基于解析数据的 DNS 安全评估与增强

毕设答辩

无 41 芦迪

指导老师：李星

Department of Electronic Engineering,
Tsinghua University

June 15, 2018

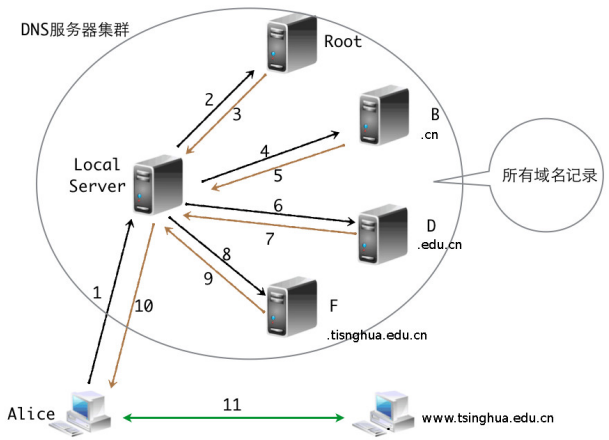
目录

目录

DNS

DNS: Domain Name System，域名系统

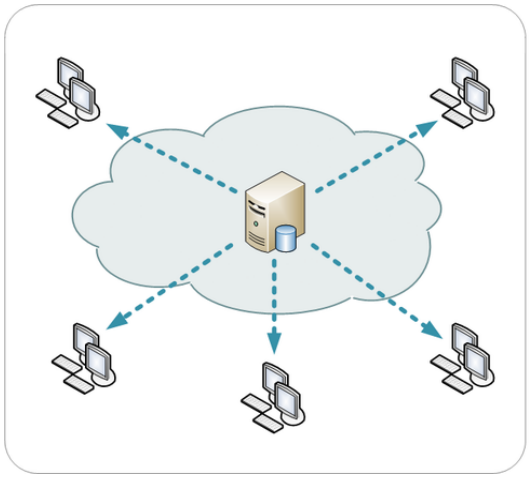
- 域名 (www.tsinghua.edu.cn) $\Longleftrightarrow$ IP 地址 (166.111.4.100)
- 重要的互联网基础设施，遭到攻击损失无法估量

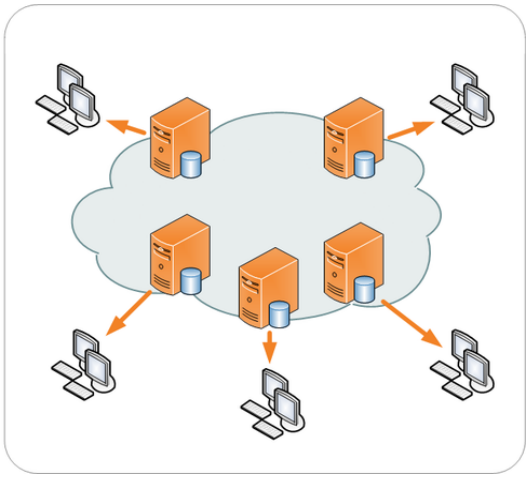


- DNS 易受攻击
  - 协议脆弱性：UDP、明文；系统脆弱性：Open Resolvers、路径复杂
  - DNS 劫持：将 DNS 请求定向到非法解析器
  - DNS 缓存中毒：将虚假域名数据注入到缓存中

CDN 与负载均衡

- 因为 CDN 与负载均衡的普遍存在，域名解析情况更加复杂
  - CDN：Content Delivery Network
    - 部署边缘服务器，使用户就近获取所需内容，降低网络拥塞





