基于域名解析数据的 DNS 劫持分析

芦迪

指导老师：李星

Department of Electronic Engineering,
Tsinghua University

January 12, 2018

目录

目录

DNS 介绍

DNS：Domain Name System

- 一个分层的分布式命名系统，将域名转换为 IP 地址
- 指定每个域的权威域名服务器分配域名，层层分配

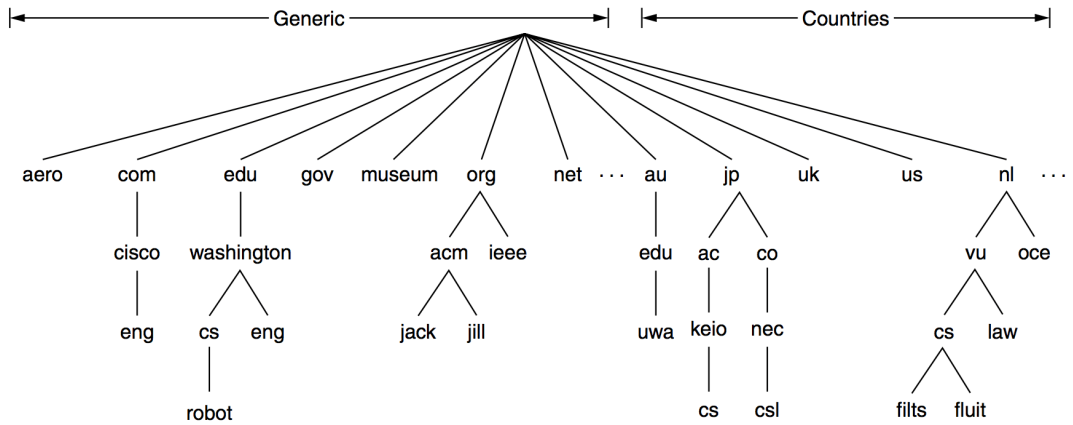
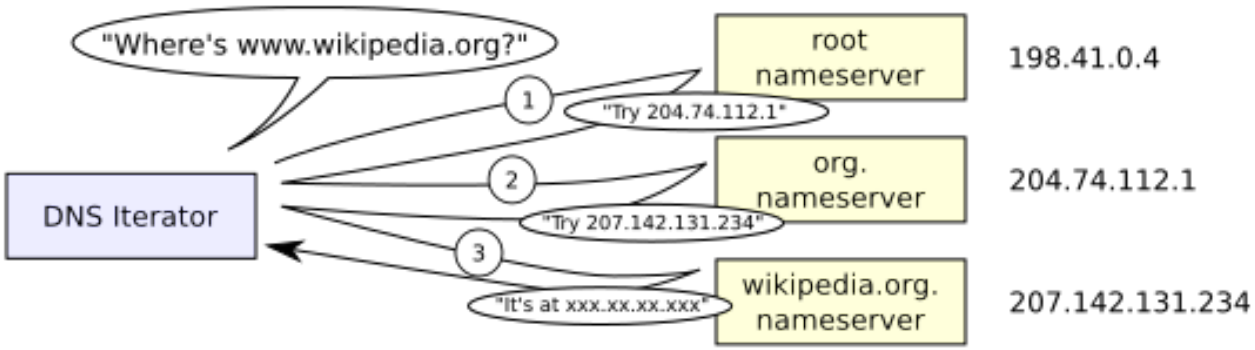


Figure: Domain Tree

DNSSEC：公钥密码机制，添加数字签名，协议增强

DNS 介绍

域名解析过程：



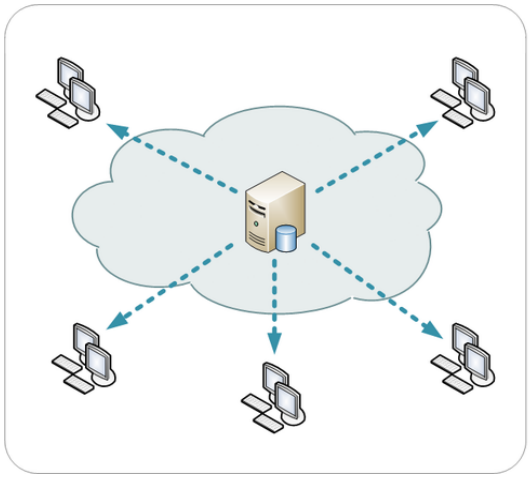
常见记录类型：

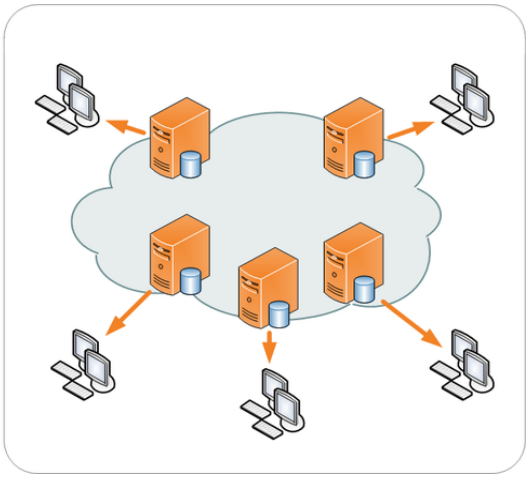
记录类型	含义
A	主机的 IPv4 地址
AAAA	主机的 IPv6 地址
NS	该域名所在域的权威域名服务器
CNAME	将当前域名映射到另一个域名
MX	将域名映射到该域的邮件传输代理列表
PTR	反向 DNS 查找指针

