网络空间安全
校园网的挑战和机遇

2017-05-05


教育现状
50万所
1800万人
26000万人
22万所
http://...
45万个
38000万条
特点
机构多
人员多
系统多
数据多
关注度高
影响面广

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

邮箱登录

搜索

工业和信息化部 新闻动态 信息公开 在线办事 公众参与 专题专栏 工信数据

首页 > 信息公开 > 法律法规 > 法律 > 正文

中华人民共和国网络安全法

发布时间：2016-11-08 来源：政策法规司

中华人民共和国主席令
第五十三号

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，现予公布，自2017年6月1日起施行。

中华人民共和国主席 习近平

2016年11月7日

中华人民共和国网络安全法

目 录

《网络安全法》六大突出亮点

一、明确了网络空间主权的原则

二、明确了网络产品和服务提供者的安全义务

三、明确了网络运营者的安全义务

四、进一步完善了个人信息保护规则

五、建立了关键信息基础设施安全保护制度

六、确立了关键信息基础设施重要数据跨境传输的规则

国家批准增设：网络空间安全一级学科

国务院学位委员会
教育部 文件

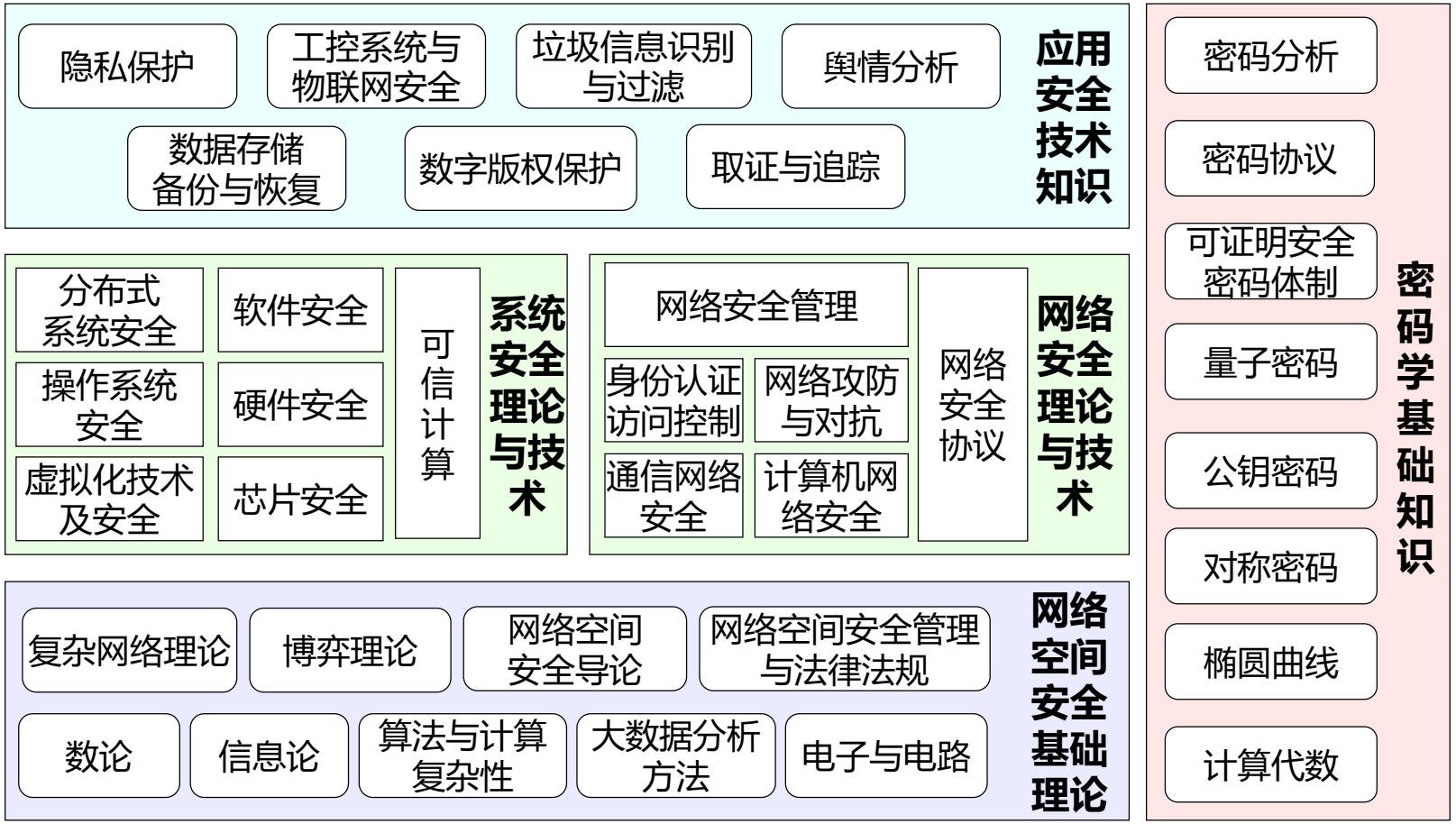
学位〔2015〕11号

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：

为实施国家安全战略，加快网络空间安全高层次人才培养，根据《学位授予和人才培养学科目录设置与管理办法》的规定和程序，经专家论证，国务院学位委员会学科评议组评议，报国务院学位委员会批准，决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位。请各单位加强“网络空间安全”的学科建设，做好人才培养工作。

学科知识体系

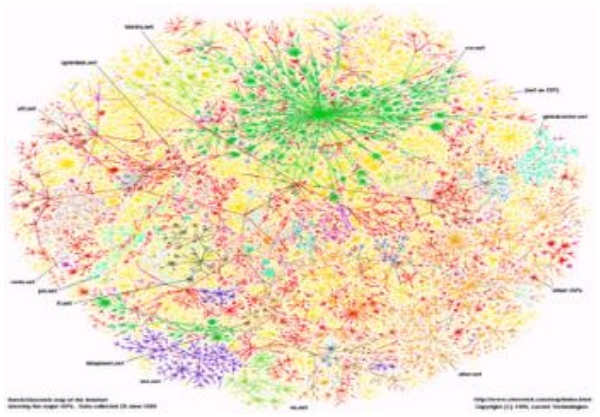

隐私保护
工控系统与物联网安全
垃圾信息识别与过滤
舆情分析
数据存储备份与恢复
数字版权保护
取证与追踪
应用安全技术知识
分布式系统安全
软件安全
操作系统安全
硬件安全
虚拟化技术及安全
芯片安全
可信计算
系统安全理论与技术
网络安全管理
身份认证访问控制
网络攻防与对抗
通信网络安全
计算机网络安全
网络安全协议
网络安全理论与技术
复杂网络理论
博弈理论
网络空间安全导论
网络空间安全管理与法律法规
数论
信息论
算法与计算复杂性
大数据分析方法
电子与电路
网络空间安全基础理论
密码分析
密码协议
可证明安全密码体制
量子密码
公钥密码
对称密码
椭圆曲线
计算代数
密码学基础知识

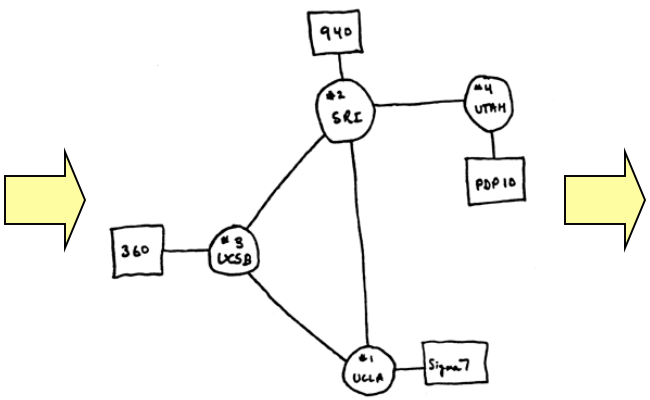
分析

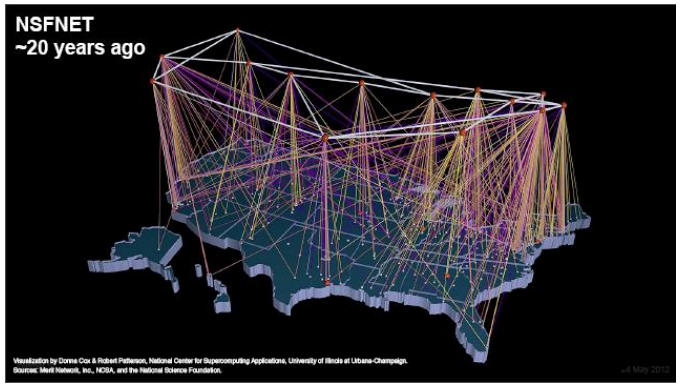
1. 网络安全是全球性的问题
2. 网络安全是国家重大需求
3. 网络安全极其复杂
4. 网络安全专业性极强（技术手段）
5. 网络安全有规模效应
6. IPv6是网络安全的新战场
7. 教育单位的困境
8. 网络安全是持续过程
9. 人才是根本

历史

- 1969 ARPANET (48)
- 1986 NSFNET (31)
- 1995 互联网商业化 (22)
- 2011 IPv4地址耗尽 (6)
- 2013 斯诺登事件 (4)



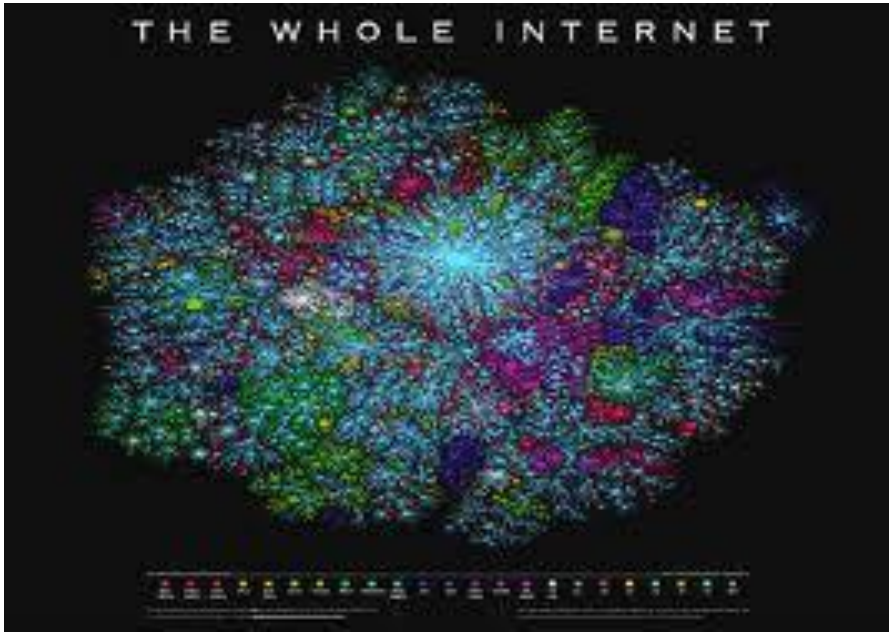




人类20世纪后期的两项最重大战略工程

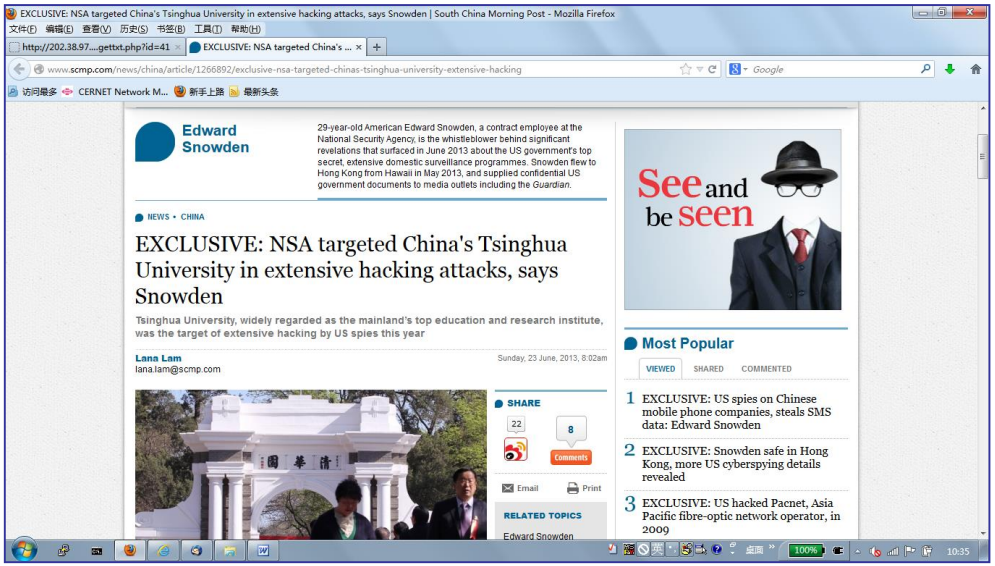
- 星球大战计划：太空空间

- 互联网计划：网络空间




文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)
marcelo jun mur...
Jonathan B. Pos...
2012 INTERNET ...
Internet History,...
ieee internet aw...
Norse - IPViking Live
大科学 - 维基百...
大科学时代背后的大...
map.ipviking.com
Google
访问最多
CERNET Network M...
新手上路
最新头条
http://labs.chinamo...
http://ireseim.allyes....
NORSE
ATTACK ORIGINS
Country
650 China
210 United States
40 Mil/Gov
33 Russia
21 Hong Kong
18 South Korea
17 Ukraine
12 United Kingdom
12 Germany
11 Netherlands
ATTACK TARGETS
Country
28 Hong Kong
9 Spain
7 Portugal
6 Liechtenstein
6 Austria
3 Turkey
3 Canada
ATTACK TYPES
Service Port
282 ms-wbt-server 3389
226 http-alt 8080
75 telnet 23
44 http 80
42 ssh 22
29 isakmp 500
29 domain 53
27 snmp 161
ATTACKS
Timestamp
Attacker
Organization Location IP
Target
Location
Type
Service Port
2014-08-29 08:15:27.91 ChinaNet Guangdong Guangzhou, China 119.147.114.80 unknown, Singapore microsoft-ds 445
2014-08-29 08:15:27.92 ChinaNet Guangdong Guangzhou, China 119.147.114.80 unknown, Singapore microsoft-ds 445
2014-08-29 08:15:28.53 Unitedlayer San Francisco, United States 209.237.229.110 Englewood, United States domain 53
2014-08-29 08:15:28.53 Unitedlayer San Francisco, United States 209.237.229.110 Santa Clara, United States domain 53
2014-08-29 08:15:28.54 Versaweb, LLC Las Vegas, United States 76.164.203.220 unknown, Thailand ms-sql-s 1433
2014-08-29 08:15:28.55 Versaweb, LLC Las Vegas, United States 76.164.203.220 unknown, Thailand ms-sql-s 1433
2014-08-29 08:15:28.55 Versaweb, LLC Las Vegas, United States 76.164.203.220 unknown, Thailand ms-sql-s 1433
2014-08-29 08:15:28.56 Versaweb, LLC Las Vegas, United States 76.164.203.220 unknown, Thailand ms-sql-s 1433
99%
16:15

Snowden



IETF87

IETF88

Encryption without authentication

Five hums

- The IETF is willing to respond to the pervasive surveillance attack?
  - Overwhelming YES. Silence for NO.
- Pervasive surveillance is an attack, and the IETF needs to adjust our threat model to consider it when developing standards track specifications.
  - Very strong YES. Silence for NO
- The IETF should include encryption, even outside authentication, where practical.
  - Strong YES. Silence for NO
- The IETF should strive for end-to-end encryption, even when there are middleboxes in the path.
  - Mixed response, but more YES than NO.
- Many insecure protocols are used in the Internet today, and the IETF should create a secure alternative for the popular ones.
  - Mostly YES, but some NO.

