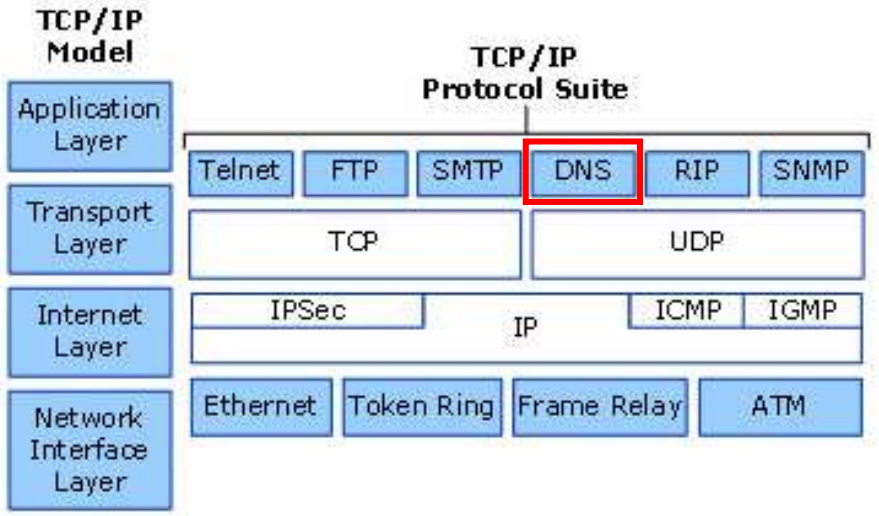
DNS安全

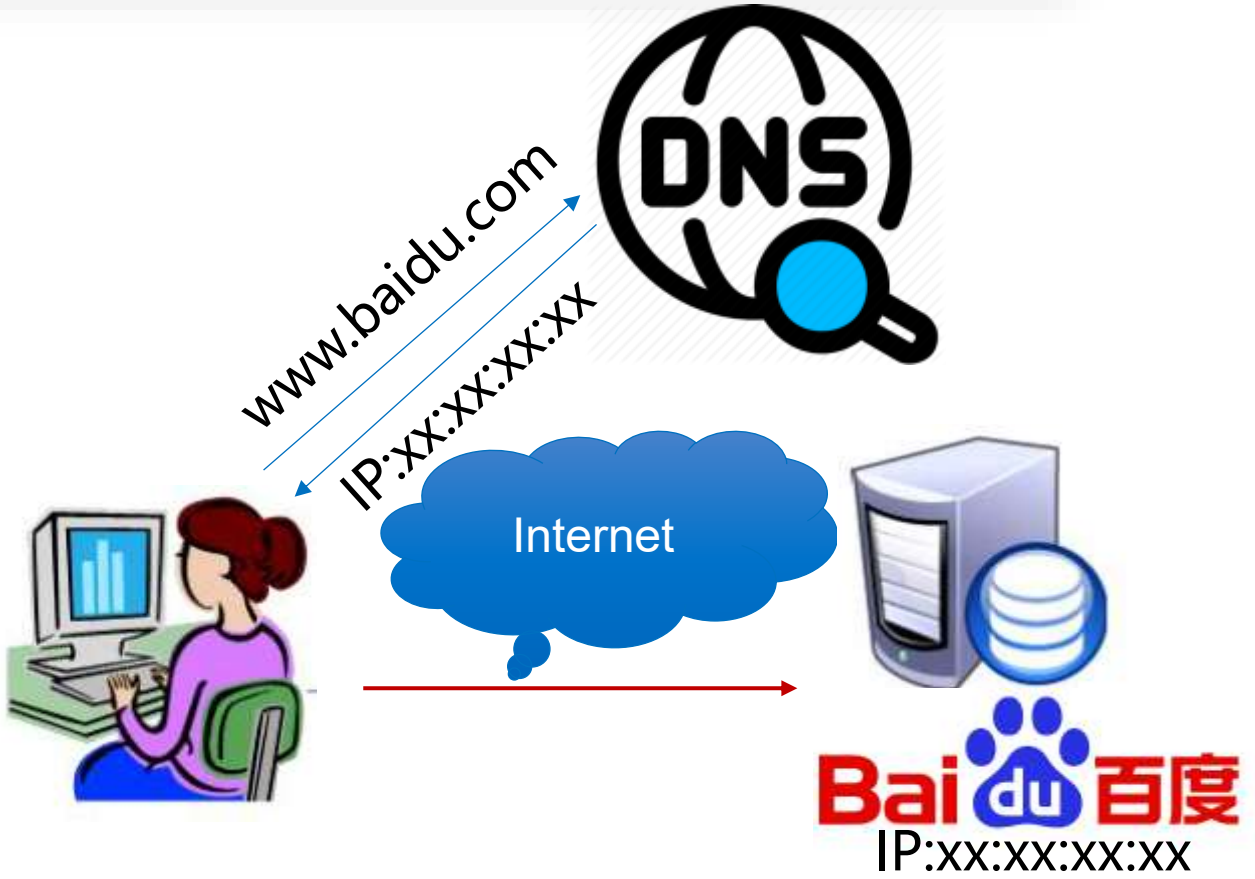
清华大学

域名系统--互联网关键基础设施

域名系统（DNS）位于协议栈应用层，为互联网提供核心服务，包括web页面访问，收发邮件等互联网应用通过DNS查询IP地址后获取资源，已成为互联网关键基础设施



DNS位于协议栈应用层



域名系统安全对抗不断升级

- 缓存污染、DDoS攻击等DNS安全威胁层出不穷，显示了全球DNS安全的脆弱性
- 与此同时，各类安全方案也致力于提升DNS安全性，互联网厂商如果有足够的针对自身信息系统的安全预案，就足以应对全面而复杂的威胁

