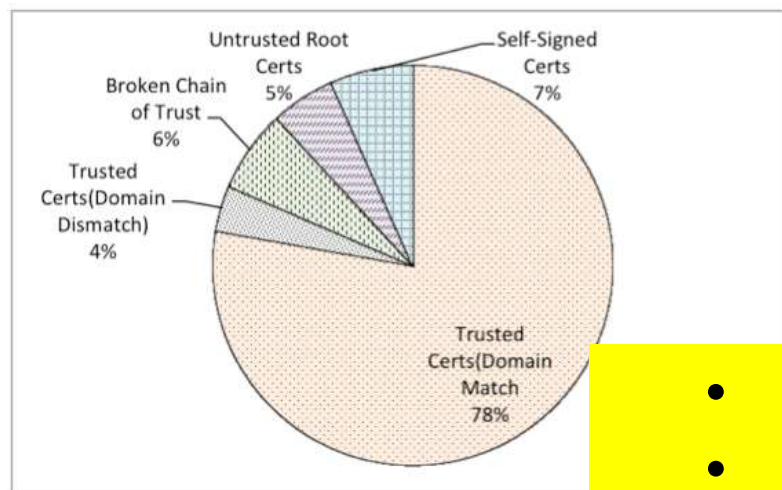
中美银行网站CA和HTTPS测量

图1 中美银行网站HTTPS和HTTP支持率

图3 中国银行网站证书链验证结果统计

表2 CA分布统计表

CA名称	中国	美国
VeriSign	67.26%	64.77%
Entrust	7.08%	11.36%
UserTrust	4.42%	0.00%
CFCA	4.42%	0.00%
Equifax	3.54%	2.27%
BeijingTopsec	1.77%	0.00%
StartCom	0.88%	0.00%
ABC	0.88%	0.00%
GeoTrust	0.00%	5.68%
AddTrust	0.00%	7.95%
Thawte	0.00%	2.27%
GTE	0.00%	2.27%
GoDaddy	0.00%	1.14%
Valicert	0.00%	1.14%
DigiCert	0.00%	1.14%
Self-Sign	9.73%	0.00%

- 可信证书：中国78%，美国100%
- 增强验证EV证书:中国14%,美国51%

发现HTTPS在CDN中的安全问题
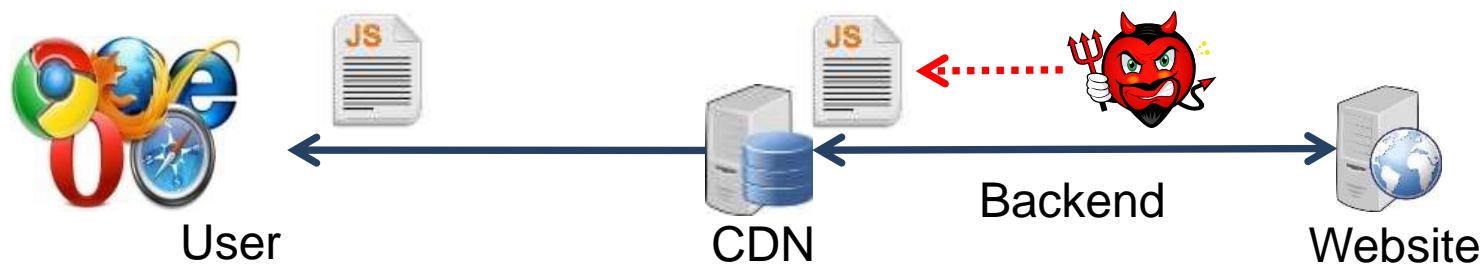
- 后端使用HTTP明文传输，或不验证证书
- CDN 要求网站共享私钥
- 证书回收问题
- 论文发表在TOP 1 安全学术会议IEEE S&P
- 帮助CloudFlare等多个CDN厂商提高了安全性，防止NSA的大规模监听

Q & A

Haixin Duan
duanhx@tsinghua.edu.cn
Tsinghua University