DNSSEC

DNS 服务的安全增强标准，为 DNS 的解析内容提供保护

- 完整性
- 真实性

DNS 简介

DNS - 域名服务器，负责端系统标识（域名）与 IP 地址之间相互转换（域名解决）

域名

Domain Name

.seu.edu.cn - 标识一个三级域名管理**域**

域名区文件

Zone file

网络中的域名按**域名区**（Zone）为单位定义，同一域名区的域名具有相同的属性

（一个域名域 Domain 中可以有多个域名区）

在一个域名注册管理域注册的域名信息的格式

- 资源记录 Resource Record，RR
- 资源记录集 RRset：允许一个域名的某种资源记录可以出现多个定义（例如一个域名有两条 A 记录，对应两个不同的 IP 地址）

DNS 解析服务

DNS 服务器 - 存放 DNS 数据库的节点

DNS 客户端 - DNS 解析器

端系统通过 DNS 客户端来访问 DNS 服务器

- 为了简化管理

  DNS 协议要求对非本地域名服务器的访问总是从顶级域名服务器开始，逐层确定最终要访问的域名服务器

- 为了提高效率

  服务器和解析器使用缓存（Cache）记录一段时间的解析结果

解析结果

- 权威：DNS 服务器获得
- 非权威：缓存获得

BIND - 最广泛的 DNS 服务器实现

DNS 安全威胁

- DNS 缓存污染：**缺乏源鉴别机制**，缓存可能被错误信息污染，导致访问导向错误或服务失效
- BIND 实现中的软件缺陷和漏洞：栈溢出攻击、源点欺骗攻击，导致 DNS 配置文件篡改或解析内容的误导
- DoS/DDoS 攻击：DNS 解析服务中断，导致网络瘫痪
- 域名区传送功能（支持域名区域名整体拷贝）：泄露网络内部结构信息，被攻击者用于发现安全漏洞的主机、目标网络的规模

攻击类型

- 域名解析欺骗攻击：防范 - 再确认
- 服务失效攻击
- 服务窃取攻击：服务请求被拦截到攻击者的站点（网络钓鱼）
- 抢占（干扰）
- 针对工作环境
  - 路由劫持导致 DNS 服务失效
  - DDoS 攻击导致 DNS 服务失效
  - 管理失误导致 DNS 服务失效

DNSSEC 工作原理

基于**非对称密钥**解决 DNS 的数据完整性和源鉴别问题

通过在 DNS 配置定义时，使用非对称密钥进行签名来实现对 DNS 记录的完整性保护，并以此作为源鉴别的依据

对 RR 内容进行签名保护：依托于一个 PKI 信任链

概念

- 鉴别链：描述构成解析路径的各个域名服务器之间的信任关系
  - 形式：DNSKEY->[DS->DNSKEY]*->DNS 记录
- 鉴别密钥：解析器验证解析结果签名的公钥
- 密钥签名密钥 KSK：在一个域名区中，签名保护其它鉴别密钥的密钥（区域主密钥）
- 域名区签名密钥 ZSK：对域名区中的域名记录进行签名保护的密钥（区域会话密钥）
- 签名密钥 - 私钥
- 鉴别密钥 - 公钥
- KSK（由上一级 ZSK 验证）是一个域名区的安全起点：KSK 验证 ZSK，ZSK 验证资源记录
- 信任锚定点：位于域名区树根节点的那个域名区的 KSK（不再验证）
- 资源记录签名记录 - RRSIG：存放签名，与被签名资源记录唯一对应（存在有效期）
- DNS 公钥记录 - DNSKEY：存放用于验证 RRSIG 的公钥
- 代理签名者记录 - DS：驻留在父域名区文件中，包含了父域名区 ZSK 对某个子域名区 KSK 的签名，可据此验证子域名 KSK 的可信性
- 下一安全记录 - NSEC

安全的域名解析过程示例

每次应答都带有相关的 DNSSEC 记录

DNSKEY 记录

- 使用非对称密钥对**权威的**资源记录进行签名的**公钥**存储在 DNSKEY 记录中
- 私钥的管理由实现决定

标记字段（16 比特）

比特 7=1：ZSK

比特 15=1：KSK

父域名区的 DS 记录要指向这个 DNSKEY 记录

RRSIG 记录

权威的资源记录的数字签名保存在 RRSIG 中

具有有效期

NSEC 记录

指出下一个安全的域名记录（按字母数字顺序排列）

使得安全解析器可以明确发现要解析的域名或记录类型是否存在，以及是否存在非法插入的资源记录

每个本域名区定义的域名记录或代理签名记录需要有一个对应的 NSEC 记录

两个信息

- 指出本域名区中下一个权威记录
- 对应的域名中出现的资源记录类型

将该域名区中所有的权威记录管理成一个**链**

NSEC3

NSEC 安全隐患：利用给出的下一个权威记录中的域名对整个域名区进行域名遍历发现

引入安全**哈希**函数来**隐藏** NSEC 记录中的**域名**

DS 记录

对 DNSKEY 记录的信任证明，包含了该 DNSKEY 记录的

- 密钥标记
- 算法标识
- 整个记录的信息摘录

出现在对应 DNSKEY 记录的父域名区，在父域名区中是权威记录

TSIG

特定一次 DNS 交互时动态计算

- 用完即丢弃
- 不可缓存

DNSSEC 部署

域名区文件生成

1. 生成非对称密钥对，据此在域名区文件添加 DNSKEY 记录
2. 域名区资源记录进行签名
3. 对资源记录排序，对应位置 NSEC（NSEC3）记录
4. 上载生成的 DNSSEC 域名区文件（对 DNS 软件进行适当配置）
5. 发布本域名区的签名公钥给其他信任域（供其解析验证本域名区域名）
6. 向父域名区注册本域名区签名公钥（生成 DS 记录并签名）

密钥更新

KSK：转滚法

每个域名区应当保持至少一个备选 KSK

ICANN 对根域名区的 KSK 进行转滚：KSK-2010 -> KSK-2017

DNSSEC 脆弱性分析

可以抵御

- DNS 服务中的缓存污染
- 对域名区文件的篡改
- 域名区传送操作中的桥接攻击

未包括

- 域名数据库的保密性和访问控制
- 对 DNS 服务器的攻击和服务失效攻击
- 管理员配置错误

负面

- 实现复杂
- DNS 的响应验证大大增加了解析器的处理负担

- DNSSEC 的层次结构使得区域的安全产生相关性（高层密钥问题危及下层 DNS 数据的完整性）
- 虽然能保证域名资源记录的可信度，但是不能保证域名与实际访问对象之间的联系可信度 – 域名的残余影响（管理员疏忽）