Hardening The Internet

IETF98, Chicago, 2017

I strongly support the use of human rights as a foundational value in considering design implications.

分析

1. 网络安全是全球性的问题
2. 网络安全是国家重大需求
3. 网络安全极其复杂
4. 网络安全专业性极强（技术手段）
5. 网络安全有规模效应
6. IPv6是网络安全的新战场
7. 教育单位的困境
8. 网络安全是持续过程
9. 人才是根本

Building a new governance hierarchy:
RPKI and the future of Internet routing and addressing

- DHS
- NSA
- DARPA

4. How we got here: the historical process

An RPKI aligned with the existing IP address allocation hierarchy is not the only available approach for making routing more secure. Yet in the past 5 years it has emerged from the IETF and the RIRs as the dominant approach. Despite the many uncertainties associated with governance arrangements for RPKI (see section 5), serious and possibly irreversible implementation steps are already being taken. How and why did the technical community converge on such an implementation of RPKI? The basic answer is that the U.S. government, acting through contractors with Defense Department and DHS grants, pushed a solution that was well aligned with the incentives of the extant Internet governance institutions, just as it has actively promoted DNSSEC as the chief mechanism for securing the domain name system.

The idea for a RPKI emerged in the mid-1990s, from work funded by the National Security Agency and DARPA to address routing security problems. (Kent, Lynn, & Seo, 2000) In 1999 individuals affiliated with U.S. government contractor BBN Technologies first authored Internet drafts proposing to use X.509 extensions (digital certificates) to authenticate IP addresses, AS identifiers and BGP announcements.[5] BBN's specification required the initial development of two PKIs "to verify the identities and authorization of BGP speakers and of owners of ASes and of portions of the IP address space." (Seo, Lynn, & Kent, 2001)

正确处理安全和发展的关系

- 网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。
- 1、树立正确的网络安全观。理念决定行动。
  - 网络安全是整体的而不是割裂的；
  - 是动态的而不是静态的；
  - 是开放的而不是封闭的；
  - 是相对的而不是绝对的；
  - 共同的而不是孤立的。
- 2、加快构建关键信息基础设施安全保障体系。
- 3、全天候全方位感知网络安全态势。
  - 感知网络安全态势是最基本最基础的工作。
- 4、增强网络安全防御能力和威慑能力。
  - 要落实网络安全责任制，制定网络安全标准，明确保护对象、保护层级、保护措施。

网络空间安全挑战的主要特点

- 整体的，不是割裂的
  - 涉及网络空间的各个方面：系统、网络和应用
- 动态的，不是静态的
  - 网络空间安全事件常常是动态发生，或不可重复
- 开放的，不是封闭的
  - 网络空间安全事件发生在开放环境下，难以追踪
- 相对的，不是绝对的
  - 网络空间安全事件的时刻发生，安全成本是相对的
- 共同的，不是孤立的
  - 网络空间安全事件具有共同性、国际性、关联性

国家互联网应急中心2016年报告（1）

- 木马和僵尸网络
  - 2016年约9.7万个木马和僵尸网络控制服务器控制了我国境内1699万余台主机
  - 来自境外的约4.8万个控制服务器控制了我国境内1499万余台主机，来自美国的控制服务器数量居首位，其次是中国香港和日本。
- 移动互联网安全
  - 2016年，CNCERT通过自主捕获和厂商交换获得移动互联网恶意程序数量205万余个，较2015年增长39.0%，近7年来持续保持高速增长趋势
- 拒绝服务攻击
  - 2016年大流量攻击事件数量全年持续增加，10Gbps以上攻击事件全年日均达133次，100Gbps以上攻击事件数量日均达到6起以上，监测发现某云平台多次遭受500Gbps以上的攻击。

国家互联网应急中心2016年报告（2）

- 安全漏洞
  - 2016年，国家信息安全漏洞共享平台（CNVD）共收录通用软硬件漏洞10822个，较2015年增长33.9%。其中，高危漏洞收录数量高达4146个（占38.3%），较2015年增长29.8%；“零日”漏洞2203个，较2015年增长82.5%。
- 网站安全
  - 2016年，CNCERT监测发现约17.8万个针对我国境内网站的仿冒页面，约2万个IP地址承载了上述仿冒页面，其中位于境外的IP地址占85.4%
  - 2016年，CNCERT监测发现约4万个IP地址对我国境内8.2万余个网站植入后门
  - 2016年，CNCERT监测发现，我国境内约1.7万个网站被篡改

2016年我国互联网网络安全状况

- 域名系统安全状况良好，防攻击能力明显上升
- 针对工业控制系统的网络安全攻击日益增多，多起重要工控系统安全事件应引起重视
- 高级持续性威胁常态化，我国面临的攻击威胁尤为严重
- 大量联网智能设备遭恶意程序攻击形成僵尸网络，被用于发起大流量DDoS攻击
- 网站数据和个人信息泄露屡见不鲜，“衍生灾害”严重
- 移动互联网恶意程序趋利性更加明确，移动互联网黑色产业链已经成熟
- 敲诈勒索软件肆虐，严重威胁本地数据和智能设备安全

网络空间安全（1）

- 网络攻击危及社会安全与经济安全
- 网络脆弱性与安全漏洞威胁隐私信息
- 新技术引发的安全风险不断加大
- 信息技术应用受控于信息技术强国
- 管理不善带来的安全风险
- 网络军事化威胁世界和平

网络空间安全（2）

The Modern Internet Threatscape

Paradigm #1:
Expect the Unexpected

Paradigm #2:
It's All About the Greenbacks

Paradigm #3:
It's *Not* All About the Greenbacks

Paradigm #4:
Our Trust Is In Trouble

Paradigm #5:
The Bad Guys' Trust is in Trouble

网络空间安全的元问题

- 人类的科学和技术能力无法避免软硬件设计缺陷导致的漏洞问题
- 经济全球化和生产活动国际化是产业生态环境日益复杂难以避免后门问题
- 网络统计复用机制使拥塞现象不可避免，难以避免DDOS问题
- 互联网基础设施导致的信任锚链问题
- 明文传输、存储、分析导致的隐私泄露问题

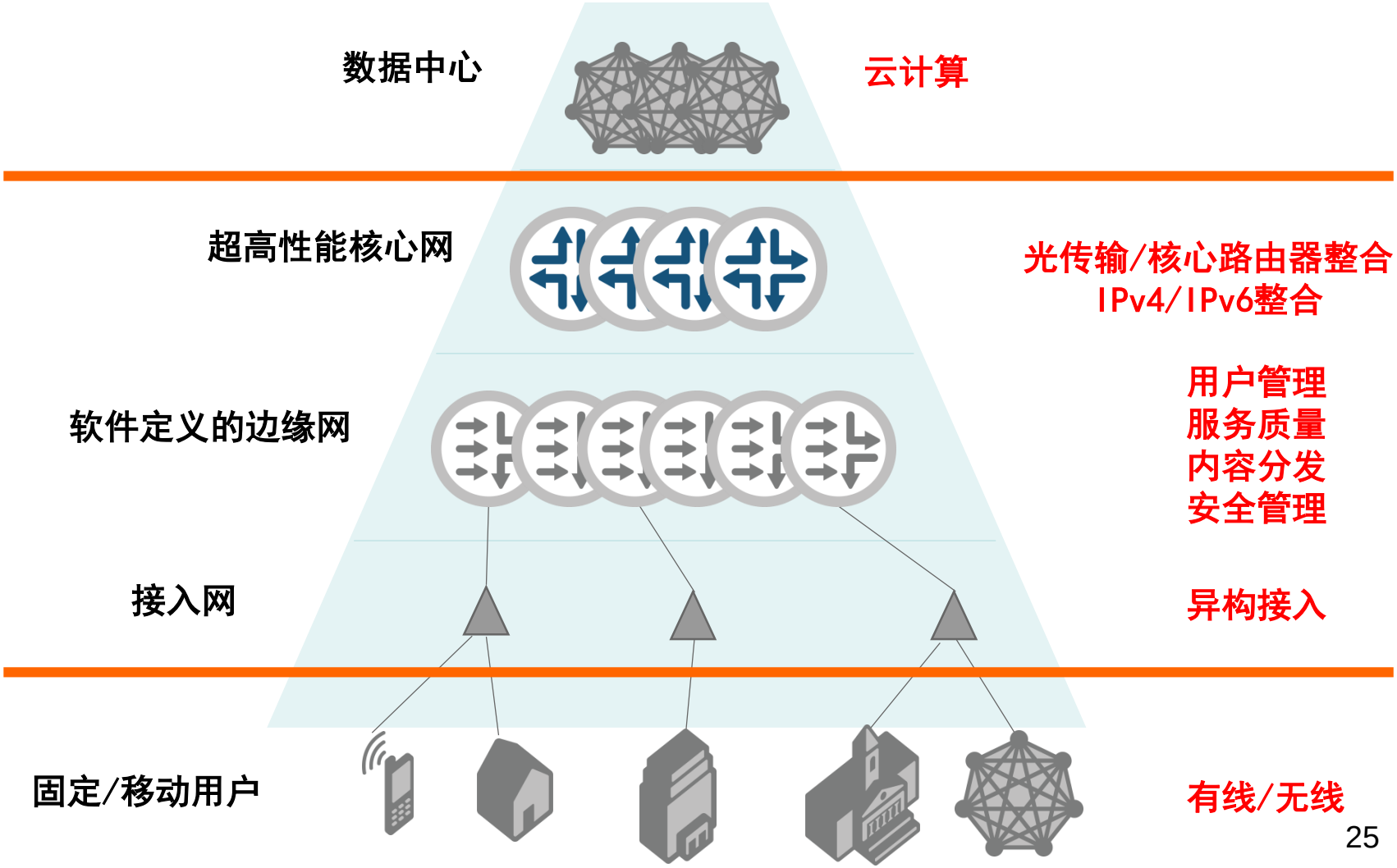
在沙滩上建大厦

中国思维（第一代）：以保护为主
美国思维（第二代）：以监测处理为主

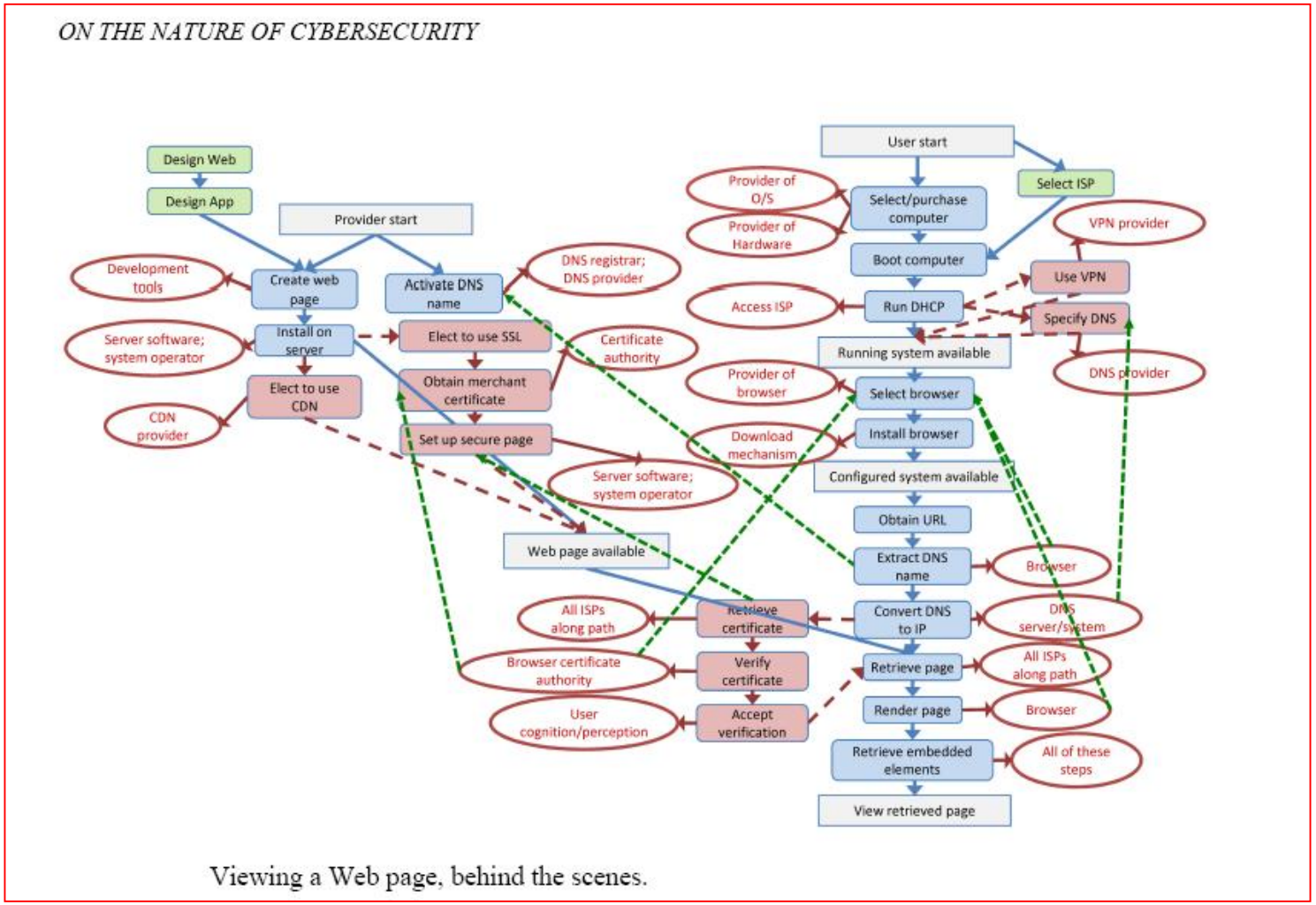
分析

1. 网络安全是全球性的问题
2. 网络安全是国家重大需求
3. 网络安全极其复杂
4. 网络安全专业性极强（技术手段）
5. 网络安全有规模效应
6. IPv6是网络安全的新战场
7. 教育单位的困境
8. 网络安全是持续过程
9. 人才是根本

