端到端安全协议的威胁、演进和部署

郑晓峰
360企业安全技术研究院

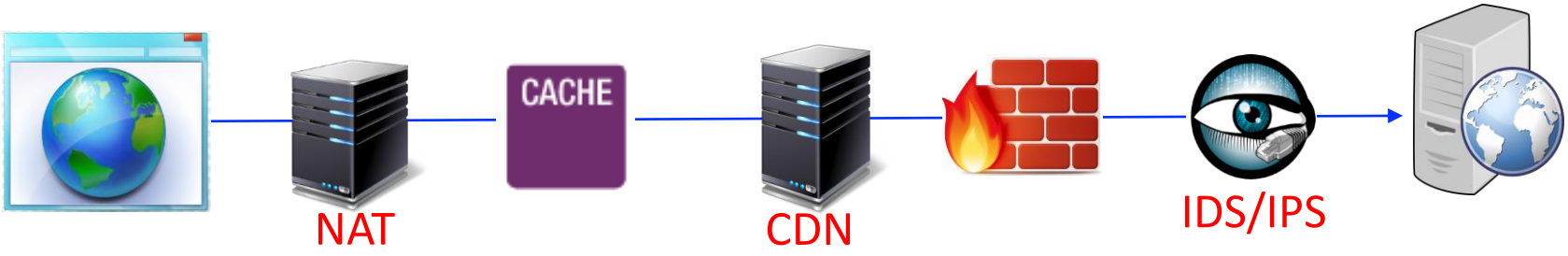
端到端原则

- 端到端的原则出现在以下权威的文献中
  - Saltzer, J. H., Reed, D. P., & Clark, D. D. 系统设计中的端到端观点, ACM TOCS,1981
  - Clark, D. D. DARPA互联网协议设计原则, CCR,1995
  - Carpenter, B.,互联网体系结构原则, RFC 1958,1996
  - Carpenter, B., 互联网透明性, RFC 2775, 2000

- 端到端原则的批评和反思
  - Blumenthal, S. & Clark, D，重新考虑互联网体系结构的设计, ACM TOIT,2001
  - Moors, T.，关于“系统设计端到端观点”的批评. ICC,2002
  - Clark, D. and etc. 扭斗的网络空间:定义明天的互联网, SIGCOMM,2002
  - J. Kempf，中间盒子的兴起与端到端的未来, RFC3724, 2004

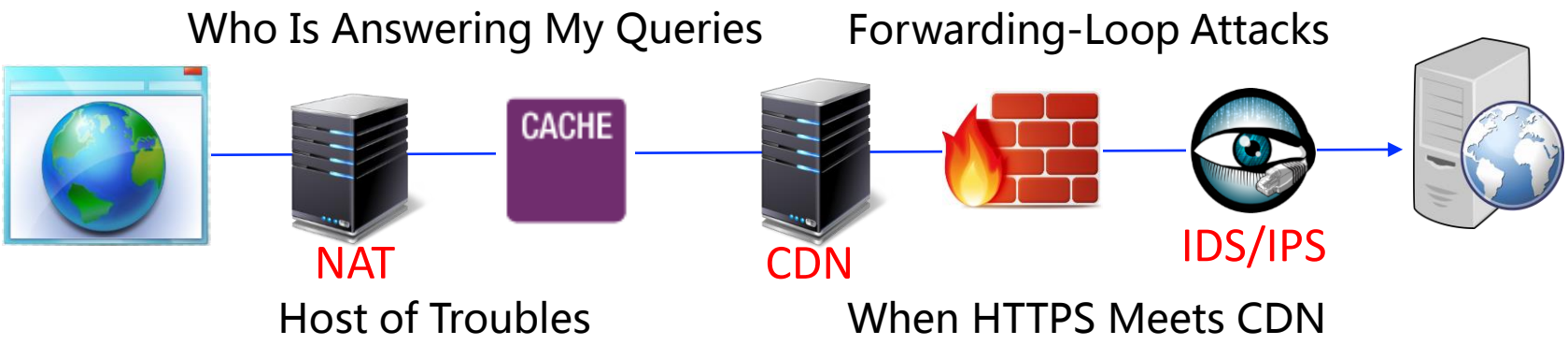
中间盒子(Middle Box)的兴起

- 变化是互联网唯一不变的设计原则[RFC1958]
- UCLA教授张丽霞提出中间盒子
- 中间盒子的分类（RFC 3234, 2002）
  - 性能：DNS 缓存、HTTP 代理/缓存、CDN
  - 协议转换：NAT, IPv4-IPv6
  - 安全保护： 防火墙、入侵检测/入侵防护系统



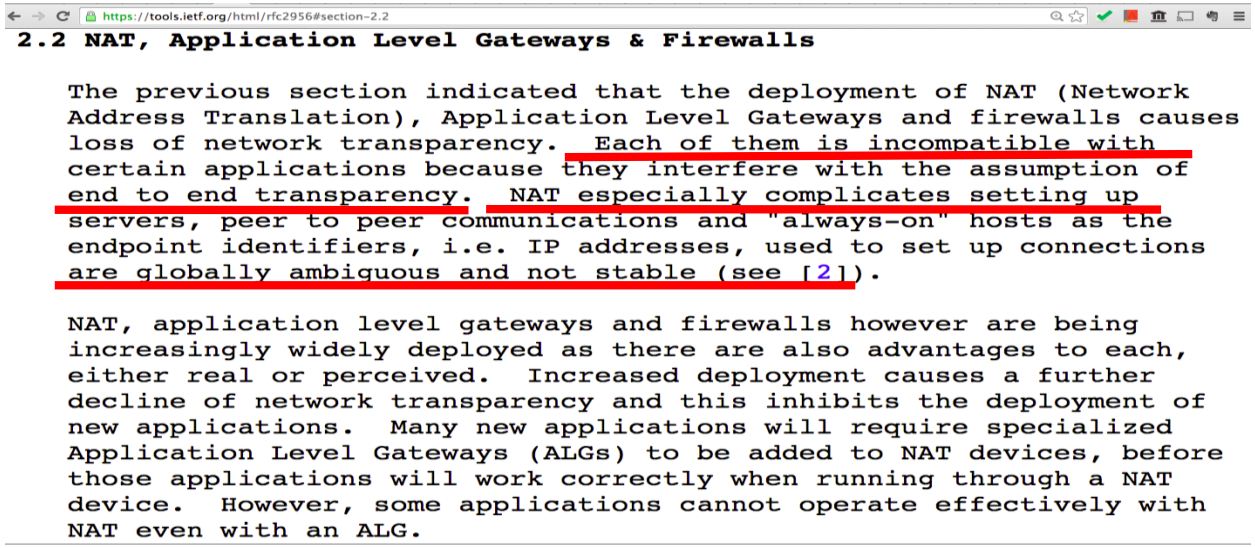
中间盒子所带来的安全威胁

- 增加了网络和应用的复杂性，NAT
- 增加了攻击面，通过攻击网络而影响端系统
- 协议理解和实现的不一致性
- 没有一个集中的协调机构验证协议的部署和事实



NAT的野蛮生长

- 在NAT蓬勃发展的初期，IETF对NAT的部署有很大争议
- IAB Network Layer workshop(RFC 2956, 1999)



https://tools.ietf.org/html/rfc2956#section-2.2

2.2 NAT, Application Level Gateways & Firewalls

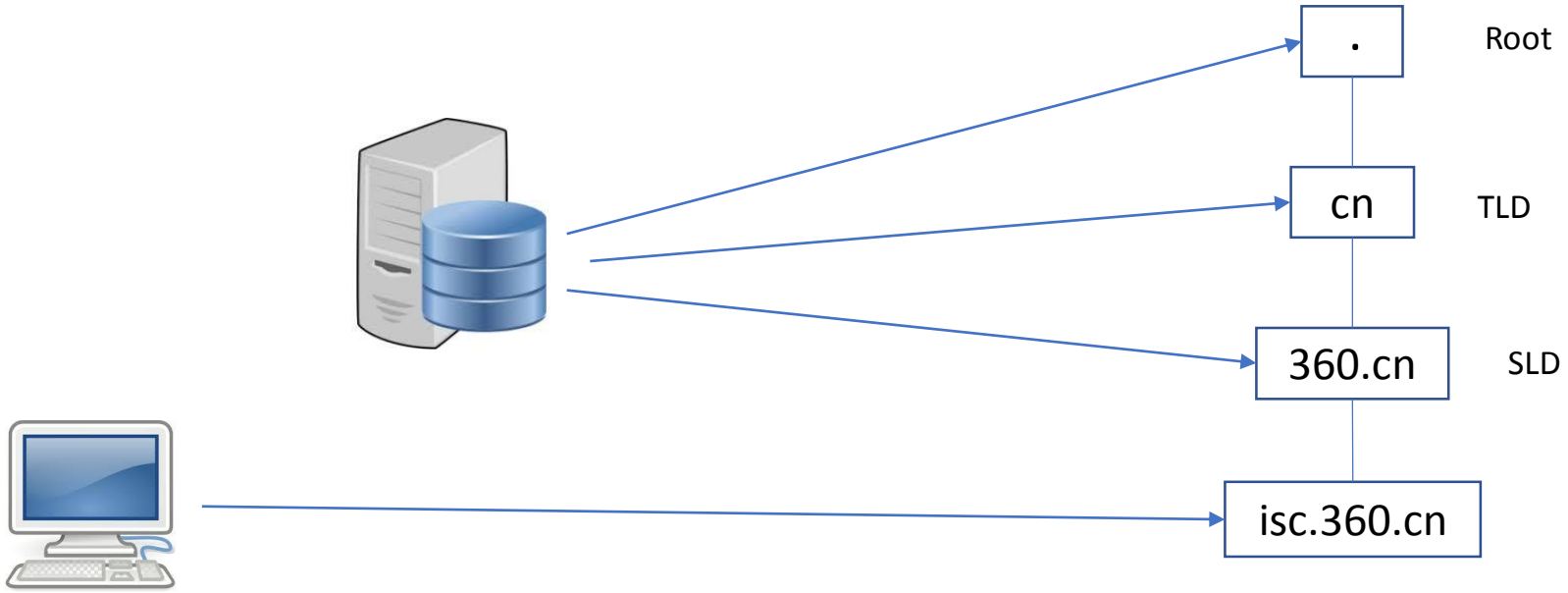
The previous section indicated that the deployment of NAT (Network Address Translation), Application Level Gateways and firewalls causes loss of network transparency. Each of them is incompatible with certain applications because they interfere with the assumption of end to end transparency. NAT especially complicates setting up servers, peer to peer communications and "always-on" hosts as the endpoint identifiers, i.e. IP addresses, used to set up connections are globally ambiguous and not stable (see [2]).

