基于域名解析数据分析的 DNS 安全现状评估与安全增强

无 41 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

- 将易于记忆的域名转换为枯燥难记的 IP 地址
- 重要的互联网基础设施，遭到攻击损失无法估量
- 因为协议脆弱性、系统脆弱性，存在极大安全隐患
  - 协议脆弱性：基于 UDP 交换消息，明文传递，不提供数字签名
  - 系统脆弱性：大量开放解析器，解析路径复杂，无法建立信任链

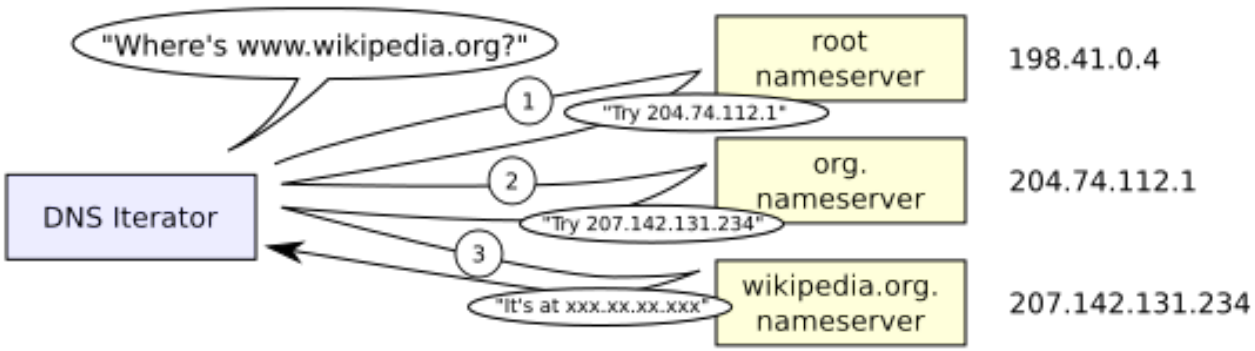
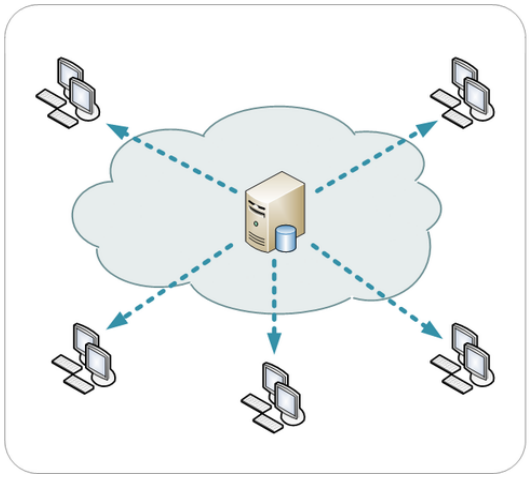
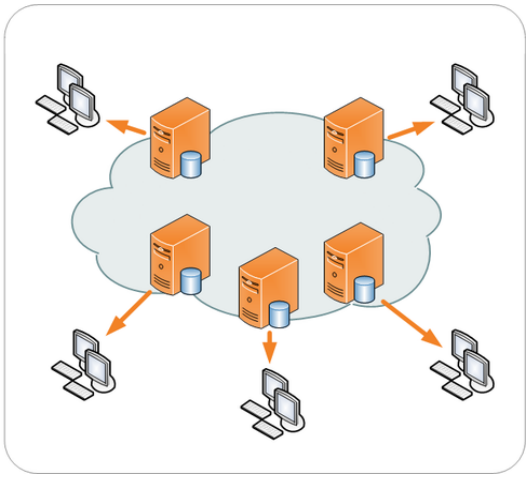


Figure: 域名解析过程

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 请求格式

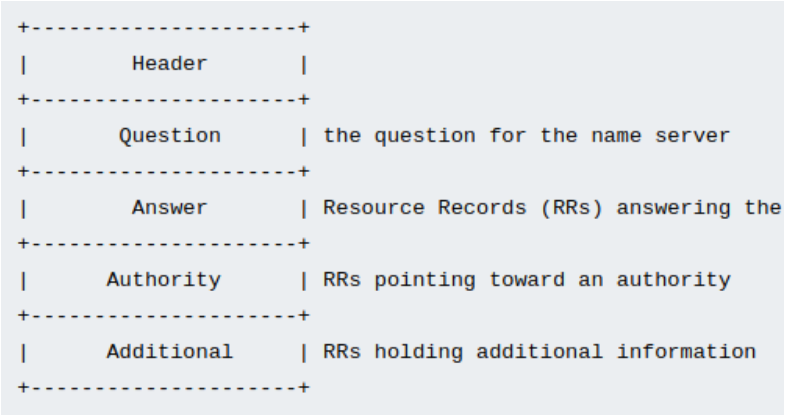


Figure: DNS Message

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	将域名映射到邮件传输列表
PTR	反向 DNS 查找指针

Table: 常见记录类型

目录

DNS 安全现状评估

- 分析域名解析数据，可以了解到域名或解析器对 IPv6 和 DNSSEC 的支持情况
  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 安全现状评估

- 分析域名解析数据，可以了解到域名或解析器对 IPv6 和 DNSSEC 的支持情况
- 搜集大量 Open Resolver 与域名数据，测试解析情况，可以进一步了解目前全网对 IPv6 和 DNSSEC 的支持情况，据此评估安全现状

DNS 安全增强

- 通过 DNS 解析，由域名得到 IP 地址，我们将其分为以下类别：
  1. 返回唯一 IP
  2. CDN 返回的结果
  3. 负载均衡返回的结果
  4. 解析遭到 DNS 劫持
  5. 缓存中毒或其他恶意结果
- 我们的目的是实现一个系统，对 DNS 解析的结果进行分类
- 实现了对 DNS 劫持与缓存中毒等恶意结果的诊断识别，就实现了对 DNS 安全增强

目录

数据获取

收集 Open Resolvers 数据及 Domain Names 数据，两个数据集叉乘，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
```

DNS 解析结果分类

- 所有 Resolver 返回结果相同，说明正常
- 一些 CDN 解析的结果包含有 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
- 文献 [2] 提出了一种名为 Kopis 的新型检测系统，用于通过被动监控 DNS 层次结构上层的 DNS 流量来检测与恶意软件相关的域名

目录

未来工作计划

- 继续文献调研，研究对 DNS 劫持、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.

Manos Antonakakis, Roberto Perdisci, Wenke Lee, Nikolaos Vasiloglou Ii, and David Dagon.
Detecting Malware Domains at the Upper DNS Hierarchy.
USENIX Security Symposium., 11:1–16, 2011.


Thank you!