- 美国国家安全局(NSA) 发布企业加密域名系统协议指南
- NSA指出，加密DNS请求的支持对于确保本地隐私和完整性保护至关重要

搜狐 | 新闻 体育 汽车 房产 旅游 教育 时尚 科技 财经

信息安全D1net

353 文章　12万 总阅读

查看TA的文章>

美国国家安全局发布企业加密DNS应用指南

2021-01-20 15:12

美国国家安全局(NSA)上周三发布了有关企业采用加密域名系统(DNS)协议(特别是基于HTTPS的DNS)指南。

DNS负责将URL中包含的域名转换为IP地址，但由于以明

成为一种流行的攻击媒介。

本章的内容组织

第一节
DNS概述

- DNS的演进
- DNS域名结构及区域组织形式

第二节
DNS使用及解析过程

- DNS使用
- DNS解析过程

熟悉DNS运行原理

思考DNS安全问题

DNS在设计之初缺乏安全考虑

第三节
DNS攻击

- 缓存中毒攻击
- 恶意DNS服务器回复伪造
- 拒绝服务攻击

掌握DNS攻击技术

了解DNS防御策略

多种攻击技术需要特定的防御策略进行防护

第四节
DNS攻击预防策略

- 基于密码技术
- 基于系统管理
- 新型架构设计

第一节 DNS概述

- DNS的演进
- DNS域名结构与区域组织形式

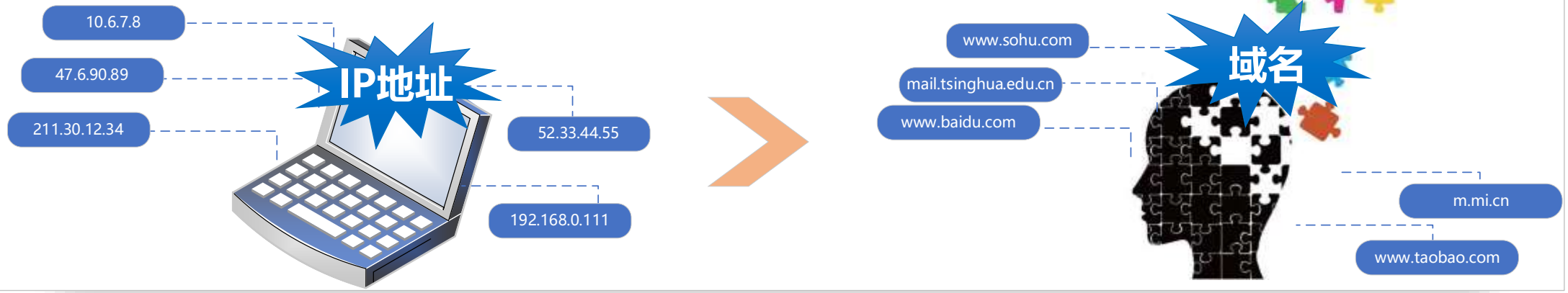
DNS的演进

网络空间两套命名体系：

用于路由寻址的IP地址和便于人类记忆的域名（Domain Name）

域名系统（DNS）功能：

实现域名与IP间转换

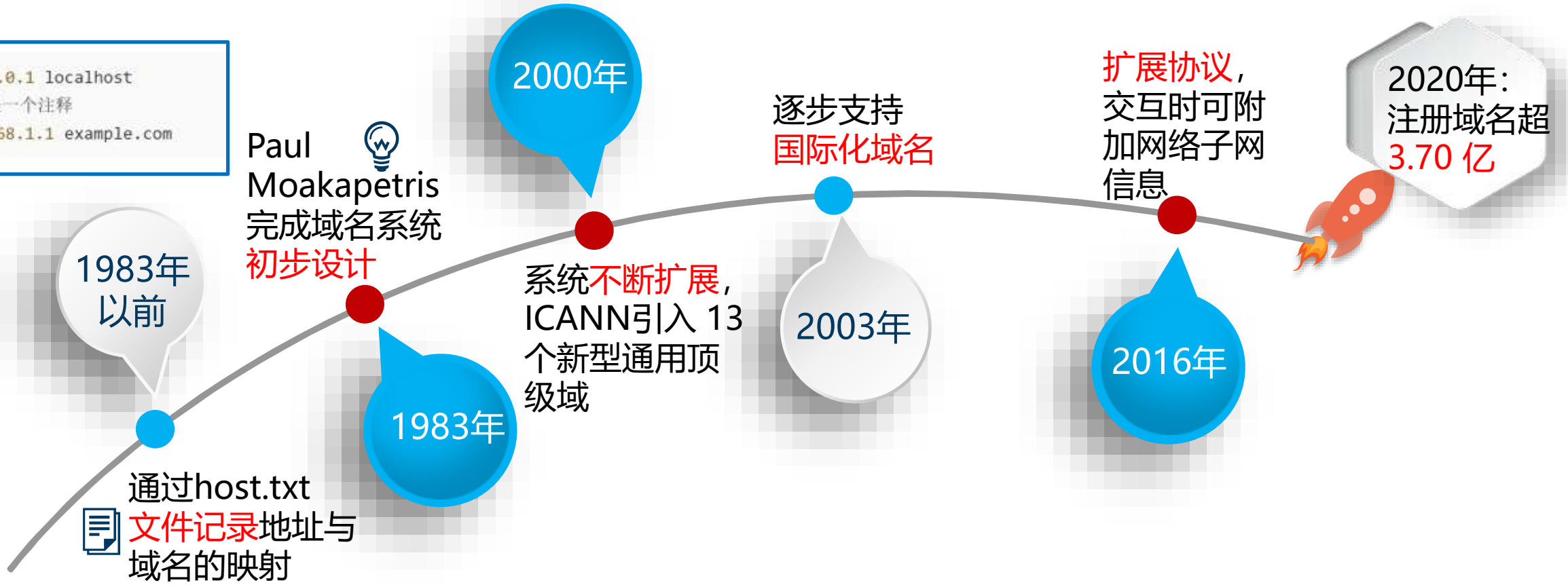


没有DNS，用户很难正常使用互联网

DNS的演进

从host.txt文件到大型分布式系统，DNS用于地址与域名的映射

```
127.0.0.1 localhost
# 这是一个注释
192.168.1.1 example.com
```