NAT, application level gateways and firewalls however are being increasingly widely deployed as there are also advantages to each, either real or perceived. Increased deployment causes a further decline of network transparency and this inhibits the deployment of new applications. Many new applications will require specialized Application Level Gateways (ALGs) to be added to NAT devices, before those applications will work correctly when running through a NAT device. However, some applications cannot operate effectively with NAT even with an ALG.

- 张丽霞：NAT技术的教训
  - “今天大多数人认同IETF最初没有标准化NAT是错误的。为什么错过了机会？简单来说是由于当时一切都不明朗。”
  - IETF对部署一个新的协议——IPv6过于乐观
  - IETF当时对工程上的妥协（trade-off）缺乏足够的理解

DNS生态系统

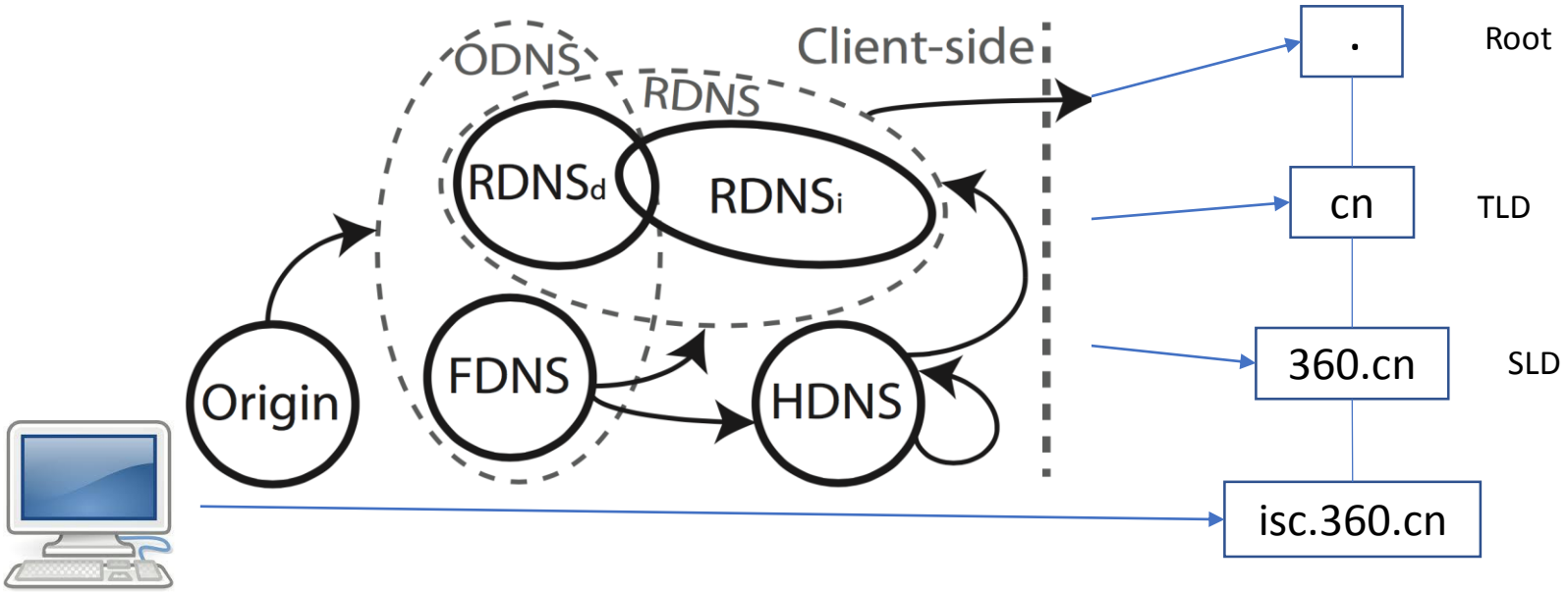
- Client , Cache, Server



K. Schomp, T. Callahan, M. Rabinovich & M. Allman, “On Measuring the Client-Side DNS Infrastructure,” *IMC 2013*

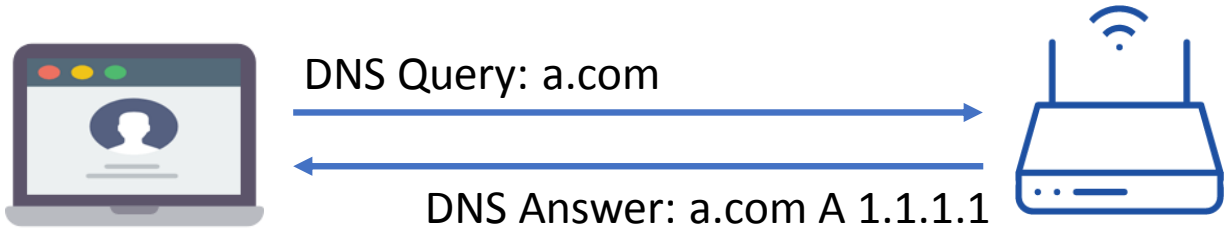
DNS生态系统

- Client , Cache, Server



K. Schomp, T. Callahan, M. Rabinovich & M. Allman, “On Measuring the Client-Side DNS Infrastructure,” *IMC 2013*

DNS劫持：一个古老的话题



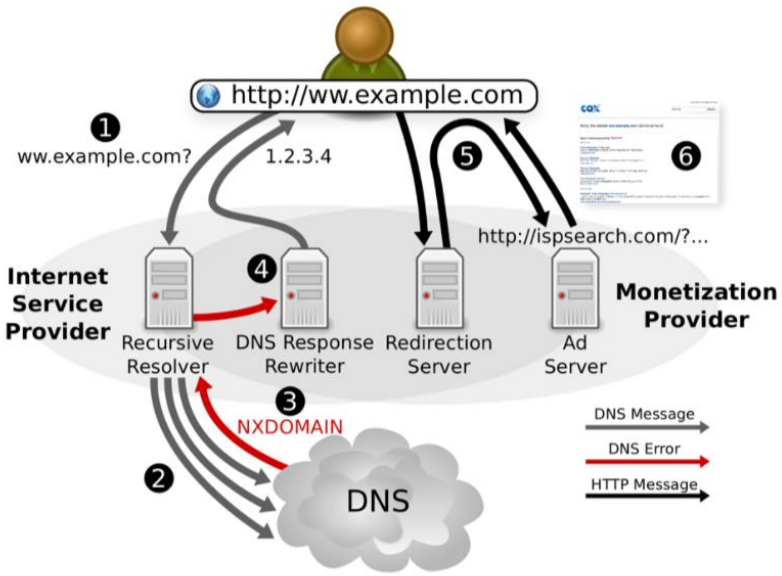
Xiaomi: miwifi.com
TP-Link: tplogin.cn
Netgear: www.routerlogin.net

```
[root@XiaoQiang:~# cat /tmp/etc/dnsmasq.d/apk_query.conf
ipset=/!server.m.pp.cn/apk_query
ipset=/!api-shoulei-ssl.xunlei.com/apk_query
ipset=/!m.gdown.baidu.com/apk_query
ipset=/qd.shouji.360tpcdn.com/apk_query
ipset=/m.sogou.com/apk_query
ipset=/so.m.sm.cn/apk_query
ipset=/dl.zhushou.sogou.com/apk_query
ipset=/act1.lianwifi.com/apk_query
ipset=/fast.yingyonghui.com/apk_query
ipset=/appstore.vivo.com.cn/apk_query
[root@XiaoQiang:~# iptables-save | grep apk_query
-A fwmark -p tcp -m set --match-set apk_query dst -m comment --comment apk_query -j MARK --set-xmark 0x40/0x40
```