  - 负载均衡：在多个服务器中分配负载，最优化资源使用，避免过载
- 一个域名会解析出多个 IP，一个 IP 也可以对应多个域名

网络安全增强

互联网天然缺乏安全性，通过完善协议可以增强安全性

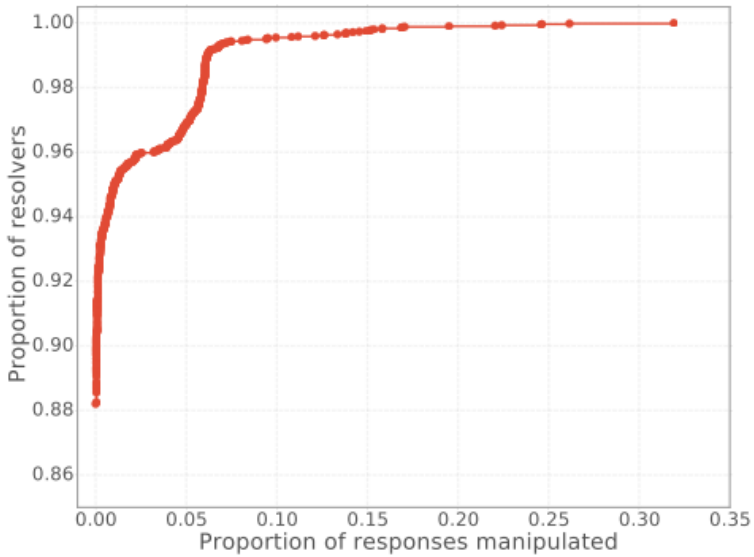
- DNSSEC：DNS 安全扩展
  - 使用公钥密码机制，以 DNS 资源记录计算数字签名，验证数字签名确保解析结果真实
  - 提供数据来源、数据完整性和否定存在验证
- IPv6：下一代互联网协议
  - IPv6 内嵌 IPSec 协议族的 AH 和 ESP，从协议上提升安全性
  - IPv6 地址空间大，增大扫描难度，可减缓现有攻击
- DNS over HTTPS
  - 使用 HTTPS 传输解析信息，增强了客户端和递归解析器之间的隐私和安全性

毕设内容

- 分析域名解析数据，了解域名或解析器对 IPv6、DNSSEC、HTTPS 的支持情况，评估安全现状
  - 根据 A 记录与 AAAA 记录，判断 IPv6 支持情况
  - 根据 RRSIG 记录，判断 DNSSEC 支持情况
  - 测试 (域名, IP 地址)，判断 HTTPS 支持情况
- 对 DNS 解析返回的 IP 地址进行判别与分类
  - 结果正常：CDN？负载均衡？
  - 结果有误：DNS 劫持？缓存中毒？

前人工作

- 文献 [1]*采用一致性和独立的可验证性指标，通过对解析结果 IP 地址、自治域、HTTP 内容、HTTPS 证书等内容进行验证，实现了对 DNS 操作的检测



- 文献 [2]** 通过对 DNS 解析结果进行过滤，并对 HTTP 请求返回的内容进行聚类，系统地分析了非合法的 DNS 响应

*Global Measurement of DNS Manipulation

**Going Wild: Large-Scale Classification of Open DNS Resolvers

目录

数据获取

Resolver	Owner	DNSSEC
8.8.8.8	Google	Y
4.2.2.2	MicroSoft	Y
9.9.9.9	IBM	Y
8.26.56.26	Comodo	Y
180.76.76.76	Baidu	Y
202.141.162.123	USTC	Y
223.6.6.6	Ali	N
114.114.114.114	114DNS	N
.....	.....	.....

Table: Open Resolvers

Num.	Domain Name
1	google.com
2	youtube.com
3	facebook.com
4	baidu.com
5	wikipedia.org
6	yahoo.com
7	reddit.com
8	google.co.in
.....	.....

Table: Top Domain Names

解析数据获取说明：

- 开放解析器与域名
- 工具：MySQL, dnspython
- 方式：UDP/TCP, IPv4/IPv6
- 腾讯云 CVM，公网 IP：211.159.174.23
- 解析数据的快速获取；频繁请求解析器可能拒绝服务