网络结构

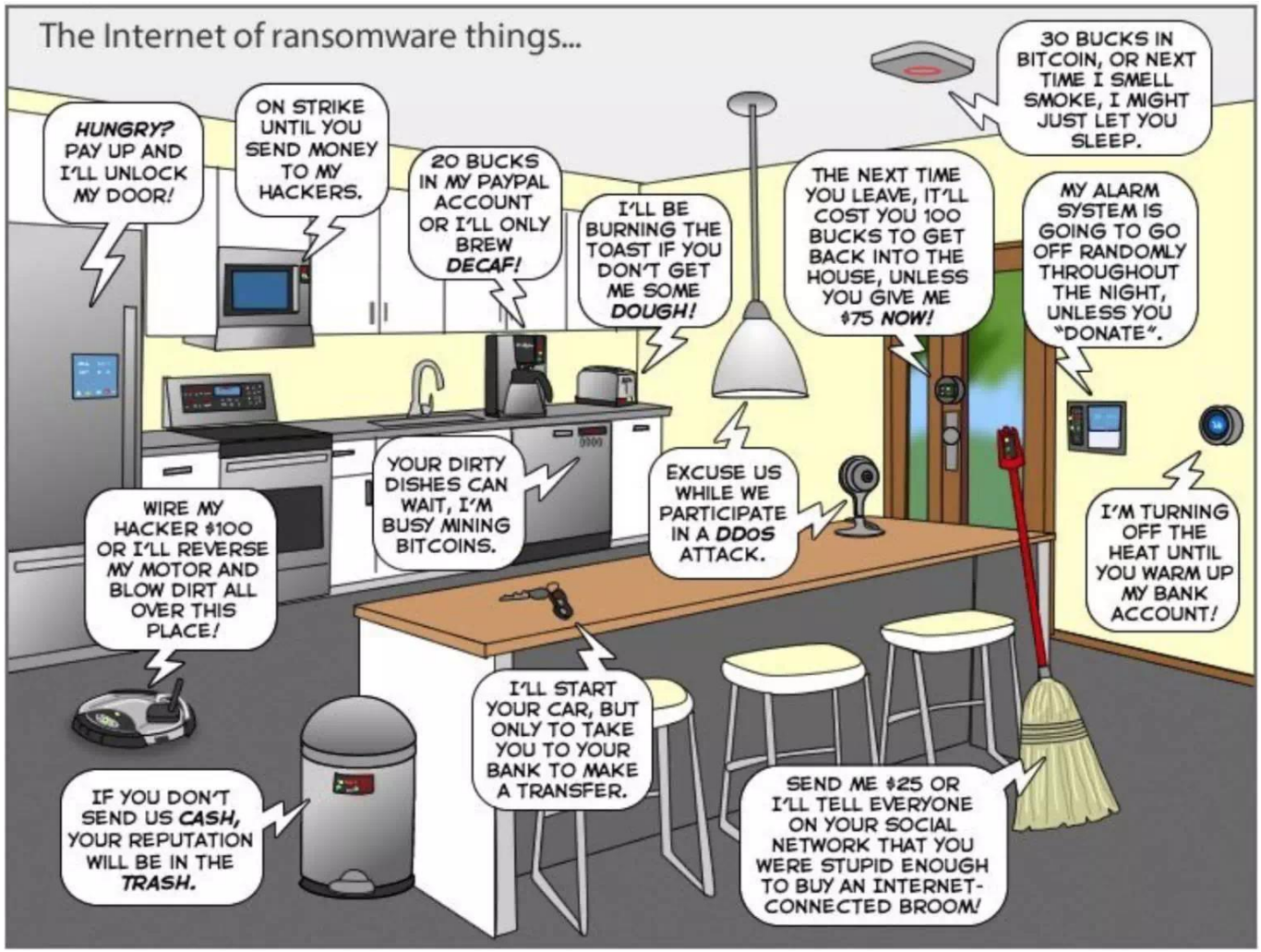

数据中心
云计算
超高性能核心网
光传输/核心路由器整合
IPv4/IPv6整合
软件定义的边缘网
用户管理
服务质量
内容分发
安全管理
接入网
异构接入
固定/移动用户
有线/无线

Control points



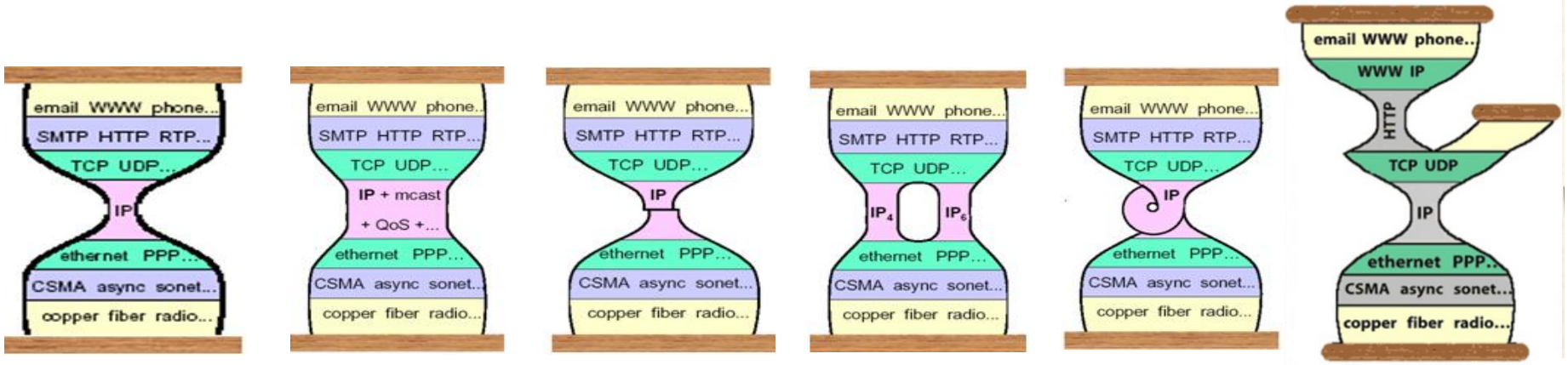
Viewing a Web page, behind the scenes.


你好，我是你儿子学校的。
我们的电脑出了点问题。
呃，我儿子他弄坏的吗？
算是吧…
你真给你儿子起名叫Robert'); DROP TABLE Students;-- ？
是啊，还给他起了个小名叫"表表"
漂亮，我们今年的学生记录全没了。
这回你满意了吧。
这回你学会清洁数据库输入了吧。


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

- 我认为机器人应该是定义比较广泛的，像自主驾驶汽车还有其他设备这些也都是机器人。我认为任何一种可编程的器件从某种角度上来讲都是属于这一类的，比如说像按摩椅，
- 我家里就有一个按摩椅，这个按摩椅有一些不同的程序和方式，当然是它一种软件。但是我从来都没有用过这个按摩椅，我自己是一个编程师，我知道有时候程序会出现漏洞，我很害怕如果我坐在按摩椅上出现漏洞怎么办，所以我就没有用过这个按摩椅，但是我的妻子很喜欢，它也是一种机器人。

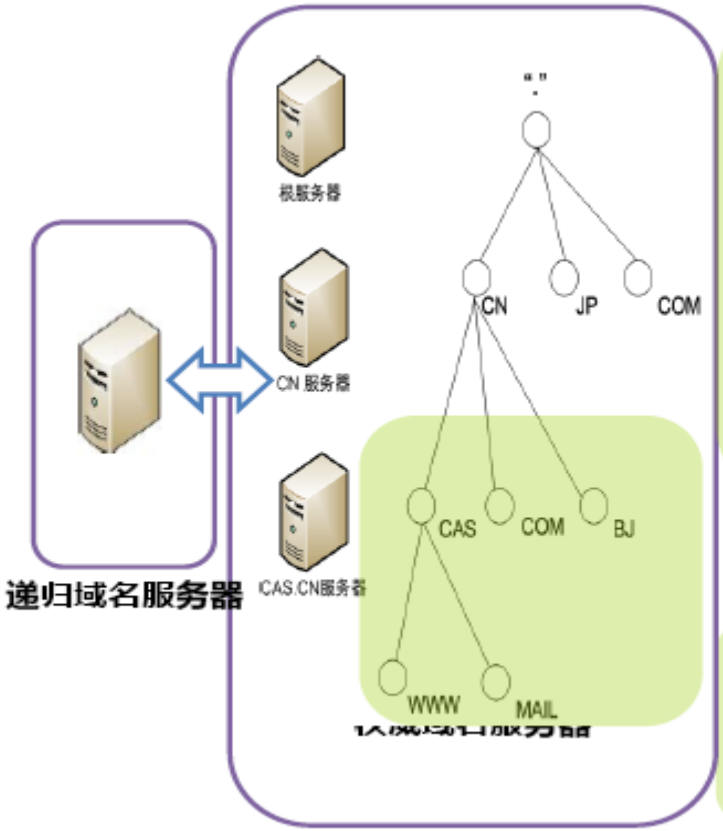
互联网演进过程的窄腰形态变化



分析

1. 网络安全是全球性的问题
2. 网络安全是国家重大需求
3. 网络安全极其复杂
4. 网络安全专业性极强（技术手段）
5. 网络安全有规模效应
6. IPv6是网络安全的新战场
7. 教育单位的困境
8. 网络安全是持续过程
9. 人才是根本

DNS安全案例



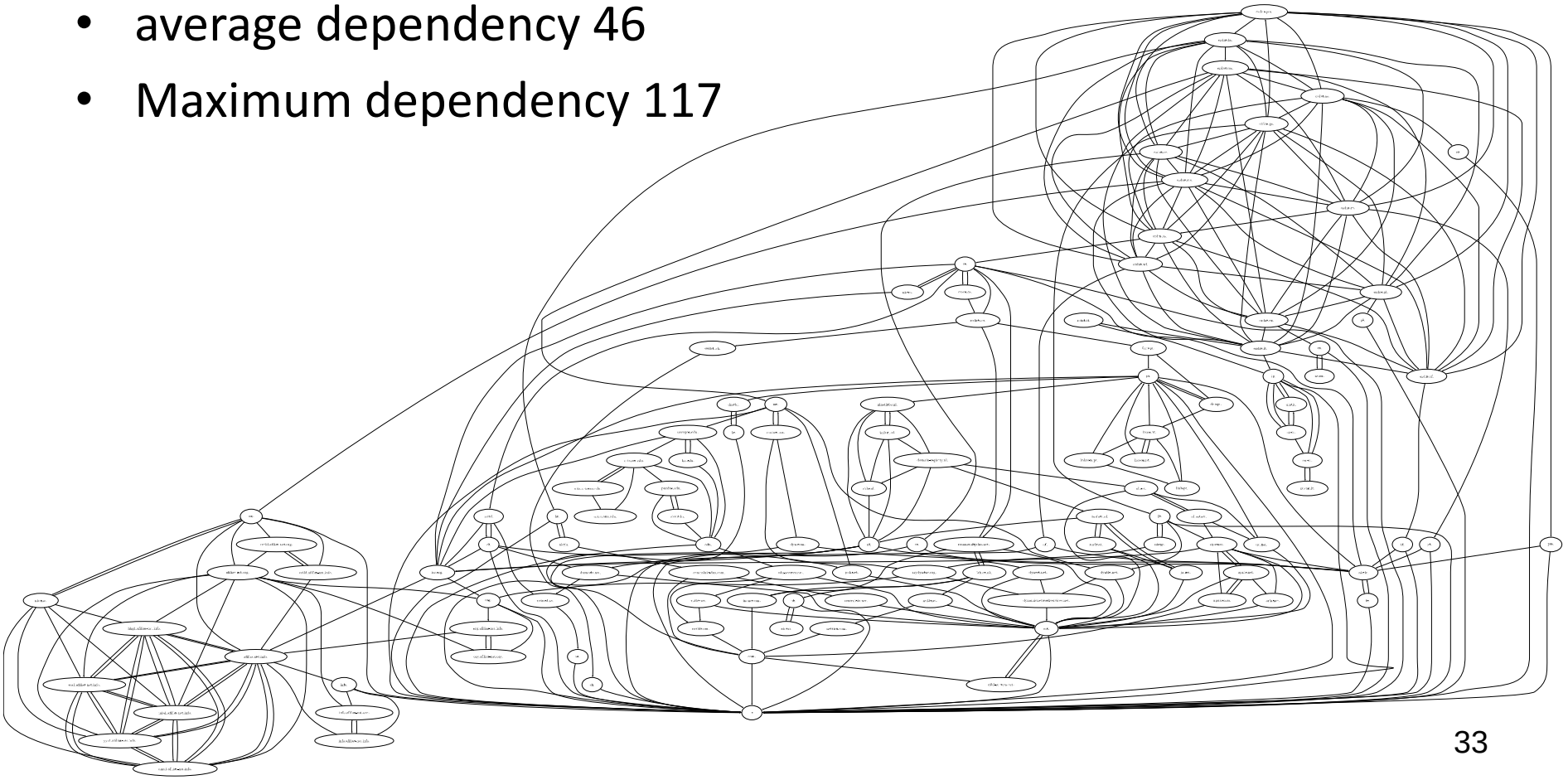
- 2014年3月26日，某CDN服务商的授权DNS无法解析，造成新浪、百度、豆瓣、凤凰、网易、CCTV、56等多家知名网站出现大规模访问故障，时间持续将近1个小时。
- 2013年1月27日，某知名CDN服务商DNS故障导致包括163、腾讯、凤凰网、百度、乐视网以及12306在内的知名网站在部分地区的访问受到影响，不少大客户断线时间超过1小时