DNS区域组织形式

权威域名服务器

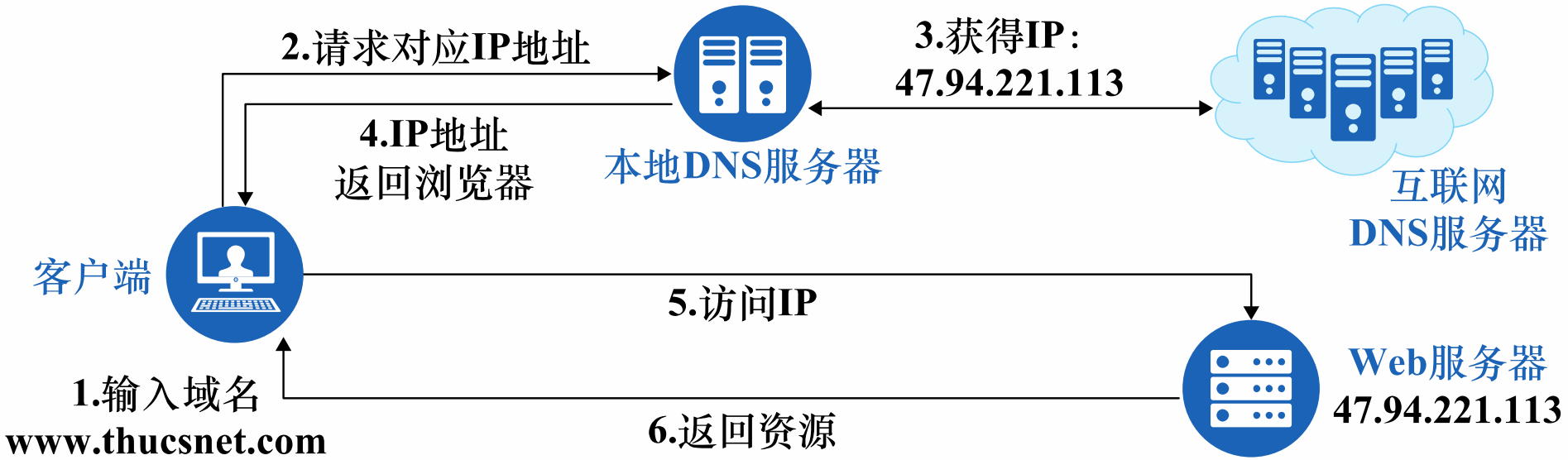
- 每个DNS区域的权威域名服务器，发布关于该区域的信息，并响应DNS查询请求
- 权威域名服务器可以配置主从服务器，主服务器存储所有区域记录的记录，而从服务器使用自动更新机制维护主记录的副本

权威域名服务器

第二节 DNS使用及解析过程

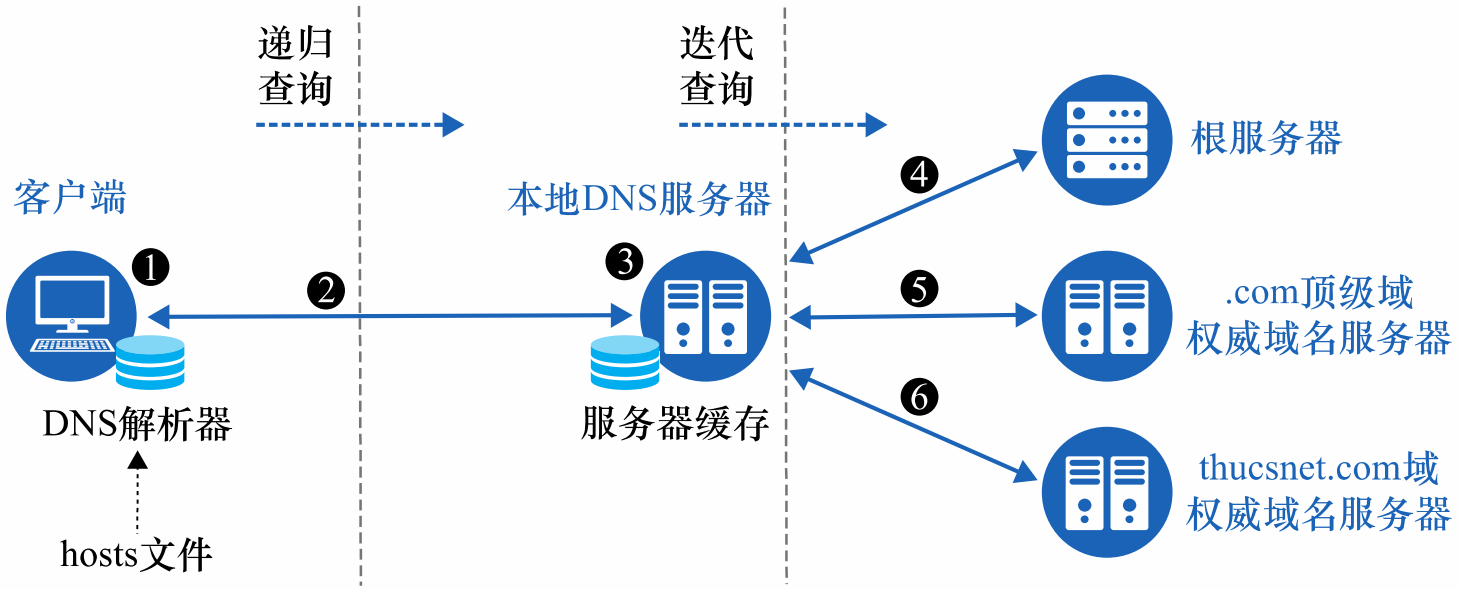
- DNS使用
- DNS解析过程

DNS使用



1. 浏览器输入域名
2. 请求到达DNS解析程序
3. 查询获得IP地址
4. 返回IP至Web浏览器
5. 访问IP地址
6. 浏览器显示该页面

DNS请求过程



1.客户端：查询本机缓存及hosts文件

2.向本地DNS服务器发送请求

3.本地DNS查找缓存，有结果就返回

4-6. 本地DNS查找根服务器、.com顶级域、thucsnet.com域，获取结果

7.本机获取IP地址

并不是每一次域名解析都完成整个查询流程

DNS反向查询

- 使用dig -x IP，DNS解析器通过迭代查询发送请求，使用IP地址获得相关域名或主机名
- 如对地址8.8.8.8发起查询，则ANSWER SECTION得到地址对应的域名

```
$ dig -x 8.8.8.8

;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa.   5       IN      PTR     dns.google.
```