数据获取

数据库中的 IPv4 记录与 IPv6 记录：

aRecordID	domainName	resolverAddr	ttl	addr
315521	weevah2.top	8.8.4.4	3326	198.134.112.242
433017	pbskids.org	156.154.71.1	60	205.251.203.136
525319	varlamov.ru	4.2.2.1	60	81.19.74.4
188624	coindesk.com	208.67.222.123	300	104.17.108.195
28067	xfinity.com	202.38.93.153	3599	68.87.41.40
502148	railwayrecruitmentgov.in	180.76.76.76	320	35.202.133.111
462800	heroku.com	101.236.28.23	60	50.19.85.156
47013	xda-developers.com	101.226.4.6	3600	209.58.128.90
135384	kinogo.by	114.114.115.119	300	104.25.188.28
332738	imasdk.googleapis.com	114.114.115.119	0	203.208.50.35

aaaaRecordID	domainName	resolverAddr	ttl	addr
40338	folha.uol.com.br	114.114.115.119	60	2804:49c:319:430::339
62027	harvestapp.com	156.154.71.1	298	2001:1838:2001:e::189
18638	etherscan.io	208.67.220.220	5	2400:cb00:2048:1::6819:f40e
97180	animesorion.tv	8.8.8.8	299	2400:cb00:2048:1::681c:c28
87071	pcgames-download.com	180.76.76.76	320	2400:cb00:2048:1::681f:526f
75684	hibapress.com	202.38.93.153	300	2400:cb00:2048:1::681c:1c4b
52526	usgs.gov	208.67.222.222	300	2001:49c8:4000:140c::43
31744	hotmovs.com	182.254.116.116	300	2400:cb00:2048:1::6819:4008
6458	adexchangemachine.com	180.76.76.76	310	2400:cb00:2048:1::6810:edb6
45079	shink.me	140.207.198.6	299	2400:cb00:2048:1::681c:1850