二级和二级以下域名服务

- 主要自建、注册服务商免费服务为主
- 是目前出现问题最多的环节

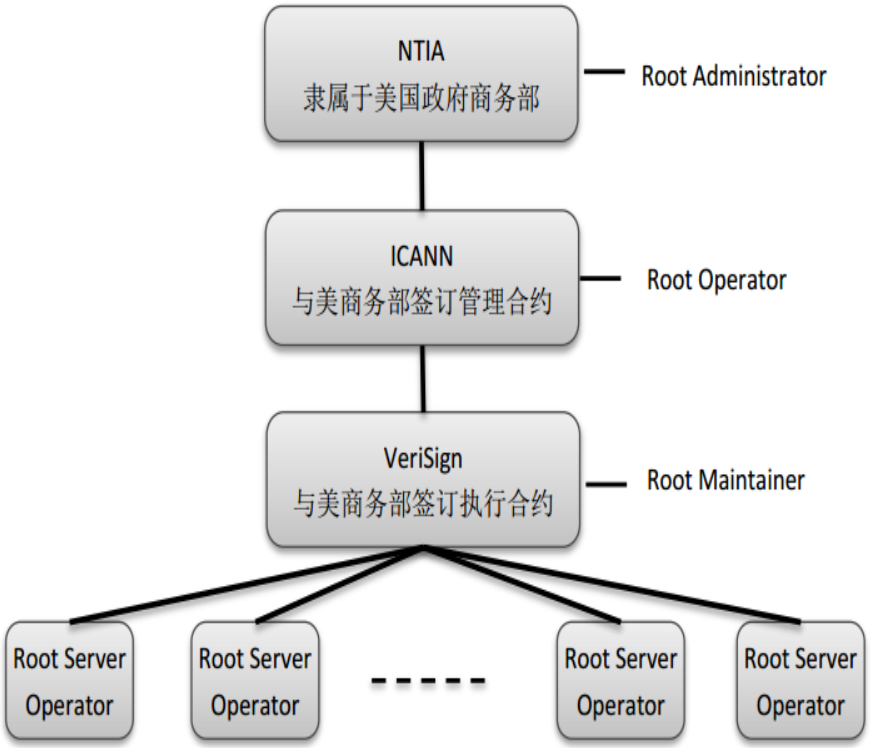
Every dependent DNS resolving process could be hijacked

- For 1M hot DNS,
- average dependency 46
- Maximum dependency 117



DNSSEC

DNS 权力体系

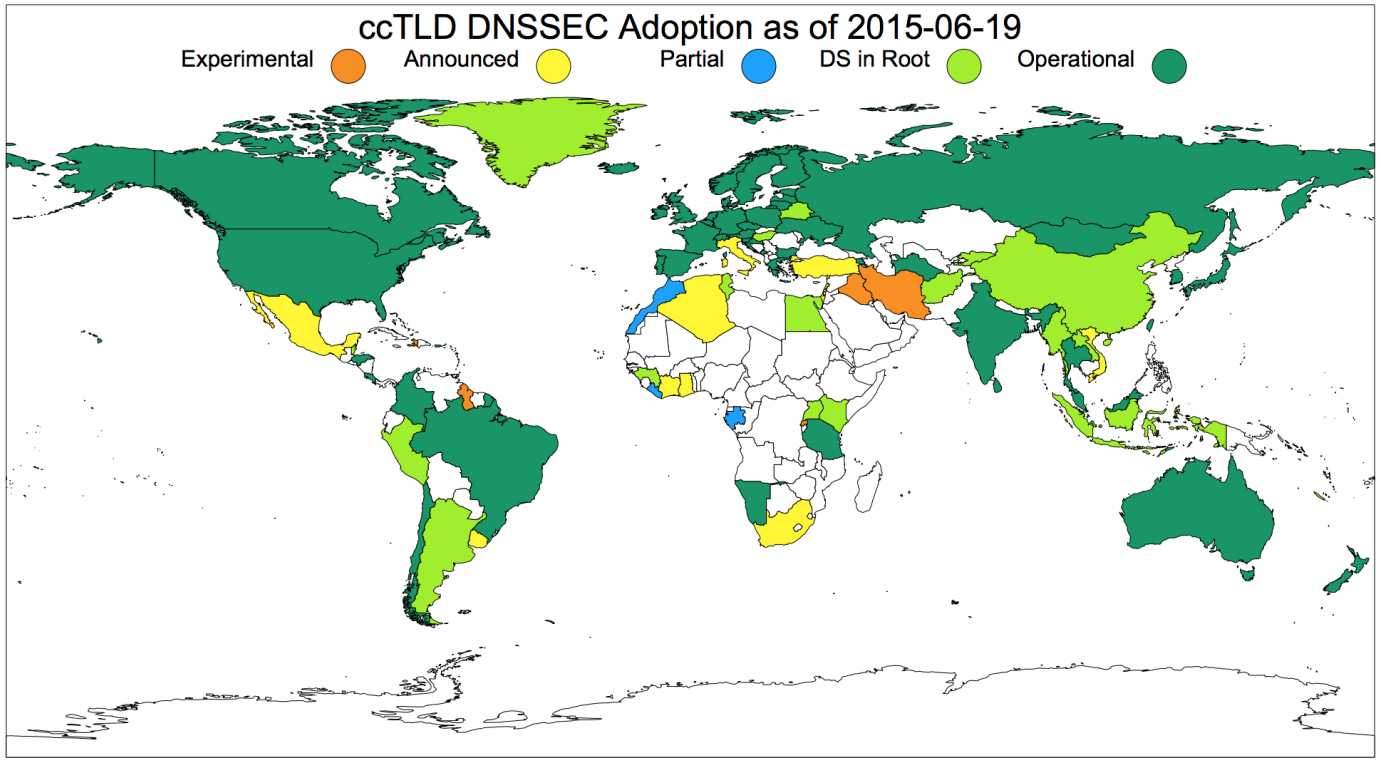


DNSSEC 权力体系

shamir 机密共享机制

Trust anchor

服务器端 DNSSEC 签名广泛部署



Experimental -- Internal experimentation announced or observed (9): GY HK HT IQ IR MS MU RW TO

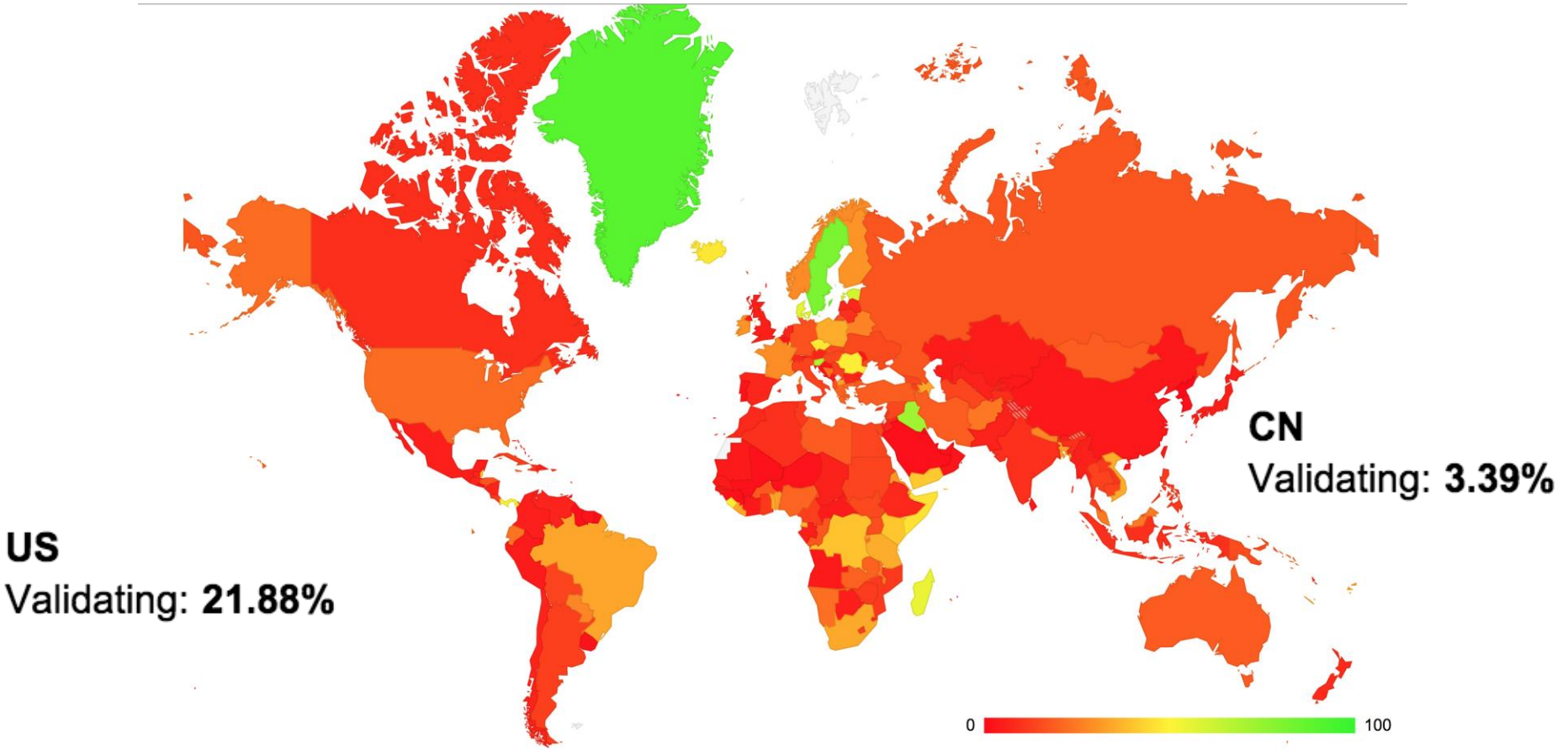
Announced -- Public commitment to deploy (11): CI DZ GH IL IT MX SG TR UY VN ZA

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

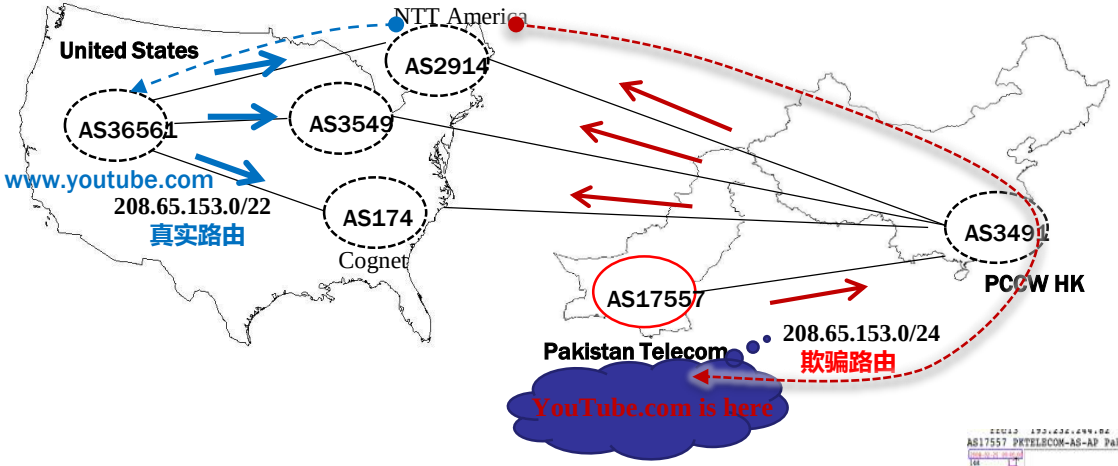
Operational -- Accepting signed delegations and DS in root (67): AC AM AT AU BE BG BR CA CH CL CO CR CX CZ DE DK EE ES FI FR GR GS HN HR IE IN IO IS JP KR LI LK LT LU LV ME MN MY NA NF NL NO NZ PL PM PR PT RE RU SB SC SE SH SI SX TF TH TL TM TT TW TZ UA UK US WF YT

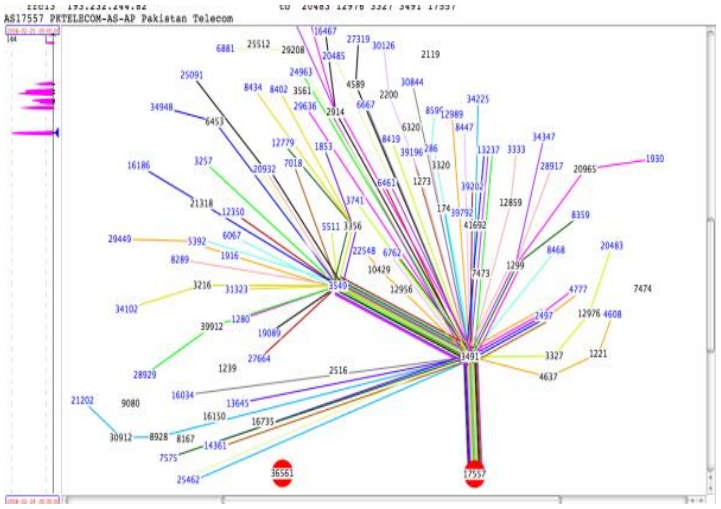
解析端 DNSSEC 验证很少部署



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

路由劫持（1）


NTT America
United States
AS2914
AS36561
AS3549
www.youtube.com
208.65.153.0/22
真实路由
AS174
Cognet
AS3491
PCCW HK
AS17557
Pakistan Telecom
208.65.153.0/24
欺骗路由
YouTube.com is here