第三节 DNS攻击

- 缓存中毒攻击
- 恶意DNS服务器回复伪造
- 拒绝服务攻击

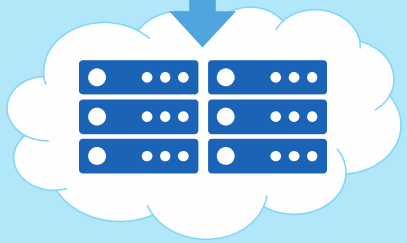
DNS攻击面

用户主机

（1）修改配置文件，导致DNS请求得到错误结果
（2）用户主机发送DNS请求时，攻击者发送欺骗回复
（3）安装流氓软件重定向DNS请求

本地DNS服务器

本地DNS服务器向互联网DNS服务器发送请求时，攻击者发起攻击



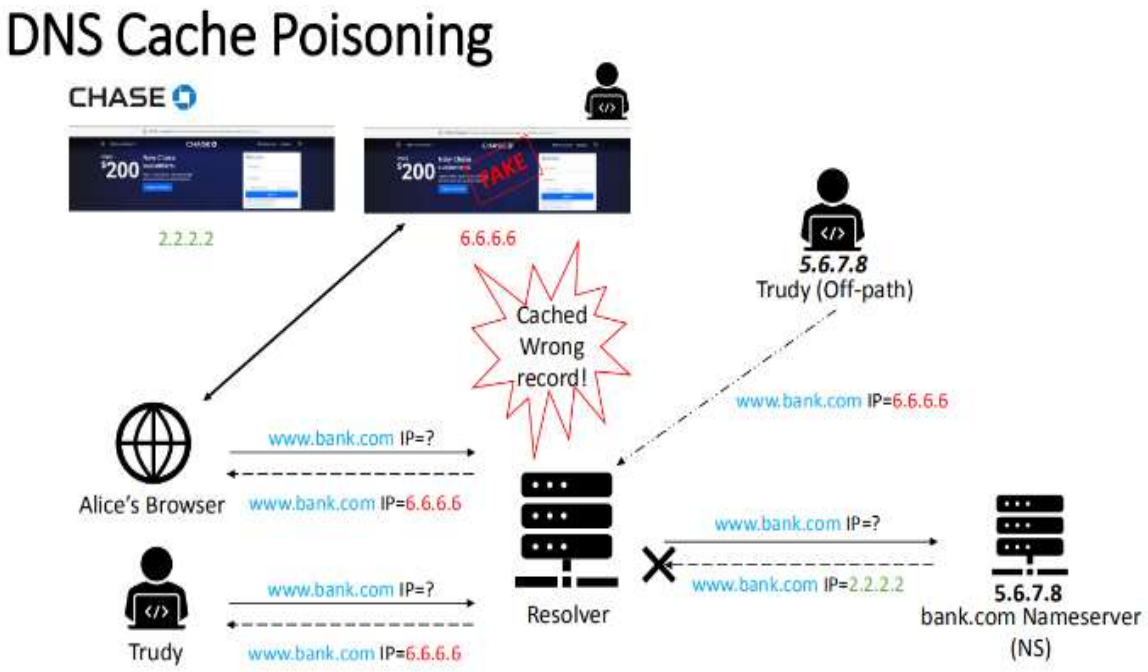
互联网DNS服务器

（1）用户接受来自恶意DNS服务器的虚假信息
（2）DNS服务器本身遭受拒绝服务等攻击

远程缓存中毒攻击：Kaminsky攻击

2008年7月，Dan Kaminsky精心构造了缓存投毒攻击，有专家认为这可能是互联网历史上最大的一次DNS安全事件

一次出人意料而名留青史的DNS投毒攻击



远程缓存中毒攻击

成功原因： **在权威区和附加区实施欺骗**

问题区：abc.example.com A

应答区： （空）

权威区： example.com NS www. example.com

附加区：www. example.com A 1.2.3.4

伪造包并没有包含abc.example.com的A记录，但告诉LDNS可以去www.example.com查询，并且www.example.com 对应的IP是1.2.3.4

解决方案： **源端口随机化，域名大小写增加攻击者猜测难度等**

远程缓存中毒攻击—基于IPID的攻击

攻击成功的前提是受害者接受该IPID，即伪造的第二个分片与真实的第一个分片具有相同IPID值，攻击者可以采取不同的操作实现

Sequentially Incrementing	Per-Destination	Random
攻击者从域名服务器中采样IPID值及增长速率，然后计算可能的IPID	对每个目的地递增的IPID，攻击者采用算法预测可能的IPID	发送多个分片按概率命中，目前Windows版本支持100个，Linux版本64个分片
>60%	<40%	少量

攻击根服务器——难以成功

DNS根服务器技术：IP Anycast + BGP

通过BGP在多个不同地点同时广播一个IP地址，BGP路由器从中选择（最近）一个作为路由

Threat Mitigation for the Root Server System

Root Server Operators
August 2019

Introduction

As of 02/28/2021 3:53 a.m., the root server system consists of 1370 instances operated by the 12 independent root server operators.