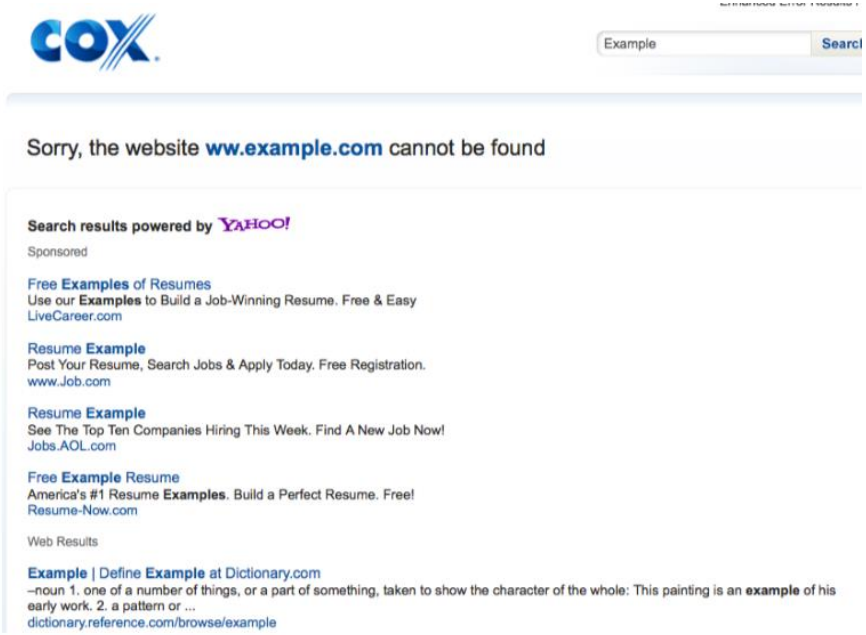
```
[root@XiaoQiang:~# cat /tmp/etc/dnsmasq.d/cache_center.dnsmasq
ipset=/formi.baidu.com/formibaidu
[root@XiaoQiang:~# iptables-save | grep formibaidu
-A PREROUTING -i br-lan -p tcp -m tcp --dport 8843 -m set --match-set formibaidu dst -j REDIRECT --to-ports 8099
```

运营商流量操控

ISP等修改域名响应的NXDOMAIN赚钱



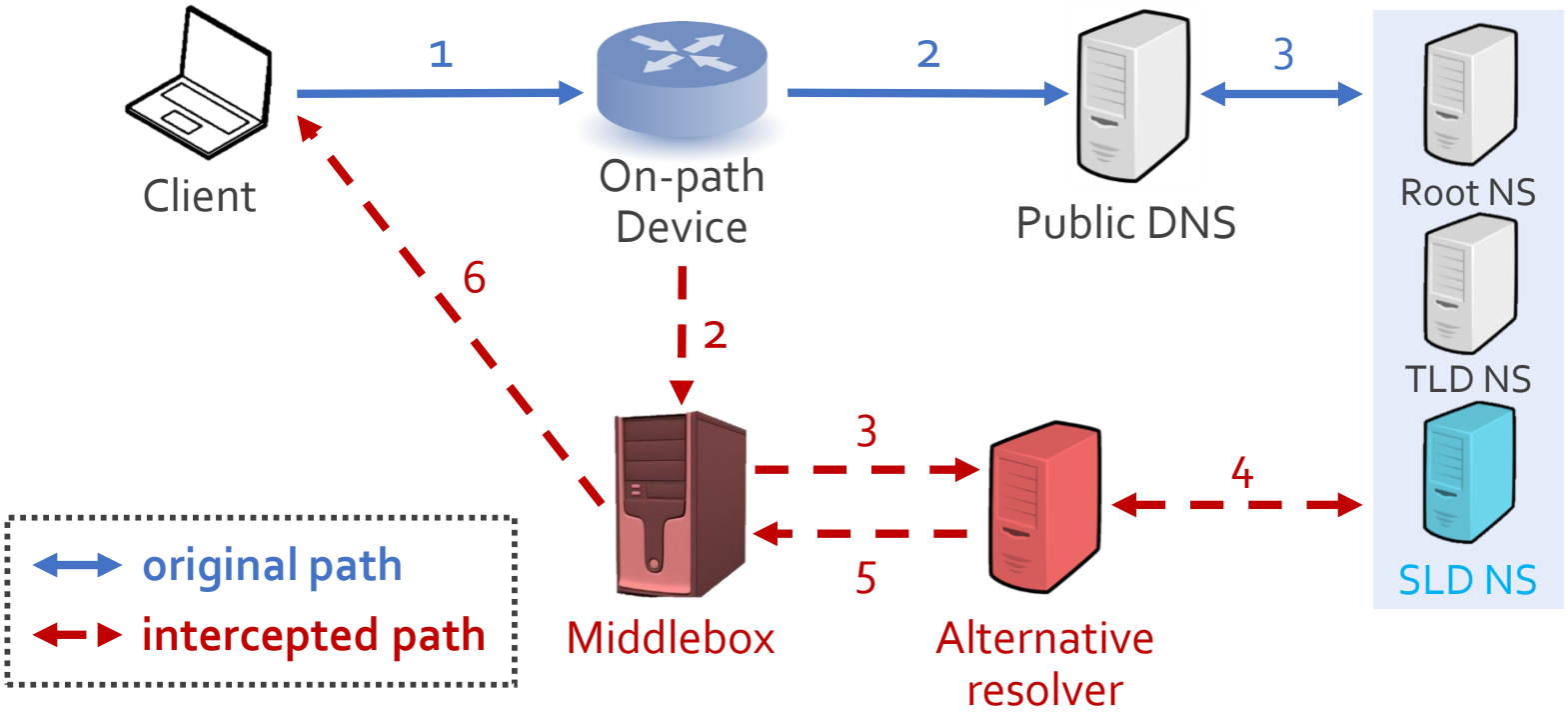
NXDomain修改可使ISP增加 1-3美元/用户/年



ICANN 强烈谴责这种行为[SAC 032,2008]

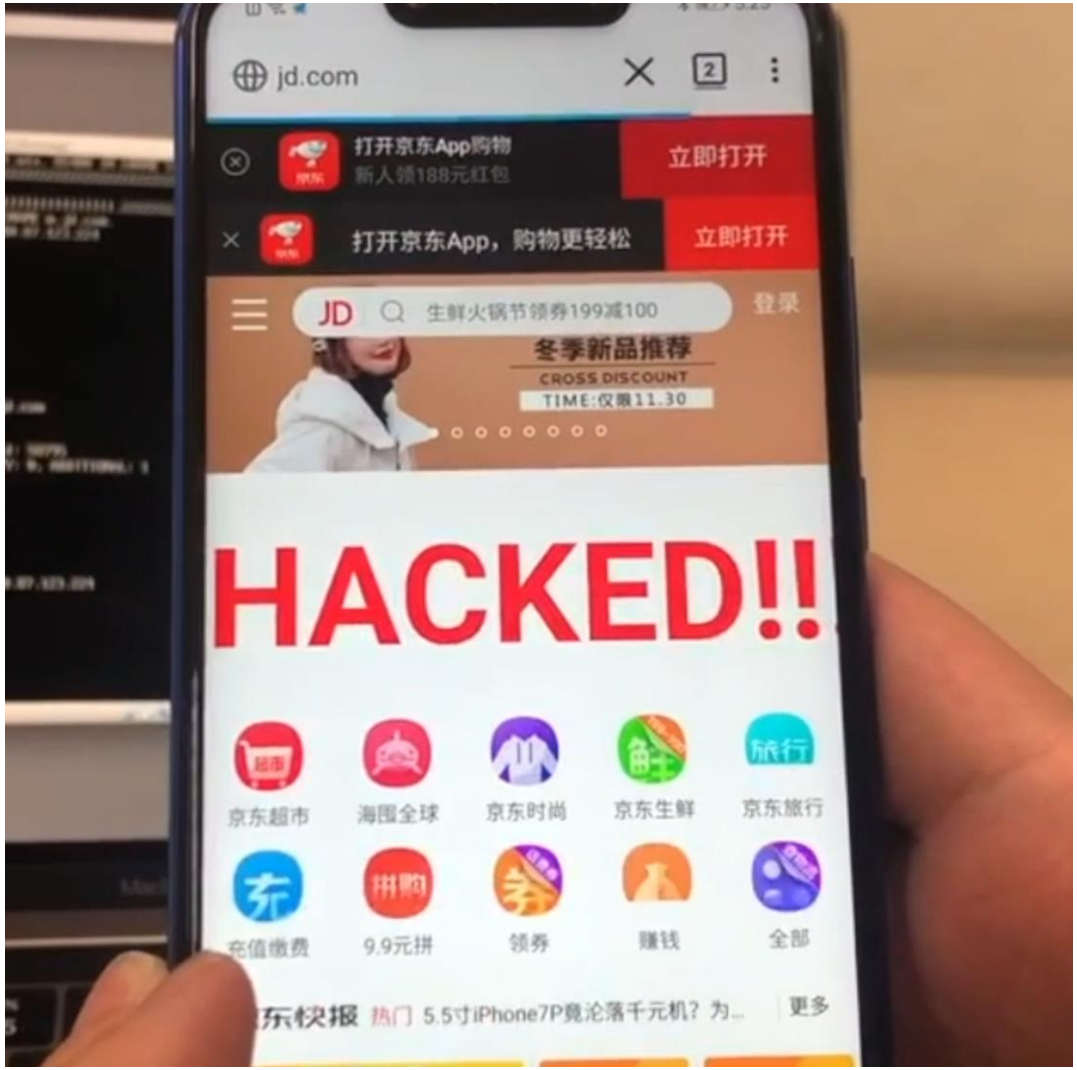
N. Weaver, V. Paxson, and C. Kreibich, “Redirecting DNS for Ads and Profit,” FOCI 2011.