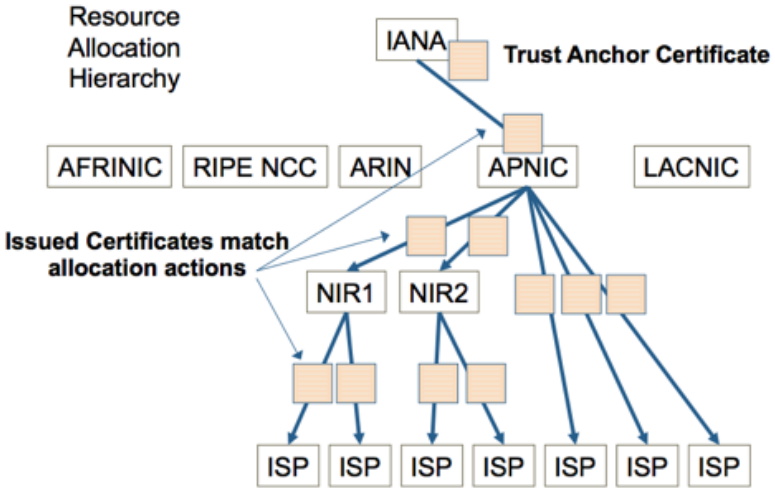

AS17557 PKTELECOM-AS-AP Pakistan Telecom

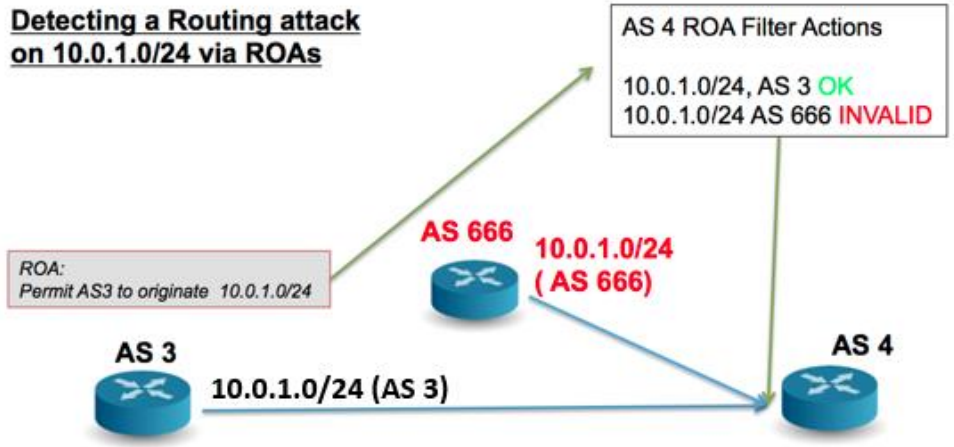
路由劫持（2）


Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via Belarus
START 1. Guadalajara, Mexico
201.151.31.149
AS11172 alestra
2. Monterrey, Mexico
3. Laredo, TX
63.218.121.49
AS3491 pccw
4. Ashburn, VA
129.250.3.180
AS2914 NTT
10. New York, NY
5. Washington, D.C.
64.209.109.221
AS3549 level3
11. Washington, D.C. END
63.234.113.110
AS209 Qwest
6. London, UK
87.245.233.198
AS9002 RETN
9. Frankfurt, Germany
8. Minsk, Belarus
217.150.62.233
AS6697 beltelecom
7. Moscow, Russia
217.150.62.234
AS20485 transtelecom
renesys
Source: Renesys Path Measurements

rPKI

- RPKI: 通过IANA层级签名构造一个地址前缀和AS的所属关系；通过BGPSEC验证路径的真实性
- Cisco, Juniper, Quagga已支持，少数ISP实验
- IANA (ICANN) 是最终的Trust Anchor

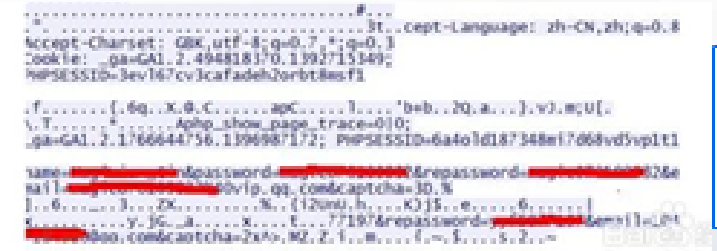




OpenSSL协议漏洞

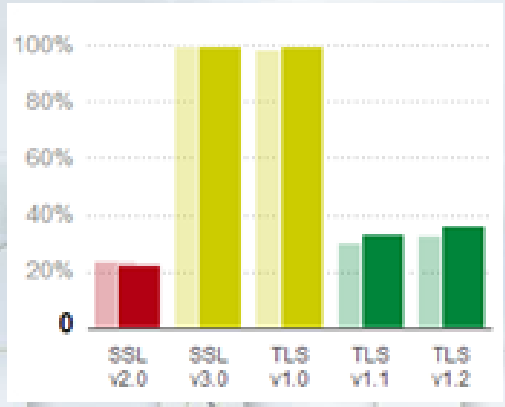
密码协议实现漏洞攻击，OpenSSL“Heartbleed”漏洞

- 缺乏边界检查，导致内存泄漏



- 服务器上64K内存数据内容泄露
- 可能有安全证书、用户名与密码等

- 受影响的网站
  - TrustInet公司统计0.8%的网站受影响，包括Yahoo、Imgur等
  - 建议漏洞修复



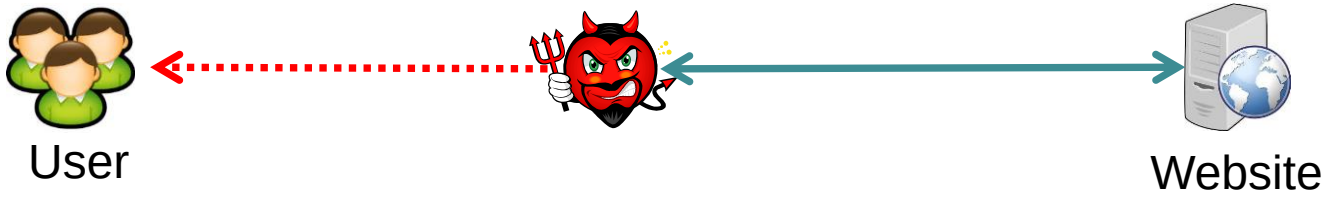

中国铁路客户服务中心
2014年4月23日 星期三
首 页
客运服务
货运
行包服务
车站引导
铁路常识
站车风采
客户信箱
站车风采
北京西站
最新动态
为保障您顺畅购票，请下载安装根证书。
关于2014年上半年京沪、京广高铁部分G字头动车组列车商务、特等、一... NEW! (2014-03-27)
关于2014年短途卧铺优惠有关事宜的公告 NEW! (2014-03-05)
铁路互联网购票身份核验须知 (2014-02-23)
沈阳铁路局关于五一期间加开管内临客的公告 (2014-04-20)
昆明铁路局关于五一期间加开管内临客的公告 (2014-04-23)
广铁集团公司关于2014年4月30日至5月3日临时加开部分列车的公告 (2014-04-22)
https://kyfw.12306.cn/otn/leftTicket/init
旅客服务
新版售
网上
退
余
旅客列
旅客列
The site's security certificate is not trusted!
You attempted to reach kyfw.12306.cn, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.
You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand

使用自签名的证书问题

- 弹出告警，是原始网站的问题，还是中间人攻击？
- 该CA 如果干坏事怎么办？
- 它签发的所有证书，浏览器都不会弹出告警
- 可信CA有第三方审计，自签名的CA有吗？
- 我信任该CA，但若被攻破了被利用怎么办？

中间人攻击

Man In the Middle

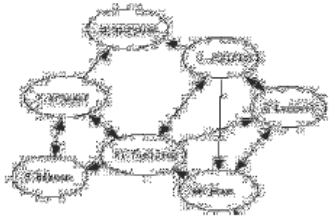


信任模型

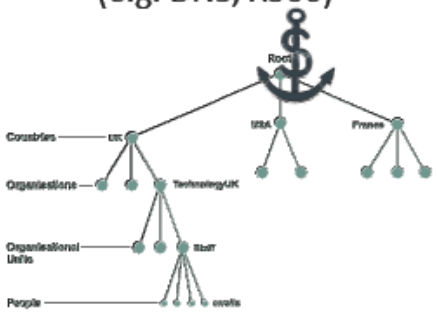
Trust on First Use, e.g. SSH, DNS/Cert Pinning

Centralized (e.g. Kerberos)

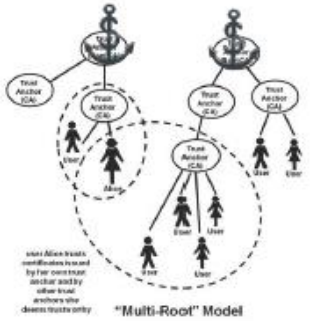
Web of Trust (e.g. PGP, BGP)



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



Forest(e.g. CA)



Block chain (e.g. bitcoin)

Underlying technology	Features
P2P communication	Decentralized structure
Digital signature	Authentication of information
Proof of work (POW)	All nodes maintain public information

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

China Tried To Get... | cpe stat all | Softwires (softwire)... | CERNET logo - Go... | IAB Statement on Inter... | Launching in 2015: ... | Launching in 2015: ...

https://www.eff.org/deeplinks/2014/11/certificate-authority-encrypt-entire-web

访问最多 CERNET Network M... 新手上路 最新头条 http://labs.chinamo... http://ireseim.allyes....

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

SEARCH

HOME | ABOUT | OUR WORK | DEEPLINKS BLOG | PRESS ROOM | TAKE ACTION | SHOP

NOVEMBER 18, 2014 | BY PETER ECKERSLEY

Launching in 2015: A Certificate Authority to Encrypt the Entire Web

Today EFF is pleased to announce Let's Encrypt, a new certificate authority (CA) initiative that we have put together with Mozilla, Cisco, Akamai, IdenTrust, and researchers at the University of Michigan that aims to clear the remaining roadblocks to transition the Web from HTTP to HTTPS.

Donate to EFF

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying

eff.org/nsa-spying

EFF is leading the fight against the NSA's illegal mass surveillance program. Learn more about what the program is, how it works, and what you can do.

Follow EFF

Britain, France and Australia: if

正在传输来自 anon-stats.eff.org 的数据...

97% 9:59

安全对策（1）

- 在开放环境下建立信任，目前不得不依赖密码算法和密码协议
- 密码技术的大规模使用依赖PKI
- 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（Trust Anchor）的疑惑（比如DNSSEC）把自己隔离在互联网之外

安全对策（2）

- 把自己建成可信的Trust Anchor，需要开放透明的规则
- 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

分析

1. 网络安全是全球性的问题
2. 网络安全是国家重大需求
3. 网络安全极其复杂
4. 网络安全专业性极强（技术手段）
5. 网络安全有规模效应
6. IPv6是网络安全的新战场
7. 教育单位的困境
8. 网络安全是持续过程
9. 人才是根本

ccert


中国教育科研网络紧急响应组
China Education & Research Computer Emergency Response Team
[最新公告][English Version]
CCERT 简介
联系方法
网络安全公告
系统安全补丁
网络安全工具
网络安全资料
垃圾邮件处理
端口扫描处理

分析

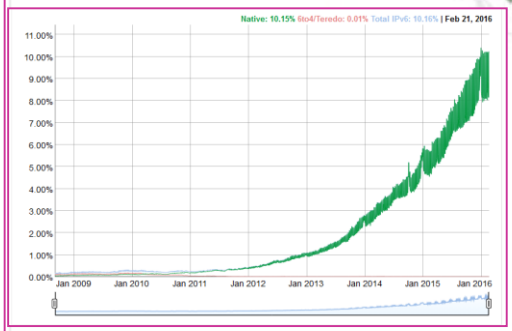
1. 网络安全是全球性的问题
2. 网络安全是国家重大需求
3. 网络安全极其复杂
4. 网络安全专业性极强（技术手段）
5. 网络安全有规模效应
6. IPv6是网络安全的新战场
7. 教育单位的困境
8. 网络安全是持续过程
9. 人才是根本

2016年初全球IPv6部署情况

IPv6 Adoption | **Per-Country IPv6 adoption**

Per-Country IPv6 adoption

2012 Rank	Economy	% of Internet Users who use IPv6	# of IPv6 Users
1	China	1.01%	5,209,030
2	United States of America	1.01%	2,500,684
3	France	4.03%	2,013,920
4	Japan	1.75%	1,766,799
5	Romania	7.40%	641,389



United States
IPv6 Adoption: **23.85%**
Latency / impact: **0ms / 0.02%**

China
IPv6 Adoption: **2.76%**
Latency / impact: **0ms / 0.9%**

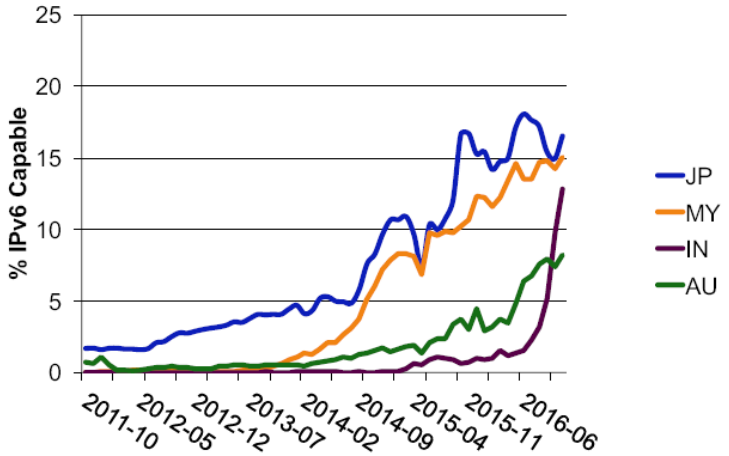
World | Africa | Asia | Europe | Oceania | North America | Central America | South America