As of 02/28/2021 3:53 a.m., the root server system consists of 1370 instances operated by the 12 independent root server operators

攻击顶级服务器—巨大威胁

2013年8月25日凌晨，.CN域名凌晨出现大范围解析故障，导致大面积.CN域名无法解析，直到当日凌晨4点左右，CN根域名服务器解析才开始部分恢复

DDoS攻击背后的利益链条

大家可能会有疑问，看似普通的DDoS攻击其背后究竟隐藏着什么？一句话：为了利益。本次事故中攻击者使用的手法(譬如攻击一些“私服”的网站或主机) 并不罕见，且近些年有愈演愈烈的趋势。自国内的互联网事业兴起以来，国内有一些常年进行DDoS攻击的组织或个人，胁迫某些“私服”游戏的运营团队并收取 “保护费”，如果不合作便采取DDoS暴力攻击，使其无法正常运营。而这

中国遭到的DDoS攻击表明 TLD服务器也不安全

2013年08月28日 15:59:49 | 作者：胡杨编译 | 来源：网界网 | 查看本文手机版

本文手机版

摘要：上周末发生的让中国的部分互联网断网的DDoS攻击表明，全球各国域名的互联网实力有很大区别。

标签 顶级域名 CNNIC TLD服务器 DDoS攻击

【CNW.com.cn独家译稿】上周末发生的让中国的部分互联网断网的DDoS[注]攻击表明，全球各国域名的互联网实力有很大区别。

运行中国“.cn”顶级域名的服务器在美国东部时间星期日早上2点遭到了攻击。运行这个顶级域名的中国互联网信息中心(CNNIC)证实了这次攻击，并且向受到影响的用户道歉。

攻击特定域名服务器—影响深远

2016年，攻击者控制大量物联网设备发起DDoS攻击，造成CNN,BBC,PayPal等网站无法访问

美国Dyn公司声明：关于2016年10月21日的DDoS攻击

2016-10-23 19:06

DNS安全问题的原因及特征

DNS安全问题的本质原因?

1.客观上协议设计的不完备，缓存等面向性能优化的设计带来了安全风险

2.主观上基于利益驱动，攻击者不断挖掘漏洞

DNS攻击有哪些共有特征?