数据获取

顶级域名分布情况及域名对 IPv6、DNSSEC 的支持情况：

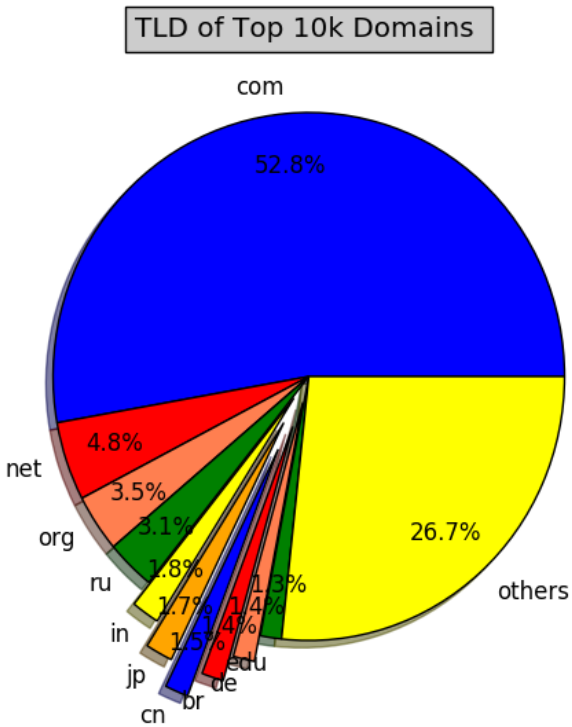


Figure: 顶级域名分布

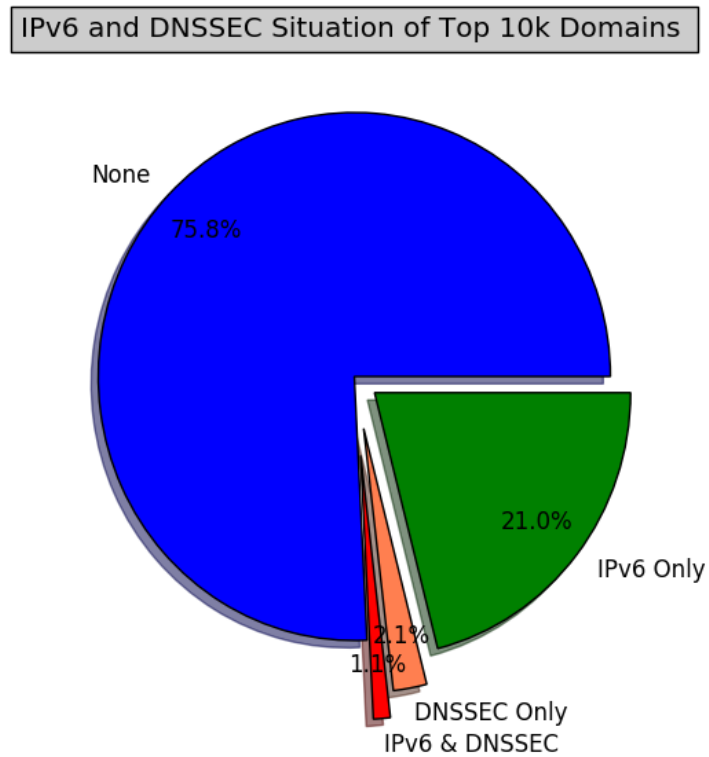


Figure: IPv6/DNSSEC Crosscheck

数据获取

顶级域名.com 和.net 对 IPv6、DNSSEC 的支持情况：

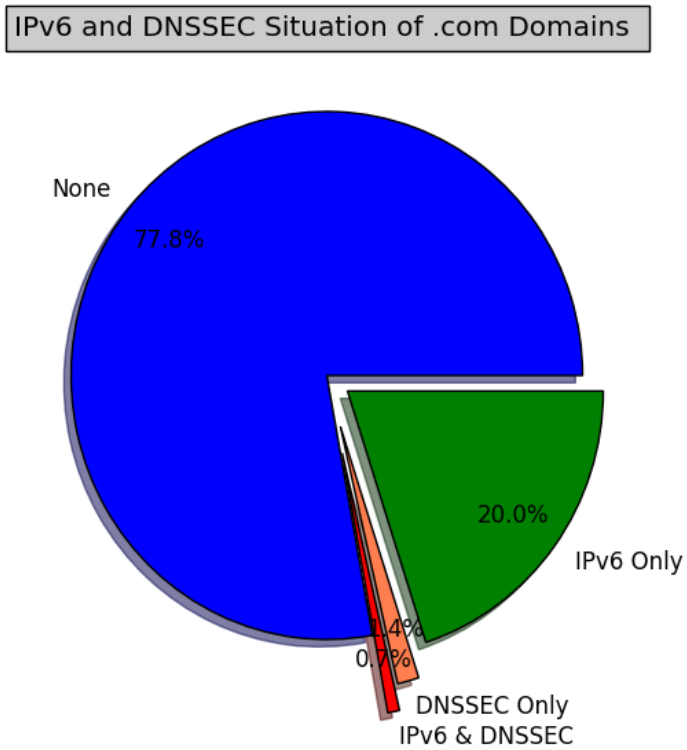


Figure: IPv6/DNSSEC Crosscheck in .com Domain

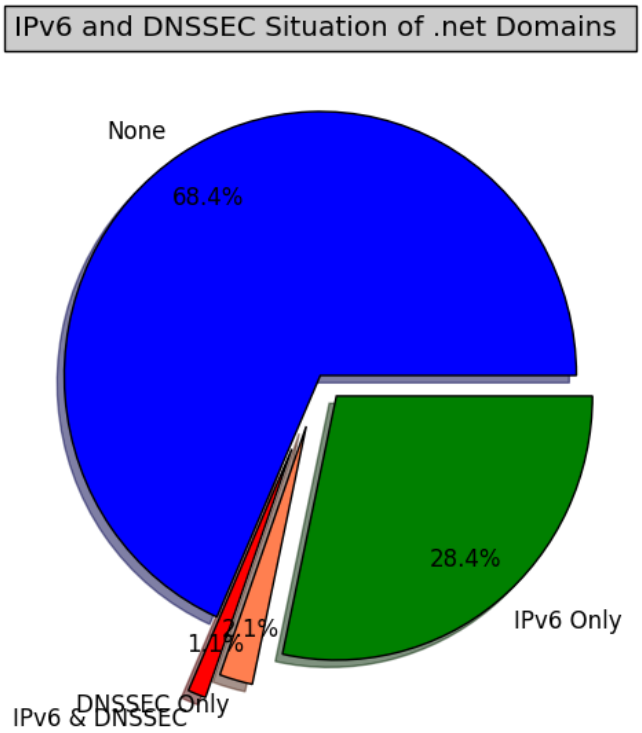


Figure: IPv6/DNSSEC Crosscheck in .net Domain

目录

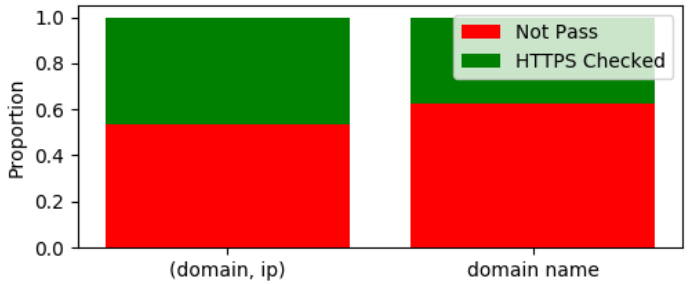
结果标记

- HTTPS