公共DNS劫持



Baojun L., Chaoyi L., HaiXin D., Ying L., Zhou L., Shuang H., Min Y: Who Is Answering My Queries. USENIX Sec 2018

DNS缓存污染：古老却顽固的存在

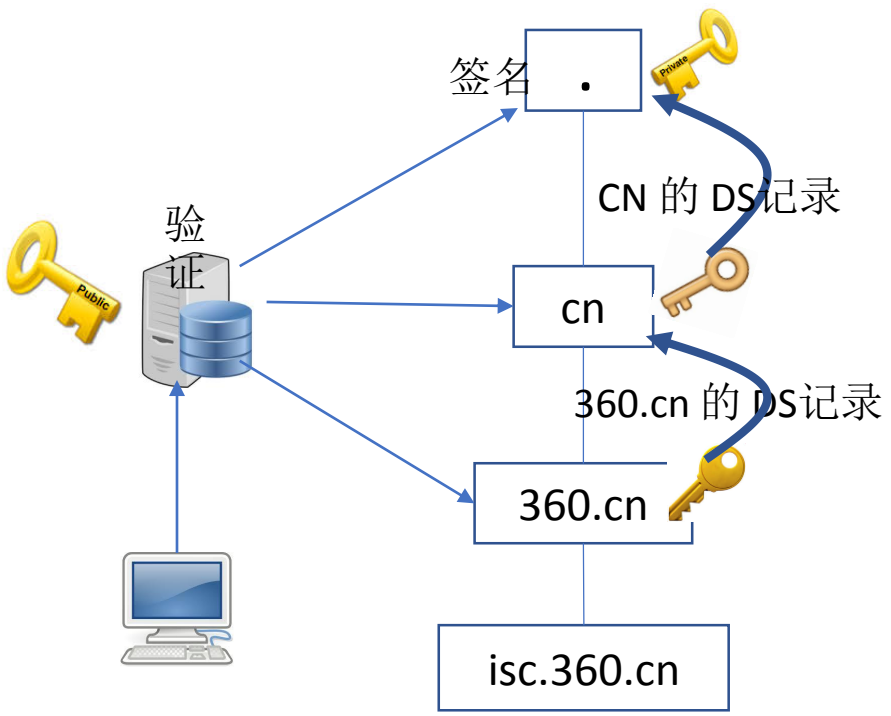


基础协议缺陷导致通用DNS缓存污染

@GeekPwn2018

解决之道：DNSSEC

- DNSSEC: 完整性
  - 公开密钥：数字签名、验证
  - DNSSEC PKI



Paul Vixie, June 1995:

DNSSEC看似简单，但是对协议和实现影响很大——所以选择安全模型和设计方案用了一年时间。我们估计还要一年时间DNSSEC才能用在前沿领域，之后，至少再用一年时间才能用在一般的地方

BIND 8.2 blurb, March 1999:

[Top feature:] Preliminary DNSSEC.

BIND 9 blurb, September 2000:

[Top feature:] DNSSEC.

DNSSEC标准的制定和部署

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?" ...

我们现在还在做基础的研究工作：
究竟哪种数据模型对DNS安全可以工作。

"我们终于搞定了，这次是真的"
我们已经这么说够三、四次了

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.

RFC2535标准死了，
我们从头开始

DNSSEC标准的制定和部署

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.

- 标准与实现
  - 1997, RFC 2065 (Obsoleted)
  - 1999, RFC 2535 (Obsoleted)
  - 2005, RFC 4033-5(alive)
  - 2008, RFC 5155 (NSEC3)
  - 2012, RFC 6698(DANE/TLSA)
- 部署与推广
  - 2007, INAN/ICANN signed root
  - 2010, Root签名
  - 2010, Comcast 大规模部署验证
  - 2016, 所有国家代码的顶级域（ccTLD）部署

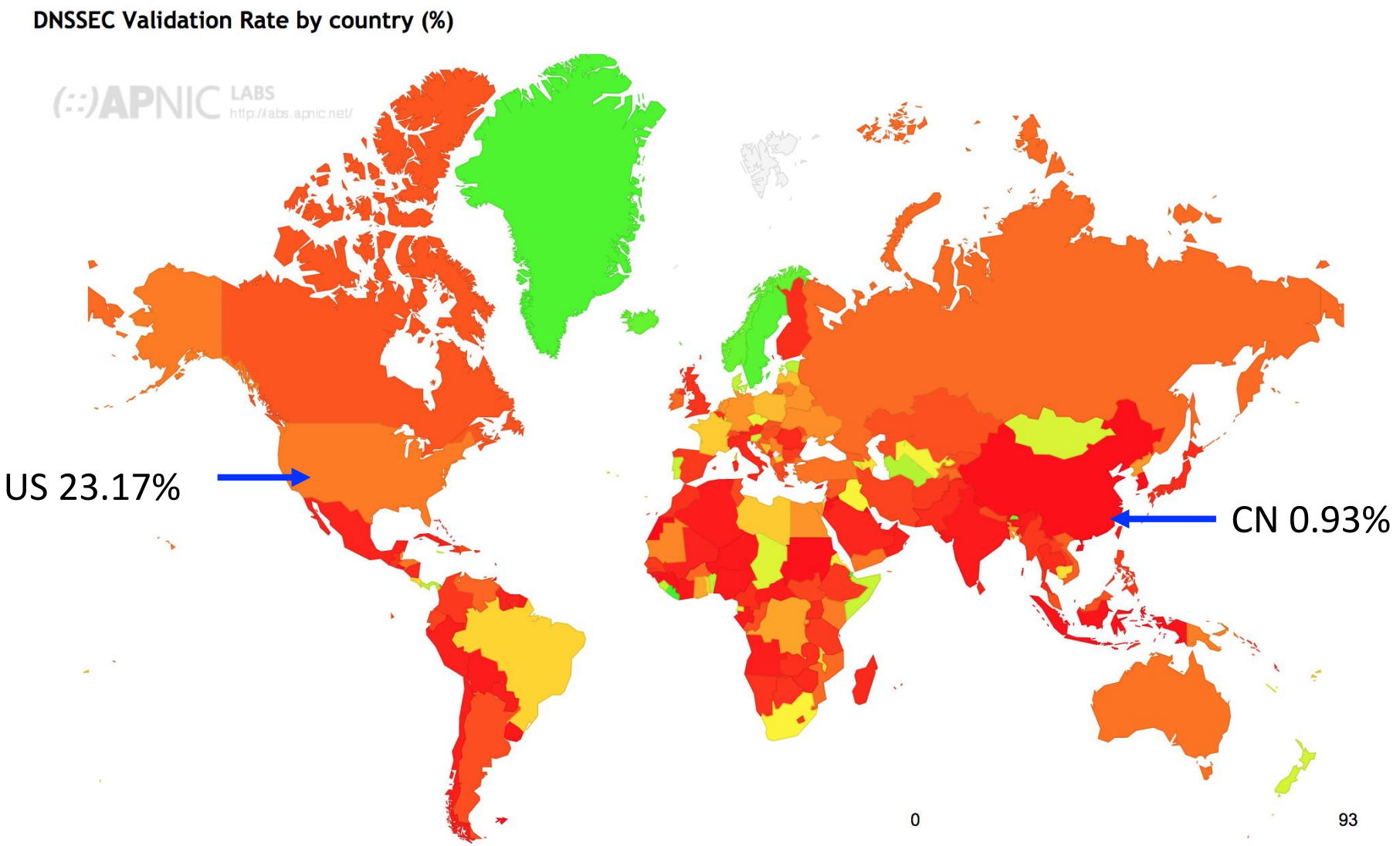
中美银行、政府、教育DNSSEC签名

域名类别	# 测试域名	#DNSSEC部署	部署比例	配置正确率
中国国内银行	996	0	0	0
美国国内银行	109	15	13.76%	100%
中国政府gov.cn	40,873	0	0	0
美国政府gov	5,379	1162	21.60%	99.05%
中国教育edu.cn	7,826	32	0.40%	0*
美国教育edu	7,311	150	2.05%	98.70%