1.针对明文传输和无身份认证的实体进行欺骗性攻击

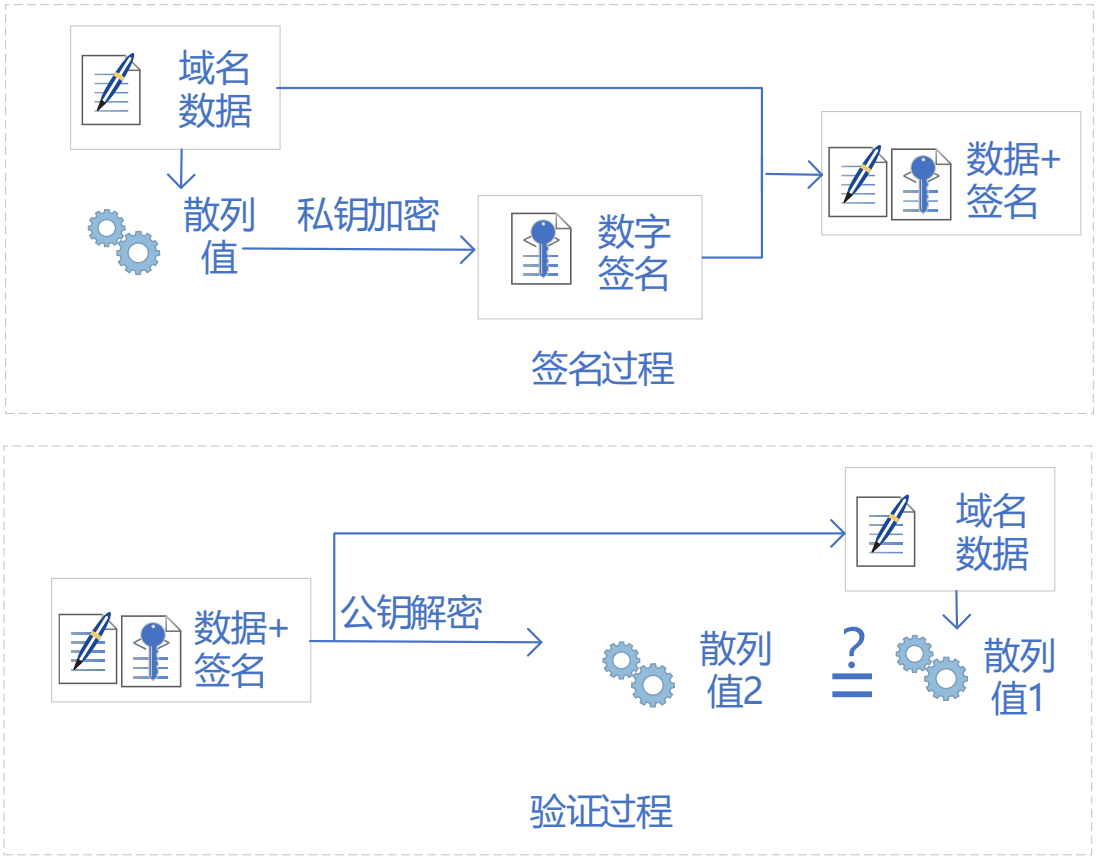
2.寻找并突破域名间复杂依赖关系，实现对域名服务器攻击

3.针对防护措施不足的服务器发起拒绝服务攻击

第四节 DNS攻击预防策略

- 基于密码技术
- 基于系统管理
- 新型架构设计

通过非对称加密验证身份--DNSSEC



DNS签名及验证过程示意图

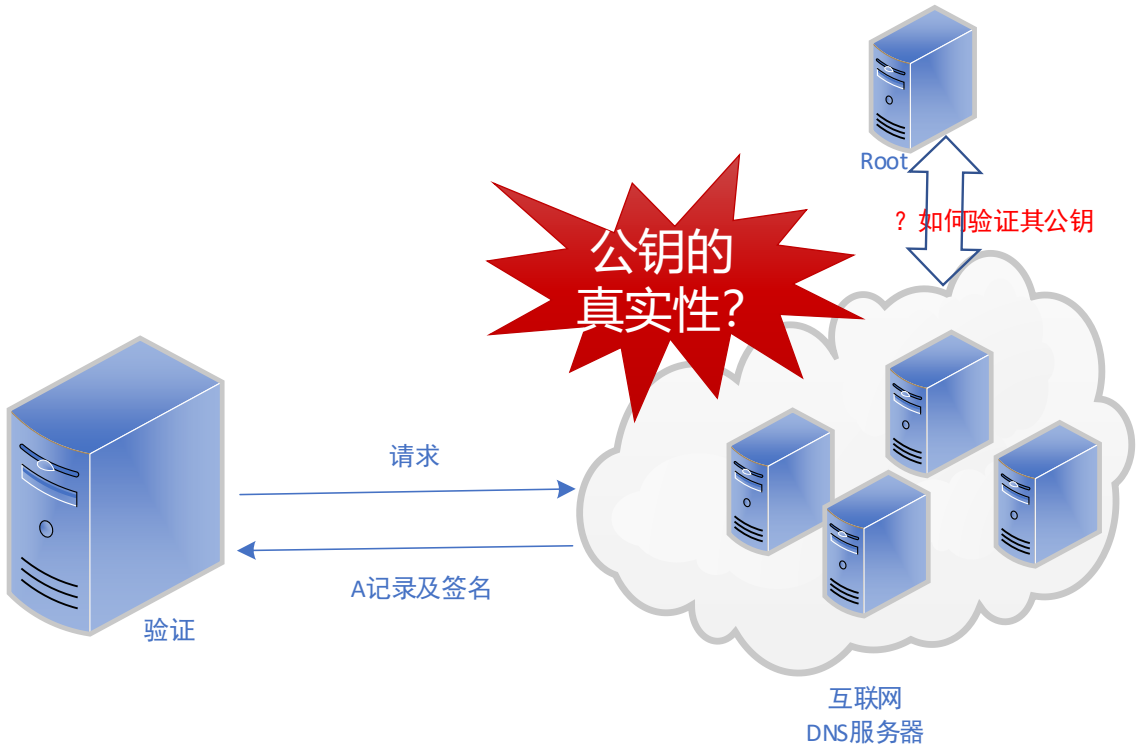
签名过程原理

域名服务器用散列函数计算回复DNS报文内容的散列值，即“内容摘要”，使用私钥对其加密（签名），加密后的信息附加到DNS报文

验证过程原理

本地DNS服务器收到DNSSEC报文，计算报文“内容摘要”，利用公钥解密收到加密“摘要”，对比“摘要”内容

通过非对称加密验证身份—DNSSEC验证公钥



DNSSEC验证需要公钥信任链

- DNSSEC需要一条信任链：支持DNSSEC的本地DNS服务器向支持DNSSEC的权威服务器发起记录请求，得到权威服务器数字签名，签名的正确性（公钥）由上级服务器保证
- 假设DNSSEC 实现了全部署，每个递归服务器只需保留根域名服务器的DNSKEY