  - 使用数字证书来验证站点的身份，加密用户和站点之间的数据交换
  - 对于解析到的 IP 地址，对其 443 端口发起连接请求，验证是否支持 HTTPS
  - 对于支持 HTTPS 的 IP 地址，对其证书进行验证，将验证通过的 (domain, ip, resolver) 对标记为正确
- DNSSEC
  - 使用数字签名来验证 DNS 数据的完整性，从而确保用户可以到达预期的 IP 地址
  - 大多数解析器支持 DNSSEC，但部署了 DNSSEC 的域名仍较少
  - 通过公钥与签名验证解析记录真实性与完整性，从信任锚开始对信任链进行验证

HTTPS 结果

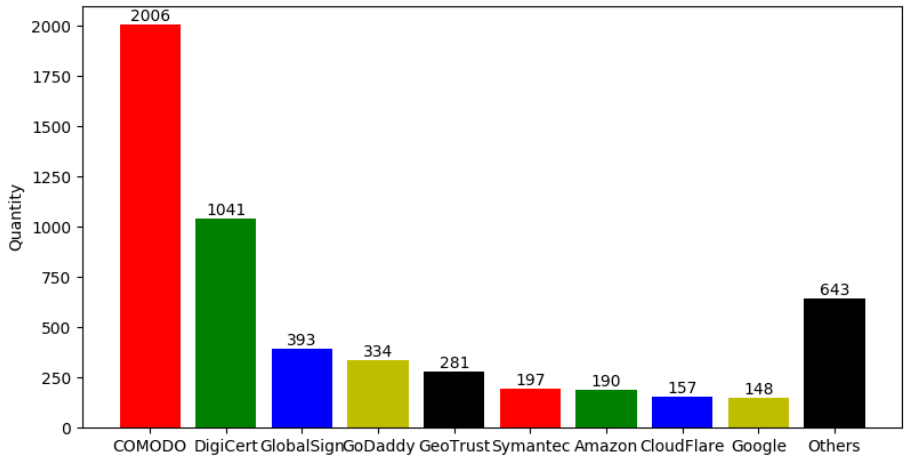
HTTPS 测试整体情况：

	Total	Succeeded	Failed	Refused
(domain, ip)	47877	25740	1245	1028
domain name	8585	5376	755	753