CDN 与负载均衡

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
- 依靠 CNAME 记录，实现网络请求重定向





负载均衡

- DNS 轮循是负载均衡的一种方法

目录

DNS 请求格式

```
+---------------------+
|        Header       |
+---------------------+
|       Question      | the question for the name server
+---------------------+
|        Answer       | Resource Records (RRs) answering the
+---------------------+
|      Authority      | RRs pointing toward an authority
+---------------------+
|      Additional     | RRs holding additional information
+---------------------+
```

Figure: DNS Message

```
0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   Opcode  |AA|TC|RD|RA|   Z    |   RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    QDCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ANCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    NSCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Figure: DNS Header

资源记录分析

我们希望通过分析解析数据，了解目前 IPv6 与 DNSSEC 普及情况：

1. 根据 A 记录与 AAAA 记录，判断 IPv6 支持情况

```
;; ANSWER SECTION:
xinhuanet.com.          3600    IN      A       202.108.119.194
xinhuanet.com.          3600    IN      A       202.108.119.193

;; AUTHORITY SECTION:
xinhuanet.com.          280     IN      NS      ns2.cdns.cn.
xinhuanet.com.          280     IN      NS      ns3.cdns.cn.
xinhuanet.com.          280     IN      NS      ns1.cdns.cn.

;; ADDITIONAL SECTION:
ns1.cdns.cn.            86      IN      A       125.208.45.1
ns2.cdns.cn.            393     IN      A       125.208.46.1
ns3.cdns.cn.            1382    IN      A       125.208.47.1
ns1.cdns.cn.            86      IN      AAAA    2001:dc7:ffeb::1
ns2.cdns.cn.            393     IN      AAAA    2001:dc7:ffec::1
```

2. 根据 RRSIG 记录，判断 DNSSEC 支持情况

```
;; ANSWER SECTION:
paypal.com.             124 IN A 64.4.250.33
paypal.com.             124 IN A 64.4.250.32
paypal.com.             124 IN RRSIG A 5 2 300 (
                               20180205064703 20180106054703 11811 paypal.com.
                               rXHdlxddoLYYUjTuDxRLmtMxkTNdHVKaYBGif8KC03Jp
                               AWjl564STz3OQcJSpyurpJJYXCHVwkUt/X6RUfkw3neQ
                               gH0CjspEEiVxaOwEqZNEcWZBUDm77Vy4t1BpYiogNWGR
                               rKqezt9lon48zCZj9Zi0gdAE4qYNjvi1Glp9HCA= )
```

DNS 解析返回类型分析

- 通过 DNS 解析，由域名得到 IP 地址，存在以下类别：
  1. 返回唯一 IP
  2. CDN
  3. 负载均衡
  4. DNS 劫持
  5. 缓存中毒或其他有害情况
- 我们的目的是实现一个系统，对 DNS 解析的结果进行分类

目录

数据获取

收集 Open Resolvers 数据及 Domain Names 数据，进行 DNS 解析测试

Open Resolvers	Top Domain Names
114.114.114.114	baidu.com
8.8.8.8	qq.com
4.2.2.2	taobao.com
9.9.9.9	sina.com.cn
8.26.56.26	youku.com
199.91.73.222	soso.com
156.154.71.1	sohu.com
199.85.126.10	163.com
.....	.....

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> baidu.com @114.114.114.114
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47194
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;baidu.com.         IN  A

;; ANSWER SECTION:
baidu.com.      33  IN  A   111.13.101.208
baidu.com.      33  IN  A   220.181.57.217
baidu.com.      33  IN  A   123.125.114.144

;; Query time: 9 msec
;; SERVER: 114.114.114.114#53(114.114.114.114)
;; WHEN: Thu Jan 11 02:51:50 CST 2018
;; MSG SIZE  rcvd: 86


; <<>> DiG 9.10.3-P4-Ubuntu <<>> baidu.com @114.114.115.115
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39813
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;baidu.com.         IN  A

;; ANSWER SECTION:
baidu.com.      179 IN  A   220.181.57.217
baidu.com.      179 IN  A   123.125.114.144
baidu.com.      179 IN  A   111.13.101.208

;; Query time: 9 msec
;; SERVER: 114.114.115.115#53(114.114.115.115)
;; WHEN: Thu Jan 11 02:51:50 CST 2018
```

数据分析

- CDN 解析的结果通常包含有 CNAME 记录
- 关于 DNS 劫持的检测，文献 [1] 提出了一种基于贝叶斯原理的判别方法

目录

未来工作计划

- 继续文献调研，研究对负载均衡、缓存中毒等类别 DNS 解析结果的判别方法
- 进一步收集 Open Resolvers，获取数据进行分析

参考文献

Boru Yan, Binxing Fang, Bin Li, and Yao Wang.
Detection and defence of DNS spoofing attack.
Jisuanji GongchengComputer Engineering, 32(21):130 – 132+135, 2006.


Thank you!