EDU.CN 已经签名， 但DS记录没有上传到CN

域名数据来源： 360 Passive DNS 4年的数据; DNSSEC验证使用Google DNS

全球DNSSEC验证的比例



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

中美公共DNS服务器DNSSEC验证部署

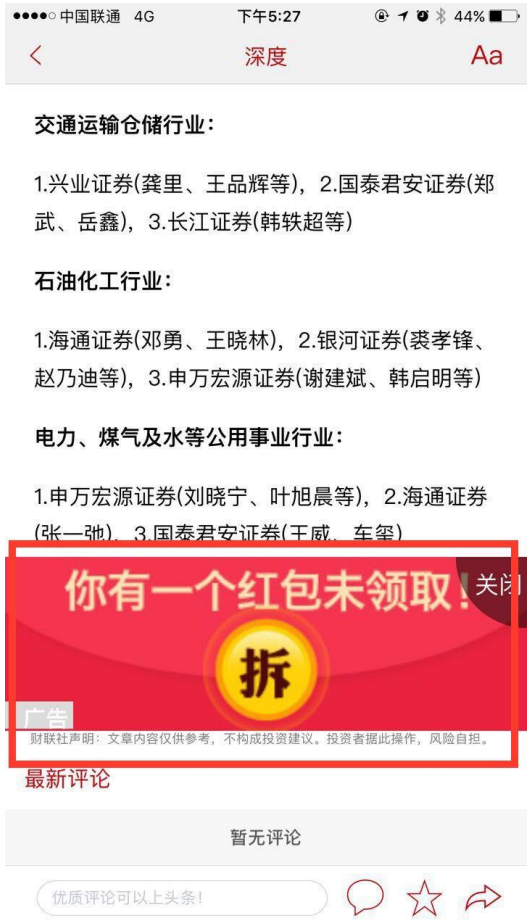
- 美国著名的公共DNS服务

运营商	IP地址	支持 DNSSEC	验证 DNSSEC
谷歌	8.8.8.8 8.8.4.4	是	是
思科 OpenDNS	208.67.220.220 208.67.222.222	否	NA
甲骨文 (Dyn)	216.146.35.35 216.146.36.36	是	是
Neustart	156.154.71.1 156.154.70.1 156.154.71.5 156.154.70.5	是	是
Level 3	4.2.2.2 4.2.2.1	是	否

- 中国著名的公共DNS服务

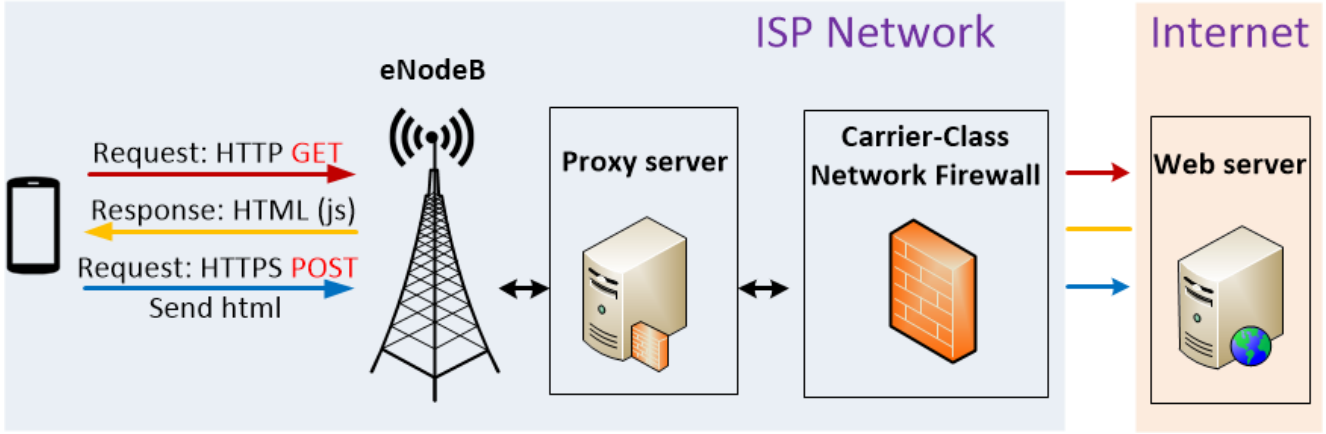
运营商	服务器地址	支持 DNSSEC	验证 DNSSEC
阿里巴巴	223.5.5.5，223.6.6.6	否	NA
百度	180.76.76.76	是	否
360 DNS 派	101.226.4.6, 218.30.118.6, 123.125.81.6,140.207.198.6, 101.226.4.6, 218.30.118.6, 101.226.4.6,218.30.118.6	否	NA
腾讯	119.29.29.29 182.254.118.118	否	NA
114DNS	114.114.114.114, 114.114.115.115	否	NA
SDNS（CNNIC）	1.2.4.8, 210.2.4.8	是	否
onedns	112.124.47.27, 114.215.126.16	否	NA
中华电信	168.95.192.1,168.95.1.1	是	否

HTTP，从流量劫持开始



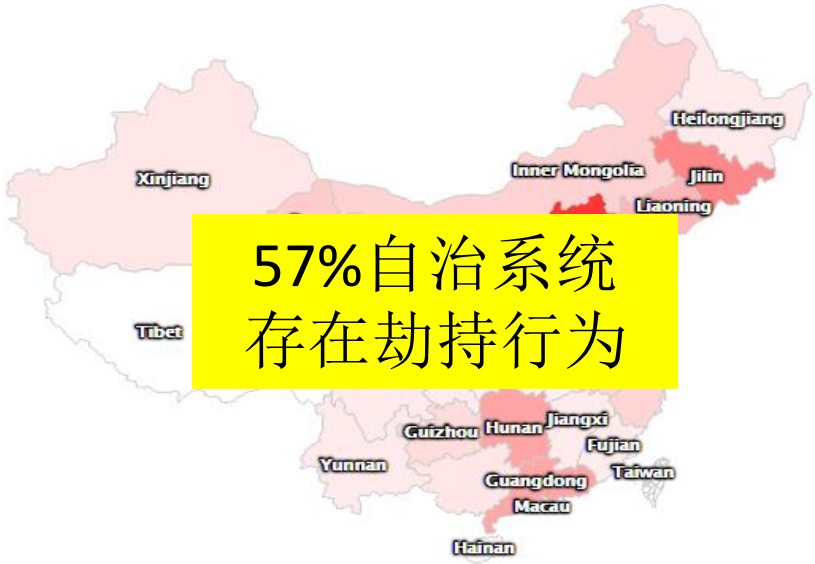
测量中国范围内移动网络中隐私泄露的威胁

移动设备



我们搭建的Web服务器

测试规模	数量	发生劫持
HTTP 会话数	33,439	1,291 (3.9%)
IP地址	30,810	451 (1.5%)
省	31	30 (97%)
自治系统（AS）	79	45 （57%）



57%自治系统存在劫持行为

Mingming Zhang, Baojun Liu, Chaoyi Lu, Jia Zhang, Shuang Hao, Haixin Duan. Measuring Privacy Threats in China-Wide Mobile Networks. 8th USENIX Workshop on Free and Open Communications on the Internet(FOCI), 2018

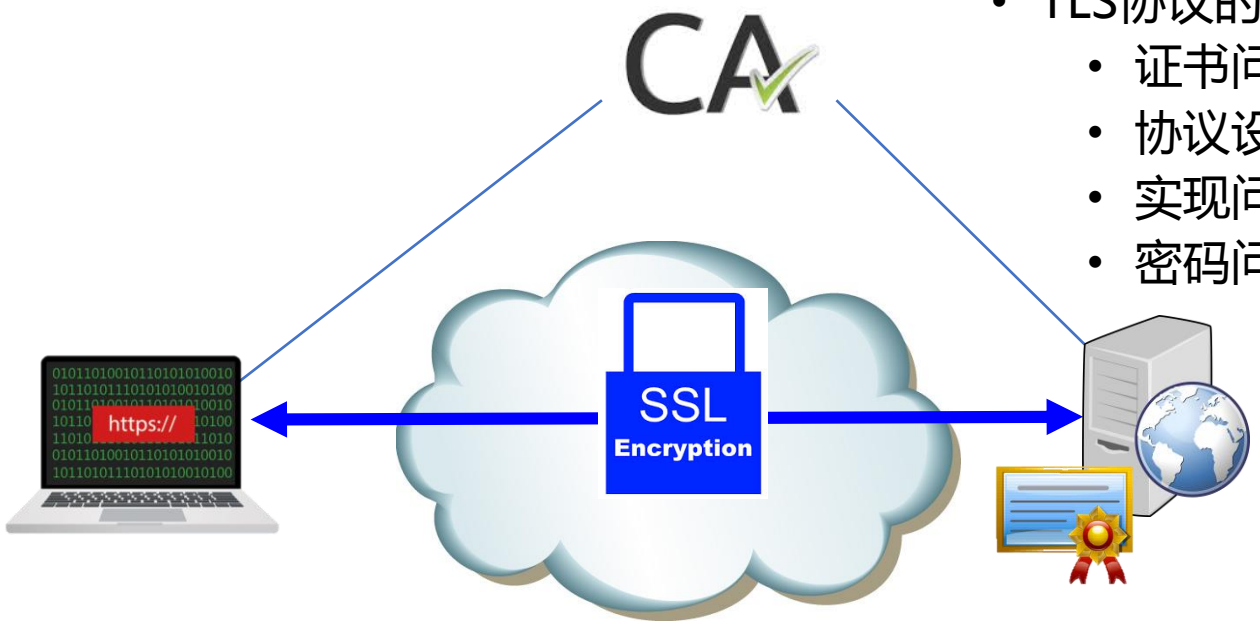
部分泄露用户隐私的HTTP Header

注入的Header	说明	劫持所发生的ISP	数量
x-IMEI*	手机序列号	ChinaMobile (GD)	12
x-IMSI*	国际移动用户标识	ChinaTelecom, ChinaUnicom	6
x-up-calling-line-id	用户手机号码	ChinaTelecom (SH, SN, QH, SC, XJ, GS, BJ, SD, LN, YN, NM, ZJ, AH), ChinaMobile (GD), ChinaUnicom (BJ, JL, LN)	50