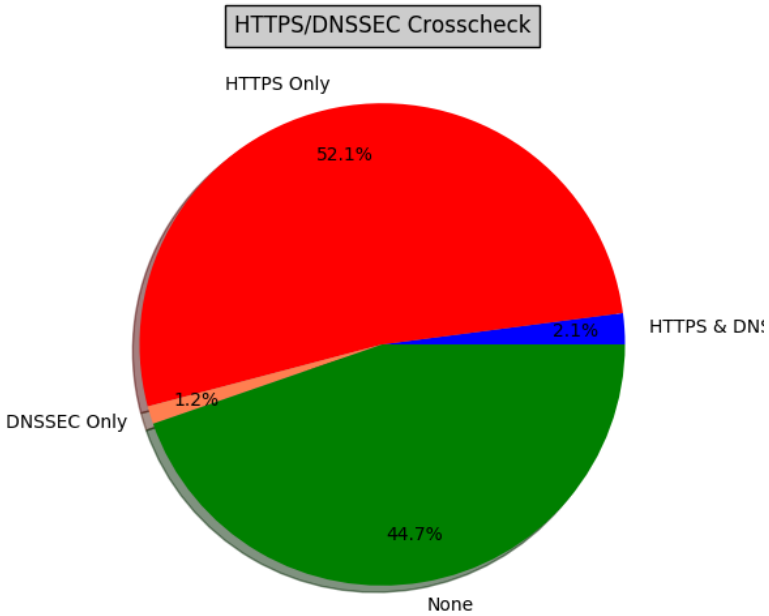
HTTPS 证书服务商统计：

Service Provider	Quantity	Percent
COMODO CA Limited	2006	37.22%
DigiCert Inc	1041	19.31%
GlobalSign	393	7.29%
GoDaddy.com, Inc.	334	6.19%
GeoTrust Inc.	281	5.21%
Symantec Corporation	197	3.65%
Amazon	190	3.53%
CloudFlare, Inc.	157	2.91%
Google Trust Services	148	2.75%
Others	643	11.93%