通过非对称加密验证身份--DNSSEC

RRSIG（Resource Record Signature）

Type covered：该RRSIG涉及的DNS记录类型

Algorithm：生成最终签名所用的加密算法

Label count：原始RRSIG记录名中的标签数（用于验证通配符）

Original TTL：所涉及记录集的TTL值

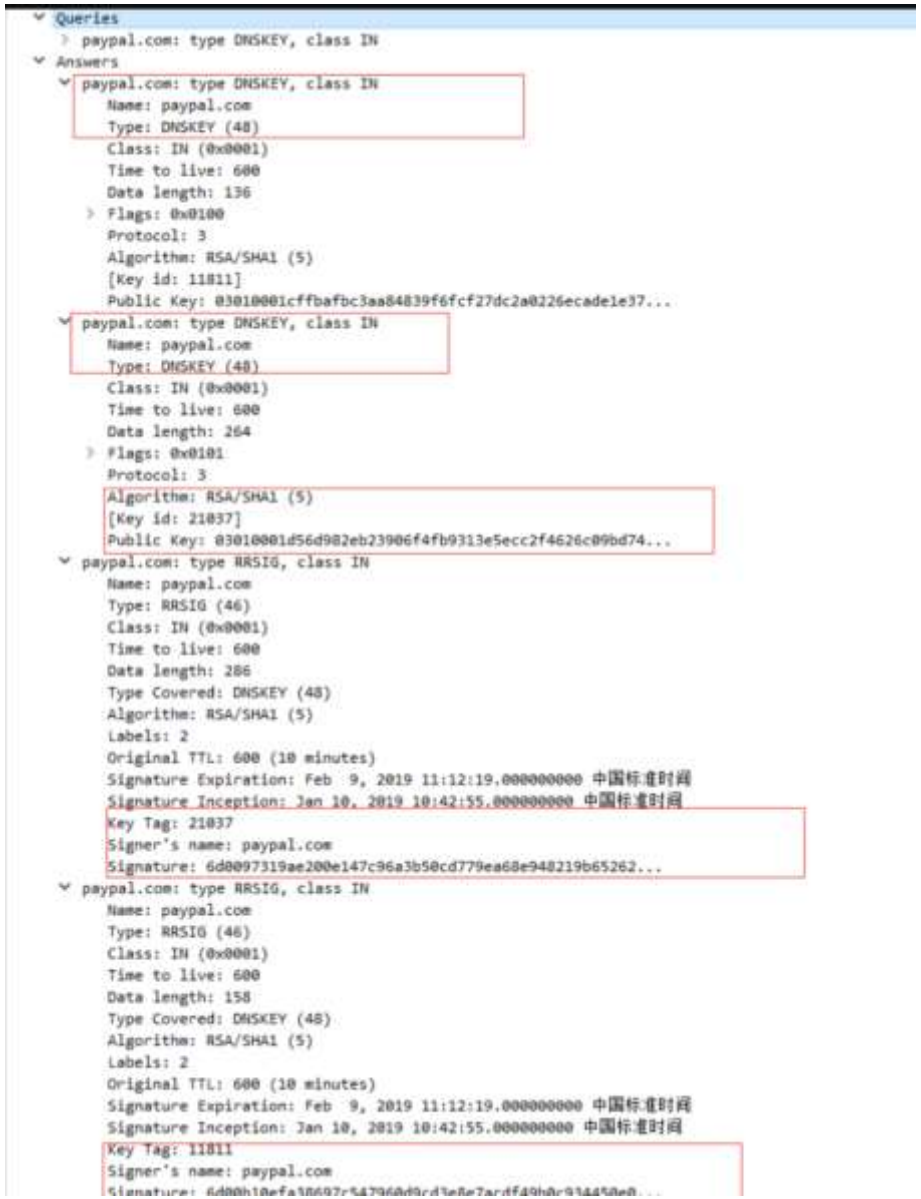
Signature expiration：签名的过期时间

Signature inception：最初创建签名的时间

Key tag：一个数字值，用于识别验证该RRSIG签名的DNSKEY记录

Signer name：用于验证该签名的DNSKEY记录名称

Signature：用于验证传输的密码学签名



通过非对称加密验证身份--DNSSEC

DNSSEC请求及验证过程

RRSIG（Resource Record Signature）

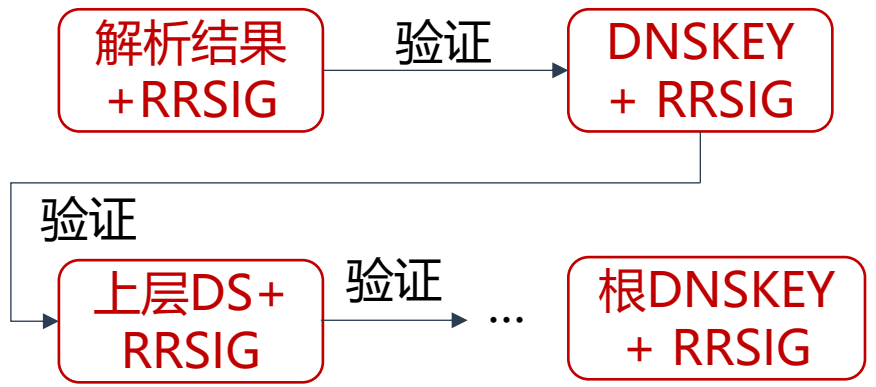
资源记录签名

DNSKEY（DNS Public Key）

公钥记录

DS（Delegation Signer）

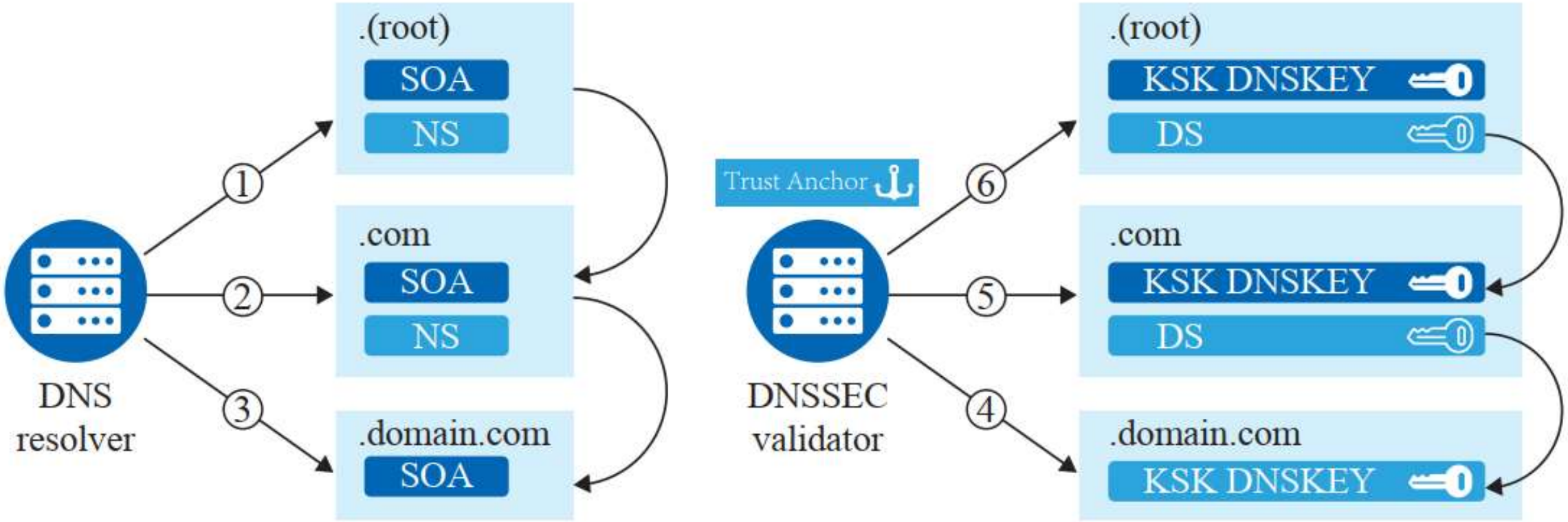
DNSKEY的散列值，DS记录存储在上级域名服务器，用于建立信任链



解析结果通过签名（RRSIG）验证，RRSIG通过公钥（DNSKEY）验证，公钥通过上级公钥散列（DS）及签名验证

通过非对称加密验证身份--DNSSEC

DNSSEC请求及验证过程



DNS-over-TLS（DoT）

可部署性

在DNSSEC被广泛接受之前（全球顶级域DNSSEC部署已经超过93%），需要找到其它解决方案有效阻止DNS攻击造成破坏

信任链

DNSSEC用DNS区域层次结构提供信任链，TLS协议依赖公钥基础设施（PKI），包括证书授权中心（CA）

数据封装

DNS-over-TLS 协议直接使用传输层安全协议对数据执行加密操作，保证了域名协议交互中信息的完整性与机密性

DNS-over-HTTPS (DoH)