HTTP安全，从HTTPS开始

- HTTPS: HTTP/TLS 或SSL
- 基于可信第三方 CA/ WebPKI
- 功能：认证、保密性、完整性

- SSL/TLS历史发展
  - 1995, SSL 2.0 发布
  - 1996, SSL 3.0 RFC 6160
  - 1999, TLS 1.0 RFC 2246
  - 2006, TLS 1.1 RFC 4346
  - 2008, TLS 1.2 RFC 5246
  - 2011, 禁用SSL 2.0, RFC 6167
  - 2015, 禁用SSL 3.0, RFC 7568
  - 2018, TLS 1.3 RFC 8446
- TLS协议的安全问题和攻击
  - 证书问题,如不可信CA证书
  - 协议设计问题，如CRIME
  - 实现问题，如HeartBleed
  - 密码问题，如RC4/MD5/SHA1



推进HTTPS部署的各种努力

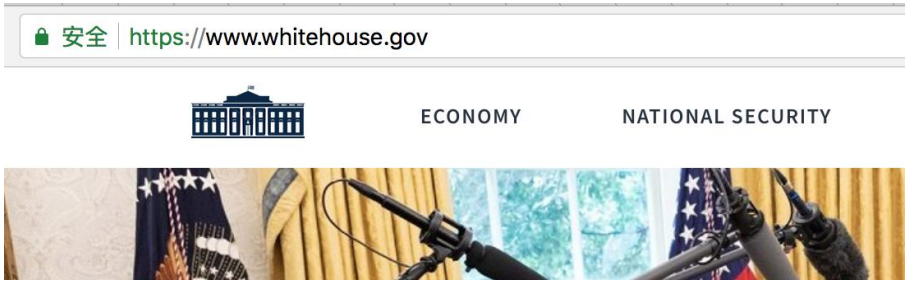
- HTTPS Everywhere, 2010

- Let's Encrypt, 2016
  - 免费的、自动的、开放的CA

- 浏览器的告警
  - HTTP网站显示不安全
  - 输入口令和信用卡号码时警告用户

- Google搜索排名
  - 排名考虑HTTPS，鼓励部署

- 美国联邦政府支持HTTPS政策

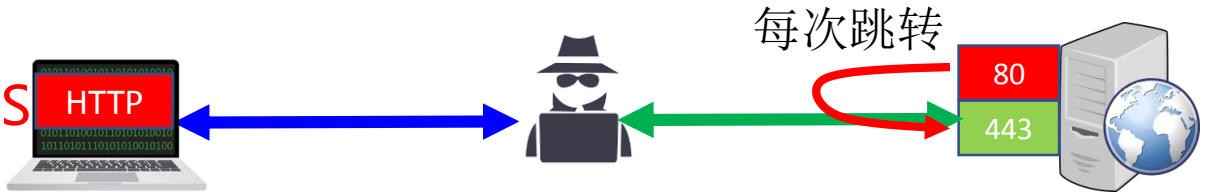


服务器端常见的HTTPS 部署情况

1. 只支持HTTP

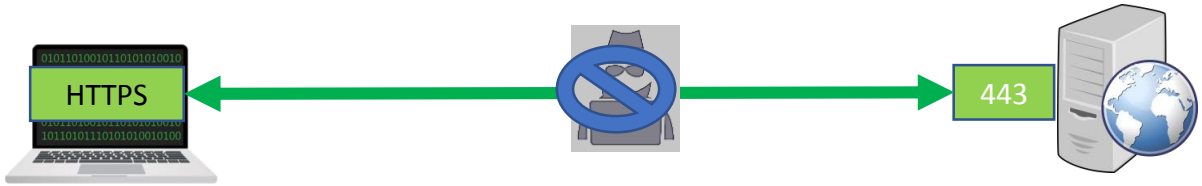
2. HTTP和HTTPS并存

3. HTTP默认跳转到HTTPS



4. 持久跳转HTTPS(HSTS)