CC	IPv6 %	CC	IPv6 %	CC	IPv6 %	CC	IPv6 %	CC	IPv6 %	CC	IPV6 %
BE	56.16%	CH	42.86%	DE	35.24%	US	34.76%	GR	32.46%	LU	29.26%
PT	27.51%	GB	23.79%	EE	20.00%	TT	19.61%	PE	18.52%	JP	17.99%
CA	17.92%	EC	17.59%	MY	14.94%	FI	14.93%	FR	14.82%	IN	13.00%
AT	12.40%	NO	11.91%	BR	11.37%	IE	10.82%	AU	10.71%	CZ	10.53%
NL	10.06%	RO	8.53%								

Above and Below the Line:

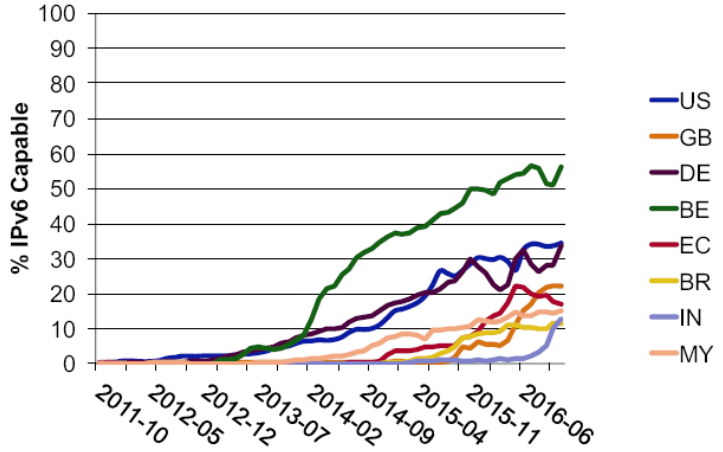
CC	IPv6 %	CC	IPv6 %	CC	IPv6 %	CC	IPv6 %	CC	IPv6 %	CC	IPv6%
ZW	7.91%	HU	7.08%	NZ	5.62%	SA	5.27%	VN	4.80%	BO	4.70%
SG	4.20%	PL	3.75%	BA	3.71%	SI	3.54%	DK	3.47%	SE	3.09%
HK	2.74%	TH	2.63%	GT	2.62%	LK	1.85%	IT	1.56%	NR	1.51%
RU	1.43%	TR	1.00%	IL	0.88%	BW	0.88%	BG	0.81%	DO	0.80%
CN	0.68%	JE	0.56%	UA	0.53%	EG	0.53%	LT	0.50%	KR	0.48%
AF	0.32%	MD	0.31%	SD	0.30%	AR	0.30%	IS	0.28%	KN	0.27%
TW	0.26%	BT	0.26%	SK	0.20%	AE	0.15%	ZA	0.15%	LR	0.15%
RS	0.13%	YE	0.12%	ID	0.11%	HR	0.10%	MO	0.09%	CL	0.08%

Higher IPv6 capability in Asia-Pacific



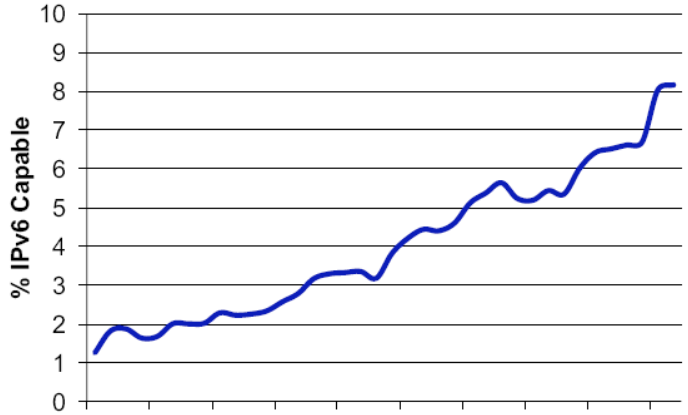
APNIC

Higher IPv6 capable Economies worldwide

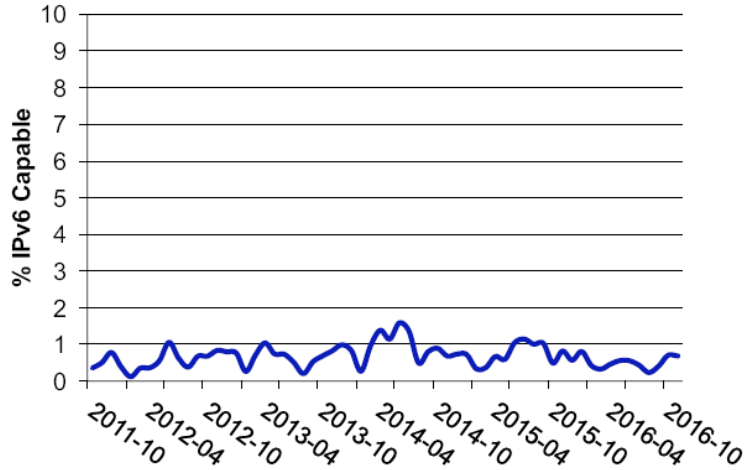


APNIC

IPv6 capability worldwide (weighted)



IPv6 capabiity, China



制约我国下一代互联网发展的原因

美国

- 基于全球公有地址

  IPv4地址耗尽后，新建网络采用IPv6地址，保证端到端通信的地址唯一性

- 形成完整产业链（引领）

  ISP：Comcast，……

  OS：Apple, Microsoft……

  ICP：Google，Facebook……

中国

- 采用私有地址转换

  解决IP地址短缺的权宜之计，不利于保障网络服务质量和网络安全，影响我国互联网长远发展

- 缺少IPv6信息资源（僵局）

  电信运营商完成IPv6网络改造

  移动终端等支持IPv6

  BAT等信息服务商等待市场形成

- 网络安全防护现状

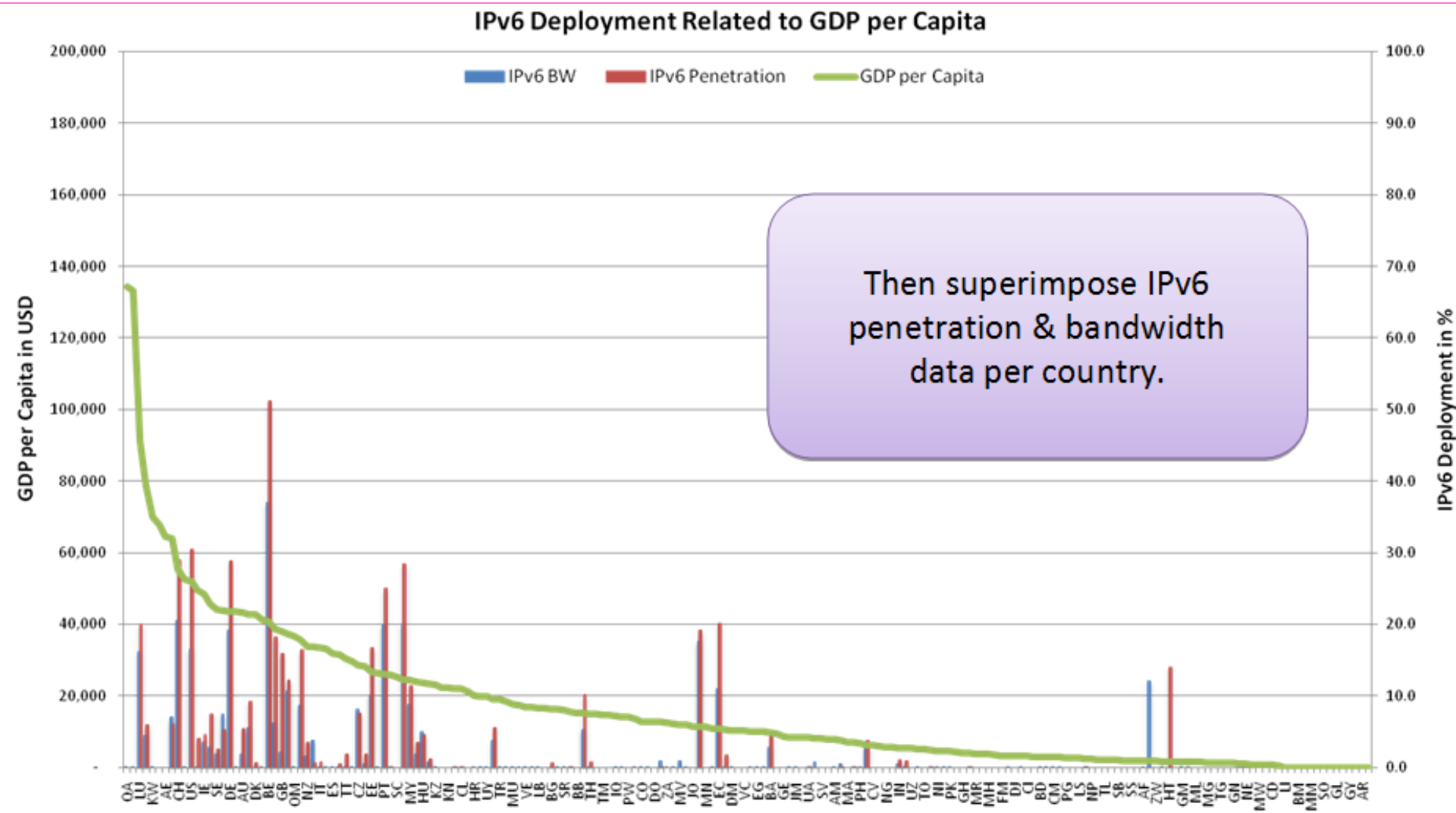
  防火墙管理控制，国内用户无法访问国外的IPv6资源

互联网体系结构委员会（IAB）声明

IAB建议IETF新标准放弃兼容IPv4 IPv6进入快车道 (2016-11-09 17:18:04) 转载

标签： gntc it 互联网 科技 ipv6

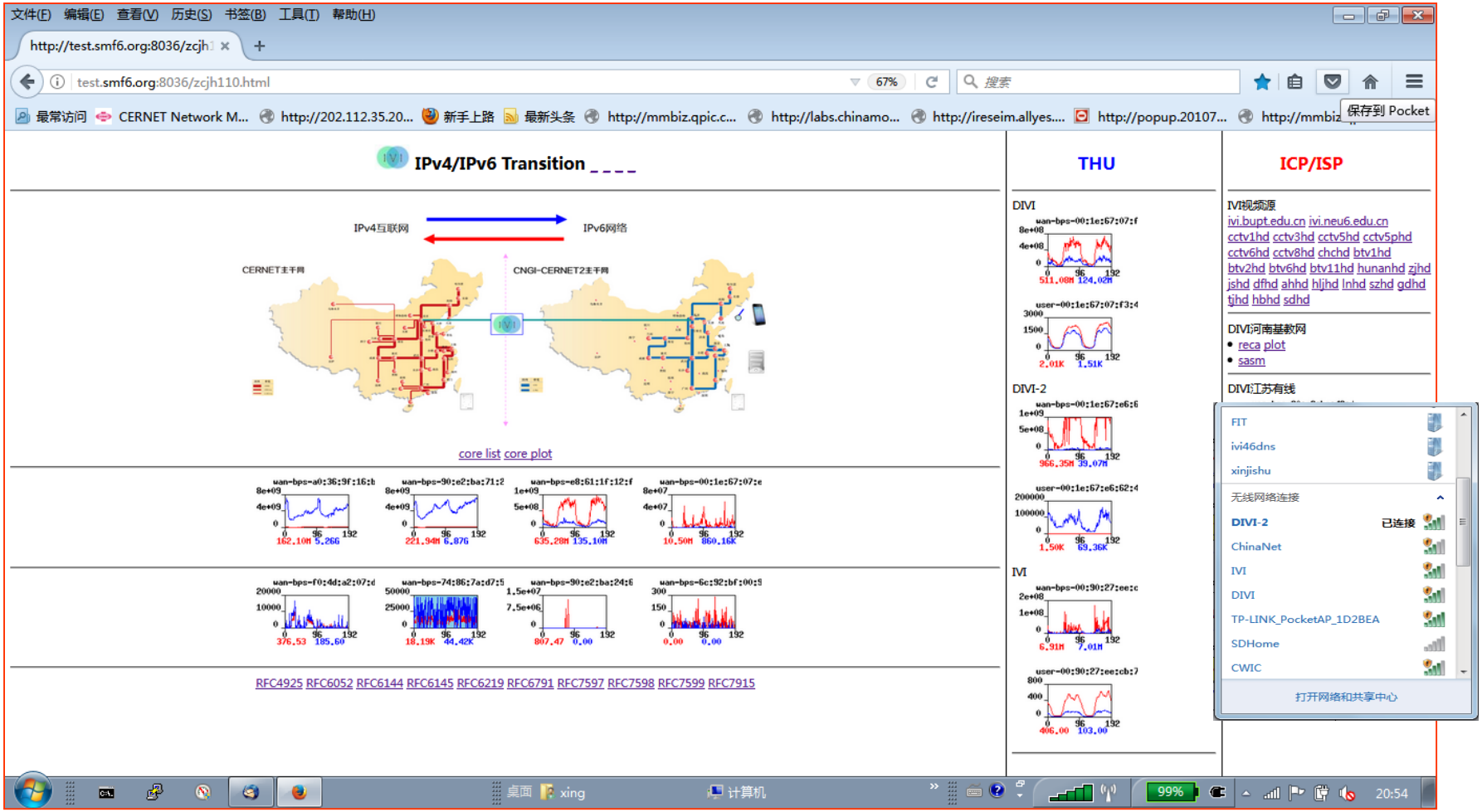
11月7日，互联网架构委员会IAB官方正式发布关于推进IPv6部署的声明，建议IETF等标准开发组织及合作伙伴放弃在新协议标准中兼容IPv4，用行动支持并实施IPv6在全球范围内的部署。2016年12月7日，“GNTC全球网络技术大会”将联合IAB、APNIC等机构举办“IPv6 Summit”，全面研讨未来IPv6发展趋势，推动产业发展。



IPv4 will still be very relevant for a long while

- The large number of countries with low GDP per capita that have very little or no IPv6 should tempers enthusiasm.