数据封装

DNS-over-HTTPS（DoH）协议与现有域名系统不兼容，采用HTTPS 信道传输域名协议数据

DoH协议流量传输路径

客户端 -> DoH服务器 -> DNS服务器 -> DoH服务器 -> 客户端

通用性

部分浏览器或操作系统直接支持DoH

基于系统管理

规范配置过程

1.规范并梳理DNS配置过程中出现的漏洞

降低攻击影响

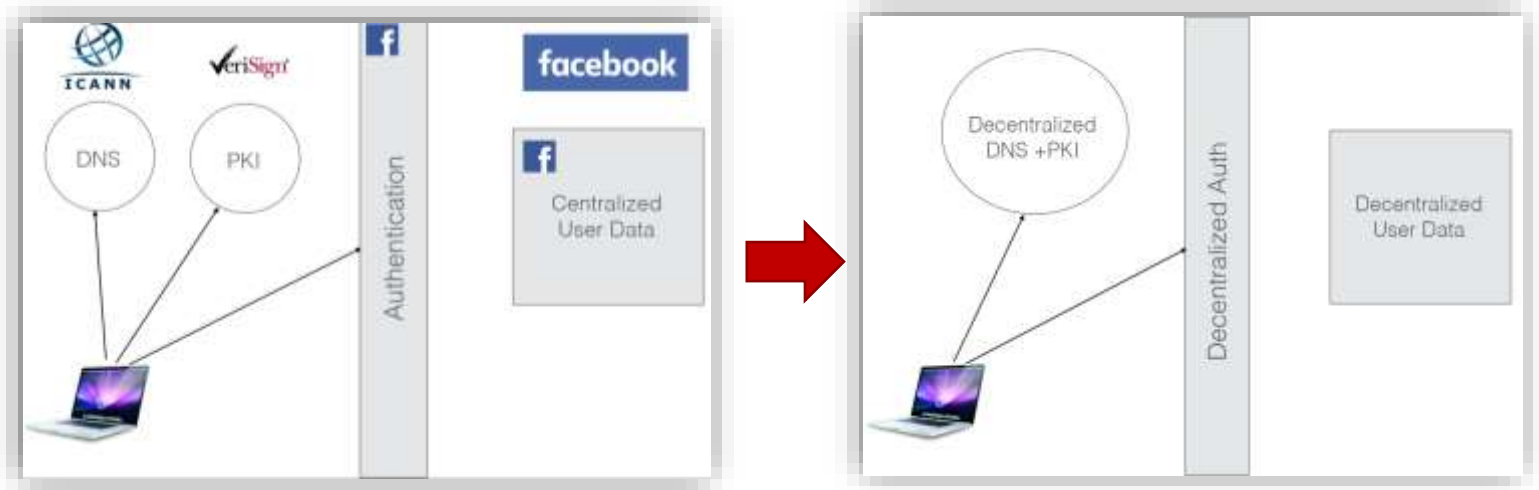
1.限制用户在短时间内发起大量DNS查询

2.增加端口猜测难度，如用于查询的UDP端口不再是默认的53，而在UDP端口范围内随机选择（排除预留端口）

3.分布式部署、恶意流量过滤等方案

蜜网和DNS防护系统联合实现BotNet检测及恶意流量过滤

新型架构设计-Blockstack



当前设计　　去中心化设计

数据层	存储用户加密后的数据
对等网络层	存储数据资源的路由信息
虚拟链层	将数据提取出来呈现给上层用户
区块链层	记录用户操作并达成共识

Blockstack 旨在建立一个去中心化的域名系统及公钥基础设施

底层采用区块链搭建，通过将域名哈希值以交易形式存储在区块链，以分布式方式避免篡改，提供可靠DNS服务

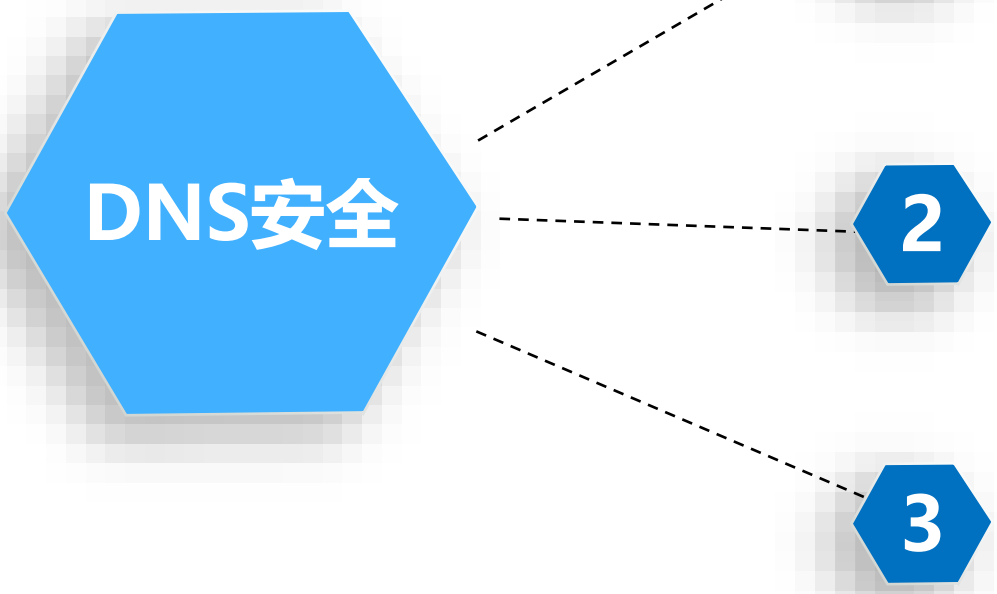
1.Muneeb Ali, et.al. Blockstack: A Global Naming and Storage System Secured by Blockchains[C] USENIX ATC 2016: 181-194

第五节 总结和展望

总结

熟悉了DNS的演进历史、域名结构、区域形式、使用原理及基本解析过程，思考了DNS潜在的安全问题，学习了常见的DNS攻击技术和防御手段

展望



现有DNS协议修改完善

基于签名、加密技术提升协议机制安全性

针对新型安全威胁寻找解决方案

研究国际化域名，以及DNS转发器等引入的新威胁

新型架构设计

从根源上解决DNS安全问题，部署较为困难，但部分思想有助于提升DNS系统的安全能力