5. **HTTPS only +HSTS**

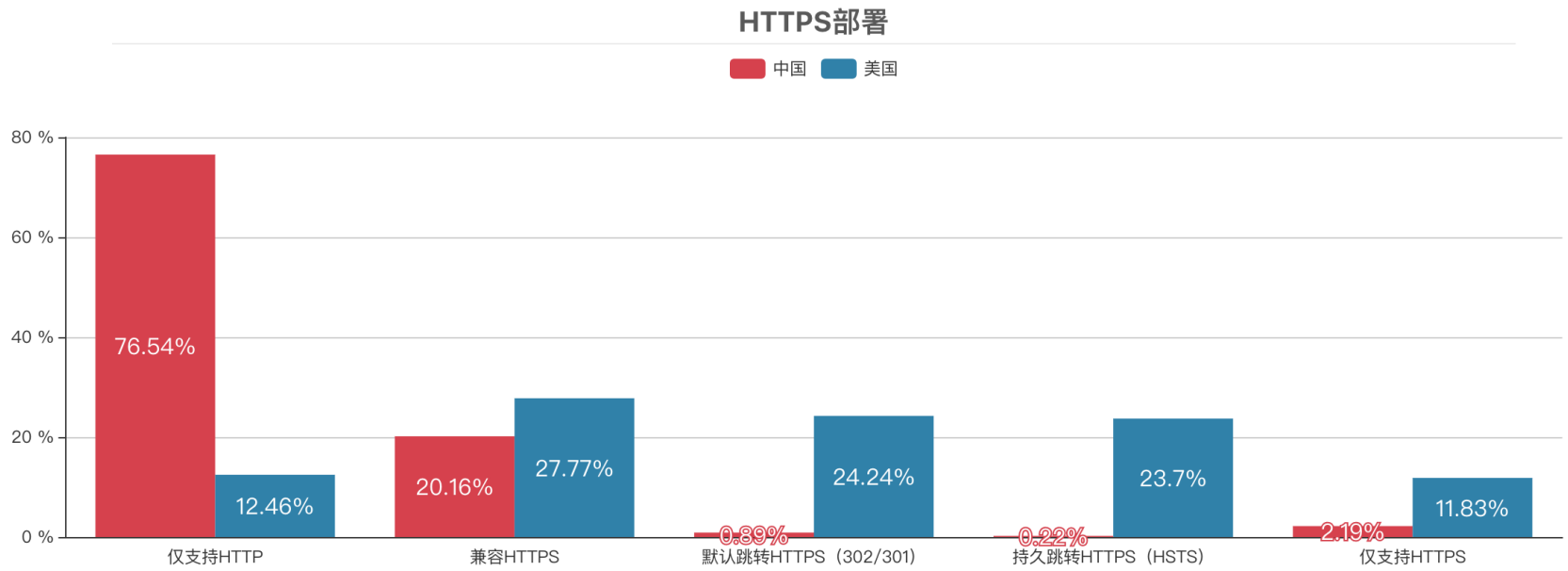


HSTS Preload+ HPKP

中国和美国政府网站HTTPS部署的对比

政府 | 教育

区域	SLD数量	子域名数量	开放Web域名
中国	57033	280972	97390
美国	6158	313242	108558



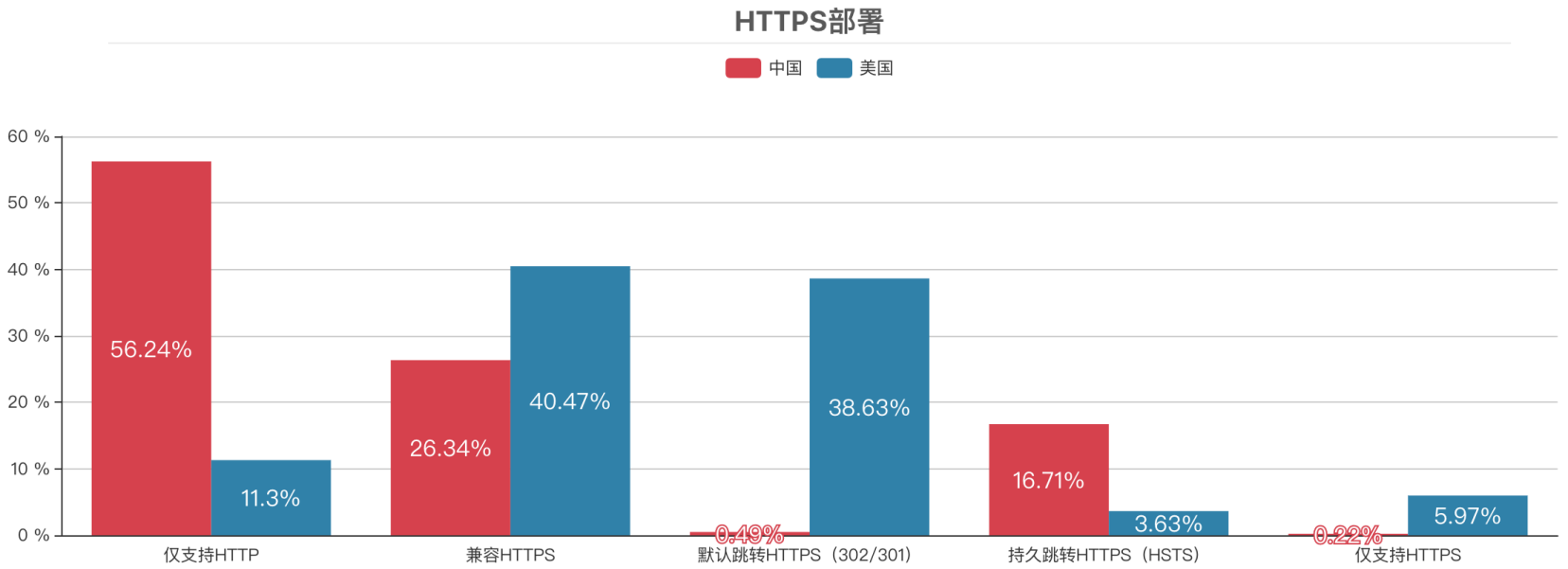
数据来源：
360 Passive DNS，
2014年至2018年
https://netlab.360.com

- 美国支持HTTPS的网站超过87%，中国仅23%
- 美国缺省使用HTTPS的71%，中国不到4%

中国和美国高校网站HTTPS部署的对比

政府 教育

区域	SLD数量	子域名数量	开放Web域名
中国	3785	15327444	2521421
美国	12866	2827599	970997



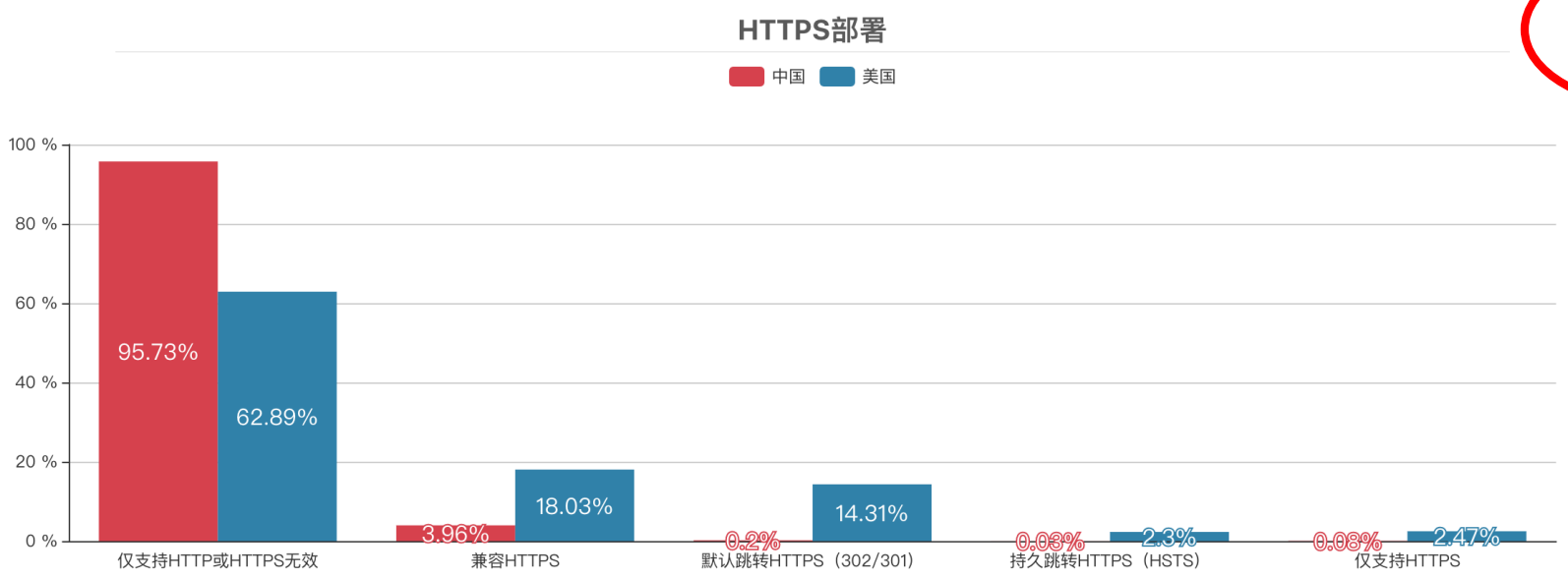
数据来源：
360 Passive DNS，
2014年至2018年
https://netlab.360.com

- 中国高校严格使用HTTPS的近17%
- 比美国高校9%高很多（？）

中国和美国高校网站HTTPS部署的对比

政府 教育

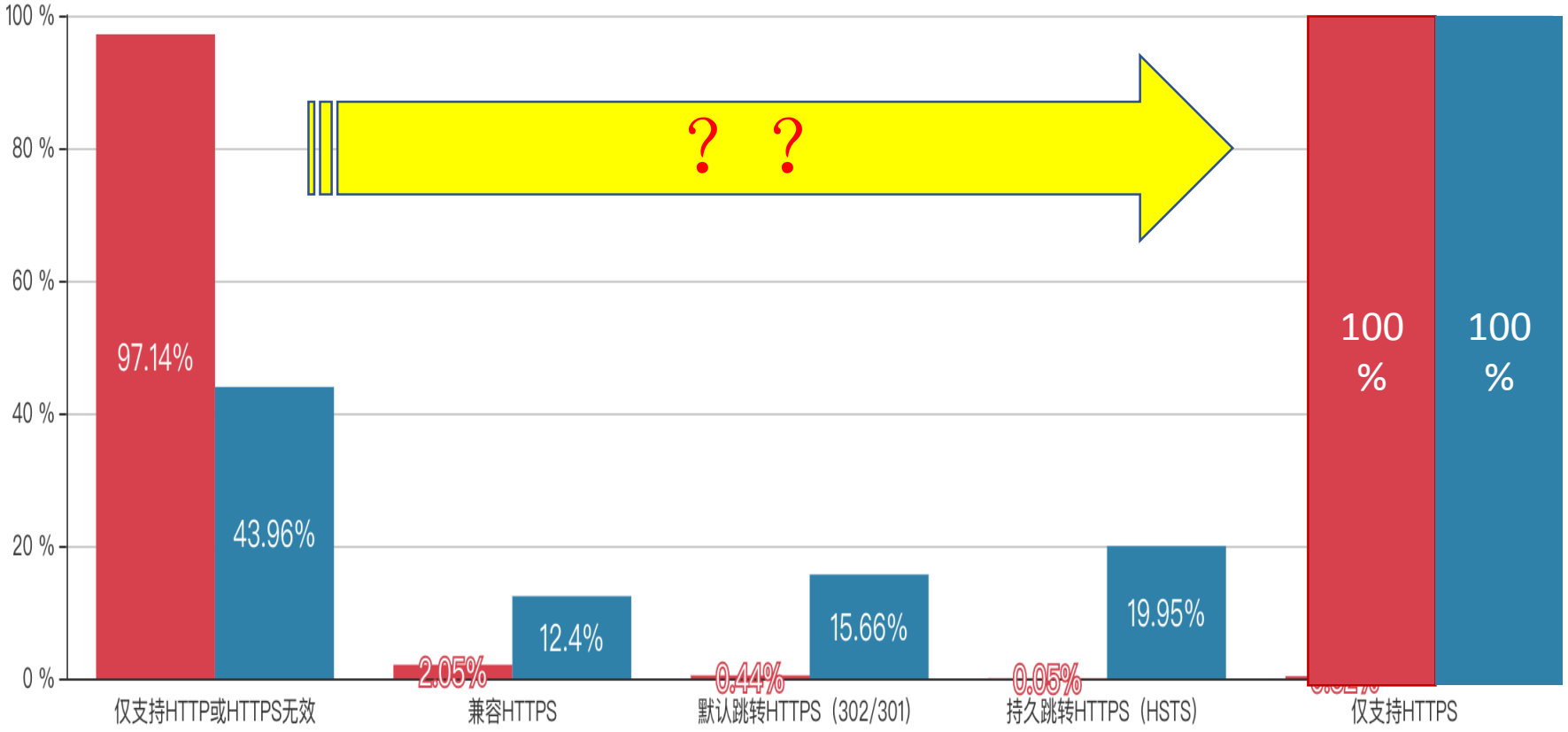
区域	SLD数量	子域名数量	开放Web域名
中国	3785	15327444	2521421
美国	12866	2827599	970997