CERNET and CERNET2



IPv6校园网部署方案

Projected to 2051 (?!)

Characteristic	1981	2016	2051
Backbone Channel Capacity	5 x 10^4 bps	10^{11} bps	2x10^{17} bps
Personal Computer Storage	< 10^6 bytes	~10^{12} bytes	~10^{18}
Telecomm Service Providers	~10^2	~10^4 (?)	10^6
Computers/User	~0.1	~10	10^3
Computers Connected	~10^4	10^9+	10^{14}

Conclusion: We will not get there with the IP paradigm (naming host interfaces, datagram service) as the interoperability layer.

分析

1. 网络安全是全球性的问题
2. 网络安全是国家重大需求
3. 网络安全极其复杂
4. 网络安全专业性极强（技术手段）
5. 网络安全有规模效应
6. IPv6是网络安全的新战场
7. 教育单位的困境
8. 网络安全是持续过程
9. 人才是根本


命令提示符
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\bigcat>nslookup bbs.tsinghua.edu.cn
服务器: a.centerdns.jscndata.net
Address: 111.208.55.6
非权威应答:
名称: bbs.tsinghua.edu.cn
Address: 166.111.8.238
C:\Users\bigcat>ping bbs.tsinghua.edu.cn
正在 Ping bbs.tsinghua.edu.cn [166.111.8.238] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。
166.111.8.238 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
C:\Users\bigcat>

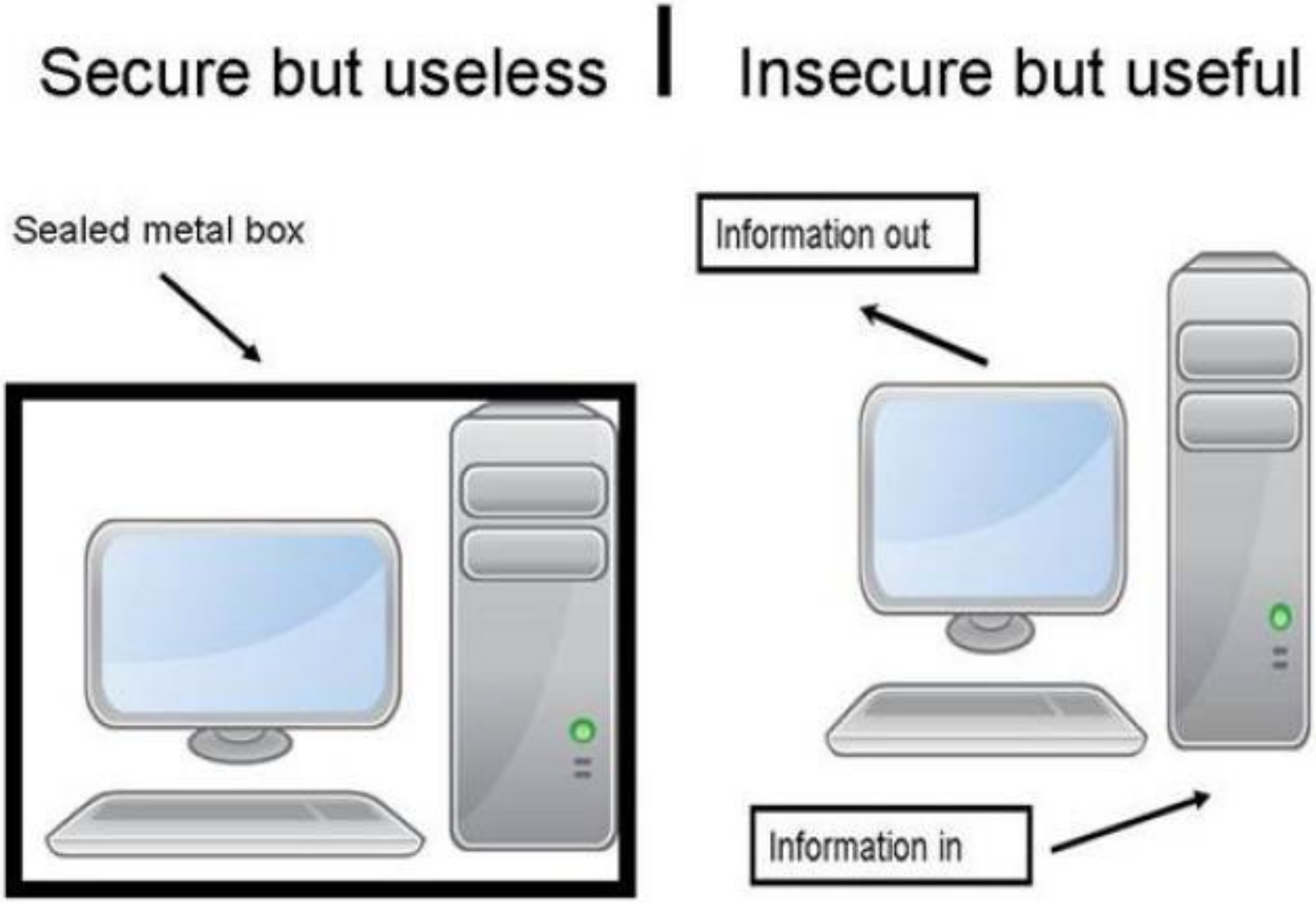
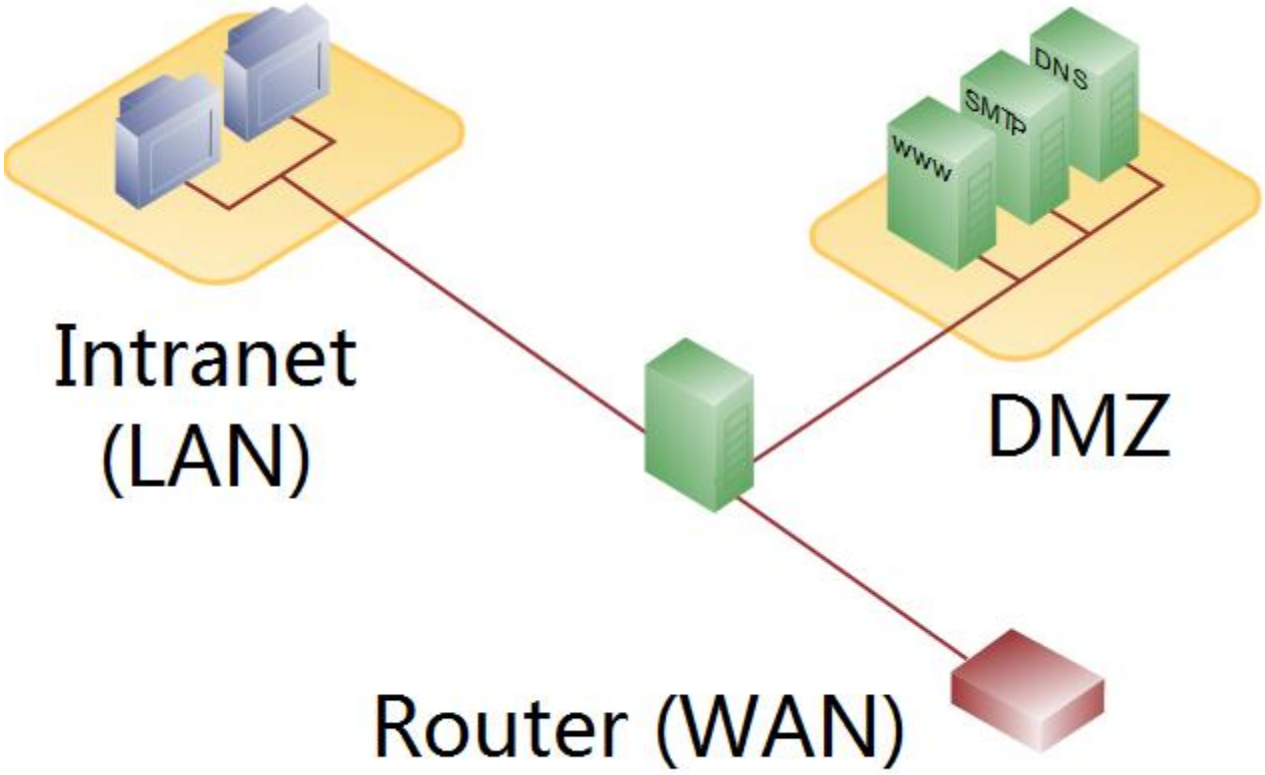


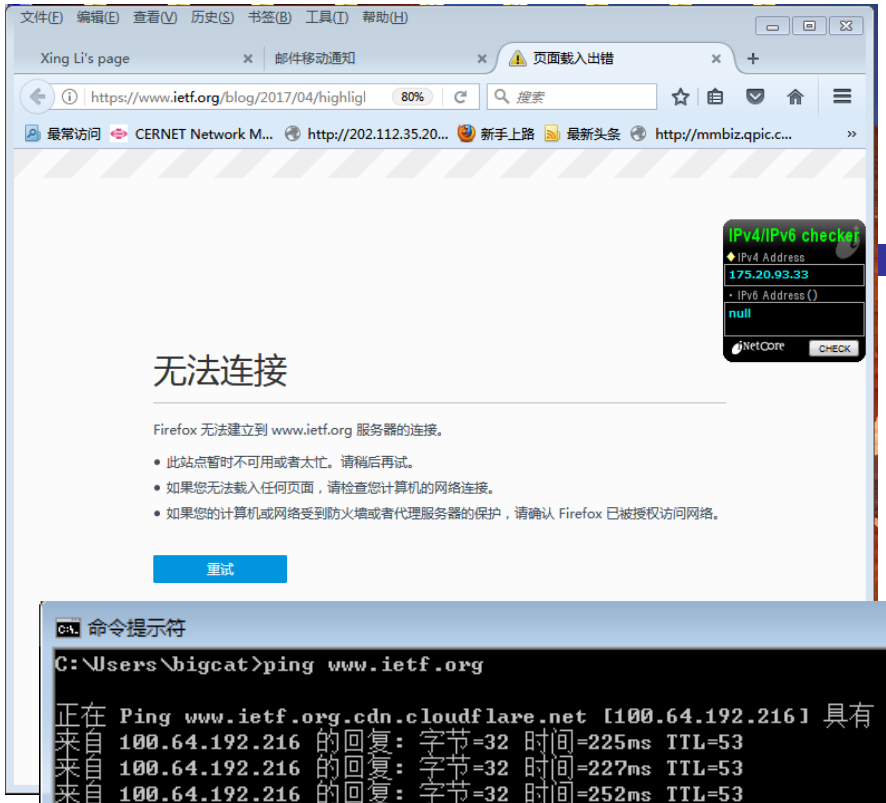
FIGURE 3.1 A secure but useless computer, and an insecure but useful computer.

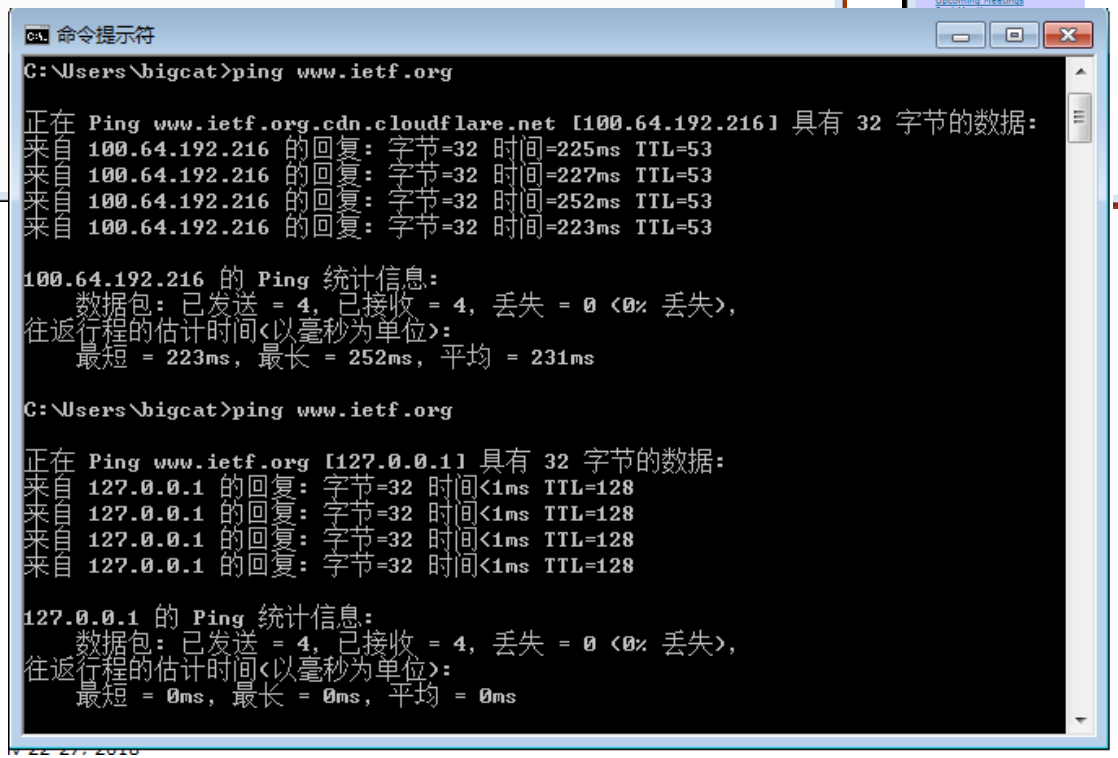
ScienceDMZ6

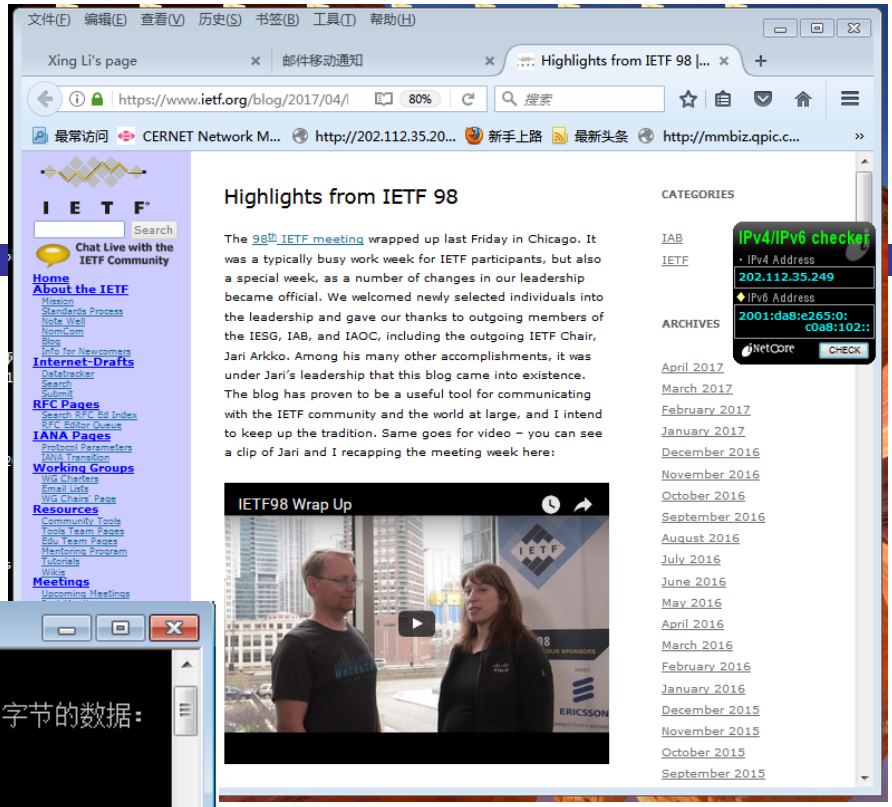


分析

1. 网络安全是全球性的问题
2. 网络安全是国家重大需求
3. 网络安全极其复杂
4. 网络安全专业性极强（技术手段）
5. 网络安全有规模效应
6. IPv6是网络安全的新战场
7. 教育单位的困境
8. 网络安全是持续过程
9. 人才是根本