目录

HTTPS/DNSSEC 分析

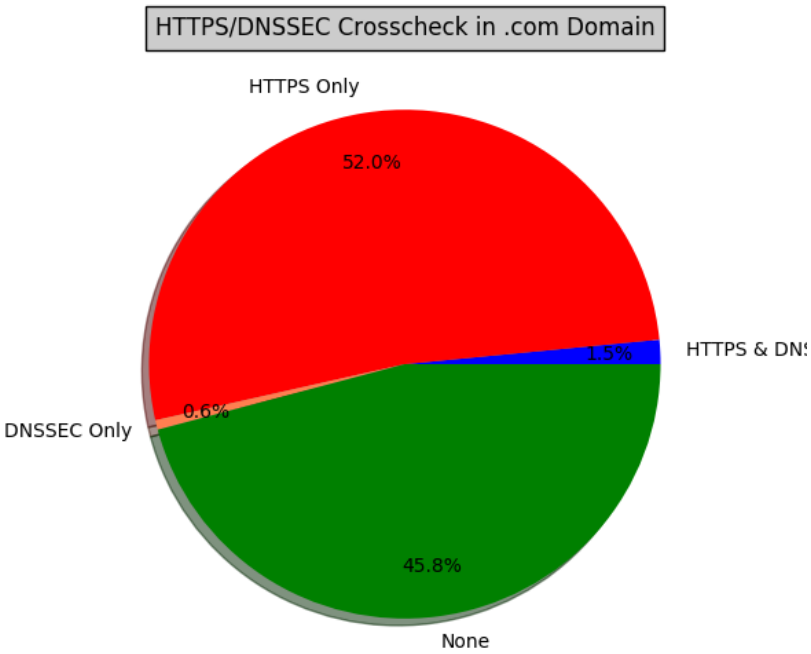


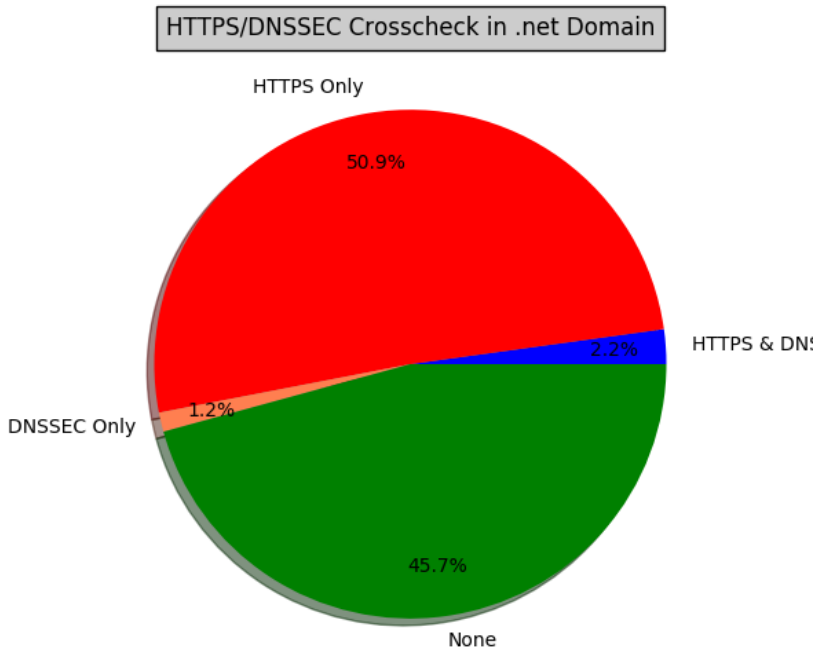
对于 DNSEC Only 的情况，发现以以下三类网站居多：

- 成人网站
- 教育机构
- 政府机构

HTTPS/DNSSEC 分析

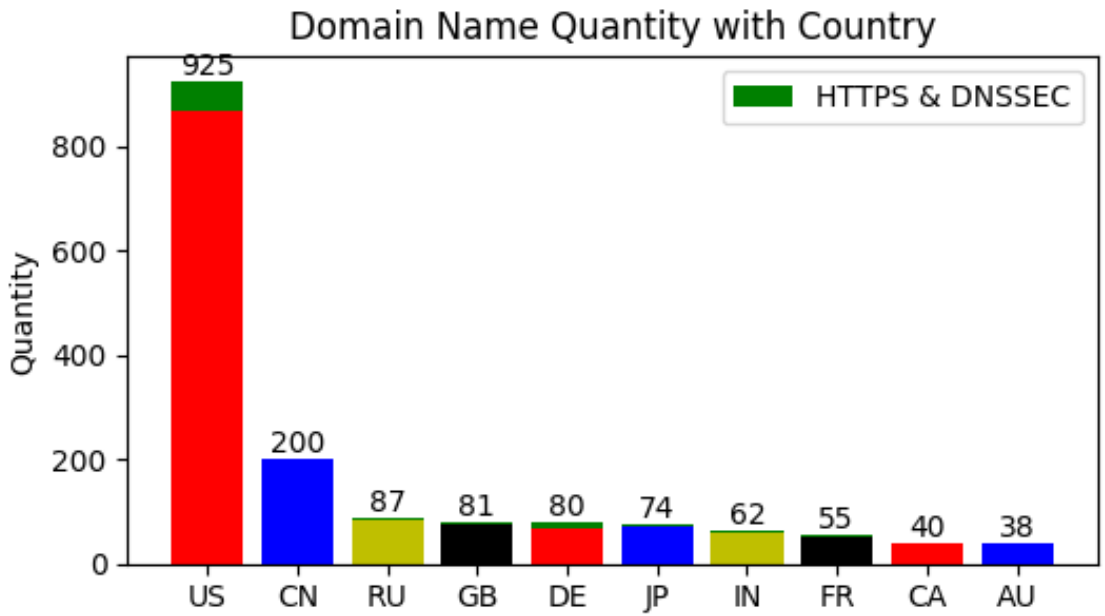
对顶级域名.com 和.net 对 DNSSEC 和 HTTPS 支持情况进行分析：





数据分析

对证书中获取的国家名称进行分析：



目录

未来工作计划

- 进一步对 IP 地址进行分类
  - IP 地址聚类，基于 AS 进行分析
  - 对 CDN 进行检测
  - 分析 HTTP Content
  - tcp 结果与 udp 结果对比分析
- 多点解析，分析 GFW 对 DNS 影响情况
- 对 IPv6 的结果做进一步分析

参考文献

Paul Pearce, U C Berkeley, Ben Jones, Frank Li, U C Berkeley, Roya Ensafi, Nick Feamster, Nick Weaver, Vern Paxson, U C Berkeley, Paul Pearce, Ben Jones, Frank Li, Nick Feamster, and Vern Paxson.
Global Measurement of DNS Manipulation.
2017.

Marc Kührer, Thomas Hupperich, Jonas Bushart, Christian Rossow, and Thorsten Holz.
Going Wild : Large-Scale Classification of Open DNS Resolvers Categories and Subject Descriptors.
pages 355–368.


Thank you!