- 中国高校大量使用了同一个公司的防火墙产品，使用了自签名证书（无效）
- 把无效证书算作HTTP类别，中国高校仍然落后于美国高校

https://secrank.cn/#/https/measure

我们还要走多久？


100 %
80 %
60 %
40 %
20 %
0 %
97.14%
43.96%
2.05%
12.4%
0.44%
15.66%
0.05%
19.95%
100 %
100 %
? ?
仅支持HTTP或HTTPS无效
兼容HTTPS
默认跳转HTTPS（302/301）
持久跳转HTTPS（HSTS）
仅支持HTTPS

我们还要走多久？

对部署一个新的协议，不能盲目乐观

对工程上的妥协（trade-off）需要有足够的理解

一些研究体会

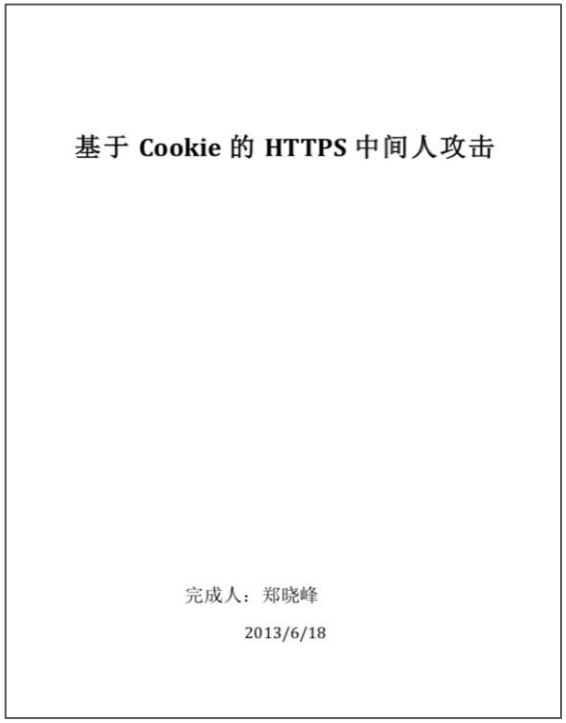
研究体会：为什么做研究？

兴趣 成瘾

研究体会：关于BIG4

- BIG4 ≠ 读博

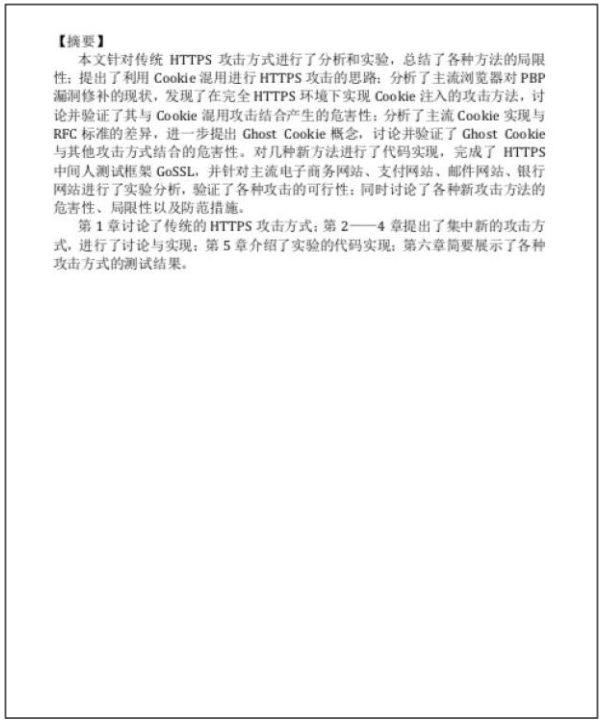
来自课程作业的BIG4



基于 Cookie 的 HTTPS 中间人攻击

完成人：郑晓峰

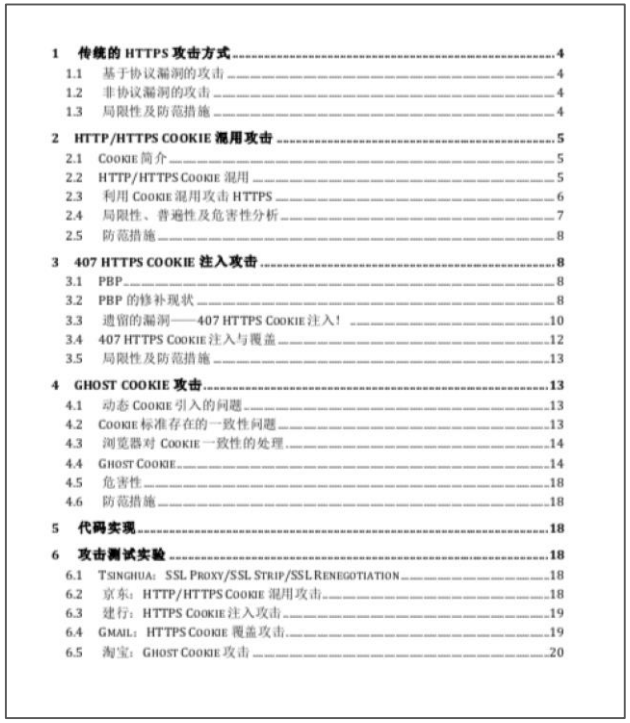
2013/6/18



【摘要】

本文针对传统 HTTPS 攻击方式进行了分析和实验，总结了各种方法的局限性；提出了利用 Cookie 混用进行 HTTPS 攻击的思路；分析了主流浏览器对 PBP 漏洞修补的现状，发现了在完全 HTTPS 环境下实现 Cookie 注入的攻击方法，讨论并验证了其与 Cookie 混用攻击结合产生的危害性；分析了主流 Cookie 实现与 RFC 标准的差异，进一步提出 Ghost Cookie 概念，讨论并验证了 Ghost Cookie 与其他攻击方式结合的危害性。对几种新方法进行了代码实现，完成了 HTTPS 中间人测试框架 GoSSL，并针对主流电子商务网站、支付网站、邮件网站、银行网站进行了实验分析，验证了各种攻击的可行性；同时讨论了各种新攻击方法的危害性、局限性以及防范措施。

第 1 章讨论了传统的 HTTPS 攻击方式；第 2——4 章提出了集中新的攻击方式，进行了讨论与实现；第 5 章介绍了实验的代码实现；第六章简要展示了各种攻击方式的测试结果。



1 传统的 HTTPS 攻击方式 4
1.1 基于协议漏洞的攻击 4
1.2 非协议漏洞的攻击 4
1.3 局限性及防范措施 4
2 HTTP/HTTPS COOKIE 混用攻击 5
2.1 COOKIE 简介 5
2.2 HTTP/HTTPS COOKIE 混用 5
2.3 利用 COOKIE 混用攻击 HTTPS 6
2.4 局限性、普遍性及危害性分析 7
2.5 防范措施 8
3 407 HTTPS COOKIE 注入攻击 8
3.1 PBP 8
3.2 PBP 的修补现状 8
3.3 遗留的漏洞——407 HTTPS COOKIE 注入！ 10
3.4 407 HTTPS COOKIE 注入与覆盖 12
3.5 局限性及防范措施 13
4 GHOST COOKIE 攻击 13
4.1 动态 COOKIE 引入的问题 13
4.2 COOKIE 标准存在的一致性问题 13
4.3 浏览器对 COOKIE 一致性的处理 14
4.4 GHOST COOKIE 14
4.5 危害性 18
4.6 防范措施 18
5 代码实现 18
6 攻击测试实验 18
6.1 TSINGHUA：SSL PROXY/SSL STRIP/SSL RENEGOTIATION 18
6.2 京东：HTTP/HTTPS COOKIE 混用攻击 18
6.3 建行：HTTPS COOKIE 注入攻击 19
6.4 GMAIL：HTTPS COOKIE 覆盖攻击 19
6.5 淘宝：GHOST COOKIE 攻击 20

研究体会：读博痛苦吗？

- 比读博更痛苦的—— 想读却不能读
- 追求幸(tong)福(ku)的“任意门”

你会怀念所有的那些曲折

我爱这艰难又拼尽了全力的每一天
我会怀念所有的这些曲折

我爱这被风带走不会再有的每一天
那只有我自己知道的快乐

当我听到风从我耳旁呼啸着掠过
那一刻我的心狂喜着猛烈地跳动

——朴树《空帆船》

360企业安全技术研究院
清华大学-360企业安全联合研究中心

等你来