文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)
Xing Li's page
邮件移动通知
页面载入出错
https://www.ietf.org/blog/2017/04/highligl
80%
搜索
最常访问
CERNET Network M...
http://202.112.35.20...
新手上路
最新头条
http://mmbiz.qpic.c...
IPv4/IPv6 checker
IPv4 Address
175.20.93.33
IPv6 Address ()
null
NetCore
CHECK
无法连接
Firefox 无法建立到 www.ietf.org 服务器的连接。
• 此站点暂时不可用或者太忙。请稍后再试。
• 如果您无法载入任何页面，请检查您计算机的网络连接。
• 如果您的计算机或网络受到防火墙或者代理服务器的保护，请确认 Firefox 已被授权访问网络。
重试


命令提示符
C:\Users\bigcat>ping www.ietf.org
正在 Ping www.ietf.org.cdn.cloudflare.net [100.64.192.216] 具有 32 字节的数据:
来自 100.64.192.216 的回复: 字节=32 时间=225ms TTL=53
来自 100.64.192.216 的回复: 字节=32 时间=227ms TTL=53
来自 100.64.192.216 的回复: 字节=32 时间=252ms TTL=53
来自 100.64.192.216 的回复: 字节=32 时间=223ms TTL=53
100.64.192.216 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 223ms, 最长 = 252ms, 平均 = 231ms
C:\Users\bigcat>ping www.ietf.org
正在 Ping www.ietf.org [127.0.0.1] 具有 32 字节的数据:
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
127.0.0.1 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms


文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)
Xing Li's page
邮件移动通知
Highlights from IETF 98 |...
https://www.ietf.org/blog/2017/04/
80%
搜索
最常访问
CERNET Network M...
http://202.112.35.20...
新手上路
最新头条
http://mmbiz.qpic.c...
IETF
Search
Chat Live with the IETF Community
Home
About the IETF
Internet-Drafts
RFC Pages
IANA Pages
Working Groups
Resources
Meetings
Highlights from IETF 98
The 98th IETF meeting wrapped up last Friday in Chicago. It was a typically busy work week for IETF participants, but also a special week, as a number of changes in our leadership became official. We welcomed newly selected individuals into the leadership and gave our thanks to outgoing members of the IESG, IAB, and IAOC, including the outgoing IETF Chair, Jari Arkko. Among his many other accomplishments, it was under Jari's leadership that this blog came into existence. The blog has proven to be a useful tool for communicating with the IETF community and the world at large, and I intend to keep up the tradition. Same goes for video – you can see a clip of Jari and I recapping the meeting week here:
IETF98 Wrap Up
CATEGORIES
IAB
IETF
ARCHIVES
April 2017
March 2017
February 2017
January 2017
December 2016
November 2016
October 2016
September 2016
August 2016
July 2016
June 2016
May 2016
April 2016
March 2016
February 2016
January 2016
December 2015
November 2015
October 2015
September 2015
IPv4/IPv6 checker
IPv4 Address
202.112.35.249
IPv6 Address
2001:da8:e265:0:c0a8:102::
NetCore
CHECK

分析

1. 网络安全是全球性的问题
2. 网络安全是国家重大需求
3. 网络安全极其复杂
4. 网络安全专业性极强（技术手段）
5. 网络安全有规模效应
6. IPv6是网络安全的新战场
7. 教育单位的困境
8. 网络安全是持续过程
9. 人才是根本

网络人才战略

互联网主要是年轻人的事业，要不拘一格降人才。要解放思想，慧眼识才，爱才惜才。培养网信人才，要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院。互联网领域的人才，不少是怪才、奇才，他们往往不走一般套路，有很多奇思妙想。**对待特殊人才要有特殊政策，不要求全责备，不要论资排辈，不要都用一把尺子衡量。**

去中心化网络

- 你可以让围墙花园变得非常动人，但从长远来看，外面的丛林永远都是更有吸引力的那一个。

  – Tim Berners-Lee

Open Internet

Open Process

- 开放的协议（Open protocol）
- 开放的实现（Open implementation）
- 开放的系统（Open system）

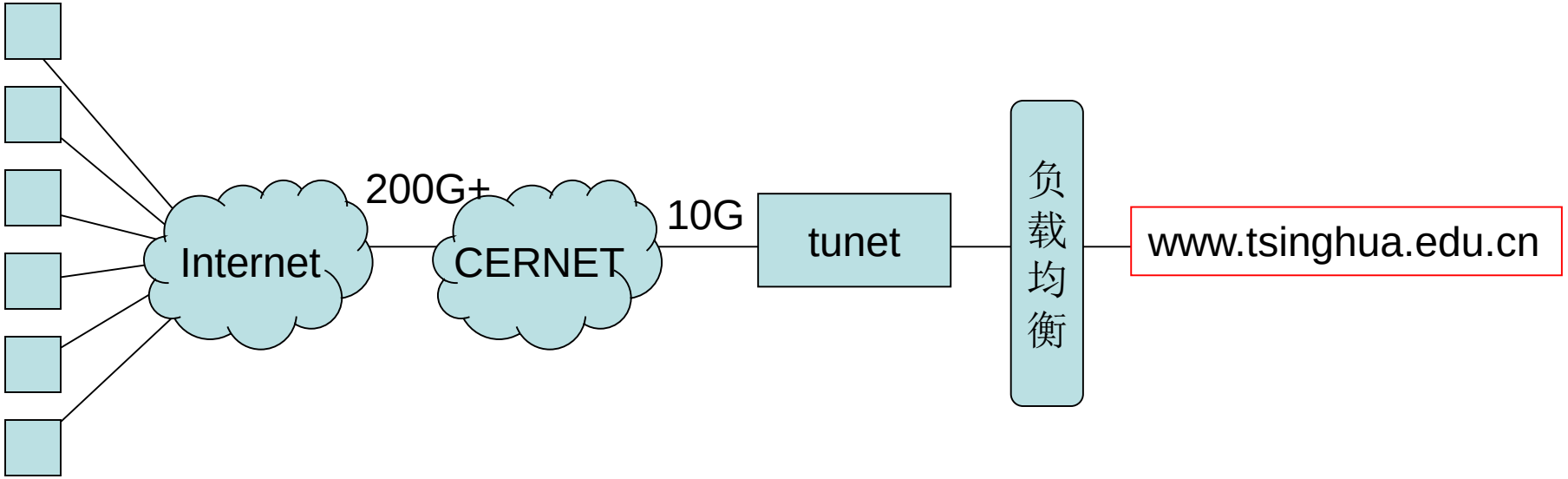
Great people

创新

- ✓ **Reality:** Internet advances at a rate that far exceeds government ability to keep pace

行动计划

抗DDOS



2016	DDOS	500G
2017	DDOS	1T

IPv6

RFC791

RFC: 791

INTERNET PROTOCOL

DARPA INTERNET PROGRAM

PROTOCOL SPECIFICATION

September 1981

RFC2460

Network Working Group
Request for Comments: 2460
Obsoletes: 1883
Category: Standards Track

S. Deering
Cisco
R. Hinden
Nokia
December 1998

Internet Protocol, Version 6 (IPv6)
Specification

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1998). All Rights Reserved.

Abstract

This document specifies version 6 of the Internet Protocol (IPv6), also sometimes referred to as IP Next Generation or IPng.

RFC6145

Internet Engineering Task Force (IETF)
Request for Comments: 6145
Obsoletes: 2765
Category: Standards Track
ISSN: 2070-1721

X. Li
C. Bao
CERNET Center/Tsinghua University
F. Baker
Cisco Systems
April 2011

IP/ICMP Translation Algorithm

Abstract

This document describes the Stateless IP/ICMP Translation Algorithm (SIIT), which translates between IPv4 and IPv6 packet headers (including ICMP headers). This document obsoletes RFC 2765.

RFC4291

Network Working Group
Request for Comments: 4291
Obsoletes: 3513
Category: Standards Track

R. Hinden
Nokia
S. Deering
Cisco Systems
February 2006

IP Version 6 Addressing Architecture

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This specification defines the addressing architecture of the IP Version 6 (IPv6) protocol. The document includes the IPv6 addressing model, text representations of IPv6 addresses, definition of IPv6 unicast addresses, anycast addresses, and multicast addresses, and an IPv6 node's required addresses.

RFC6052

Internet Engineering Task Force (IETF)
Request for Comments: 6052
Updates: 4291
Category: Standards Track
ISSN: 2070-1721

C. Bao
CERNET Center/Tsinghua University
C. Huitema
Microsoft Corporation
M. Bagnulo
UC3M
M. Boucadair
France Telecom
X. Li
CERNET Center/Tsinghua University
October 2010

IPv6 Addressing of IPv4/IPv6 Translators

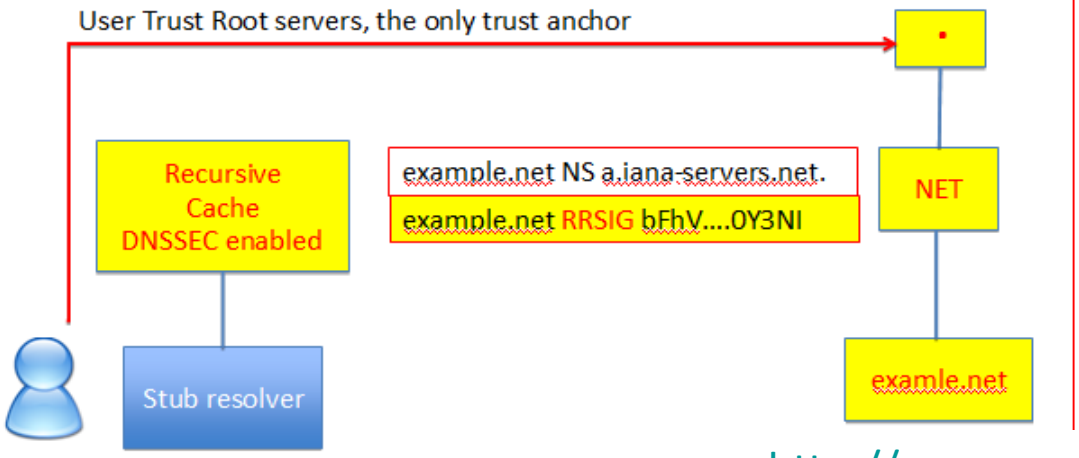
Abstract

This document discusses the algorithmic translation of an IPv6 address to a corresponding IPv4 address, and vice versa, using only statically configured information. It defines a well-known prefix for use in algorithmic translations, while allowing organizations to also use network-specific prefixes when appropriate. Algorithmic translation is used in IPv4/IPv6 translators, as well as other types of proxies and gateways (e.g., for DNS) used in IPv4/IPv6 scenarios.

DNSSec

host.txt → DNS → Anycast DNS → IPv6 root → **DNSSEC** → IANA transition

- Clients (resolvers) validate the signature with their public keys
- Servers sign all the DNS records with their private Keys



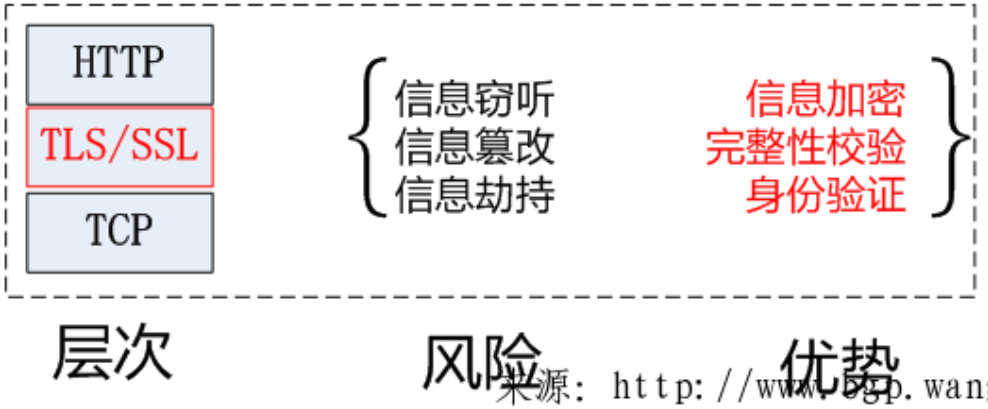
Recovery Key Share Holders

- 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

https

HTTPS = HTTP + TLS/SSL



来源：http://www.ogp.wang