第 5 章

DNSSEC 原理与实践

域名系统(Domain Name System,DNS)是因特网运行最重要的基础设施。DNS 通信双方由于缺乏数据来源真实性和完整性的认证机制,很容易成为攻击目标。DNS 安全扩展协议(DNSSEC)依赖数字签名和公钥系统保护 DNS 数据的可信性和完整性。本章介绍 DNS 基本概念,分析 DNS 面临的安全威胁,重点分析 DNSSEC 的工作原理和协议解析过程。通过 DNSSEC 解析过程分析和配置训练,加深对 DNSSEC 原理和工作过程的理解,提升 DNSSEC 的配置和应用能力。

5.1 基 础 知 识

5.1.1 DNS 基本概念

1. DNS 概述

DNS(域名系统)的主要作用是将易于记忆的主机名称映射为复杂的 IP 地址,从而保障其他网络应用顺利进行。

因特网的域名系统采用层次结构,域名的结构由若干分量组成,各分量之间用英文小数点隔开:

*.三级域名.二级域名.顶级域名

其各分量分别代表不同级别的域名。级别最低的域名写在最左边,而级别最高的顶级域名则写在最右边。每一级的域名都由英文字母和数字组成,完整的域名不超过 255 个字符。各级域名由其上一级的域名管理机构管理,而最高的顶级域名则由因特网的有关机构管理。域名系统既不限制每个域名需要包含下级域名的数量,也不规定每一级域名的具体含义。设计这种层次结构可以保证每个域名都是唯一的,并且也利于对具体域名的查询。

目前顶级域名 TLD 有以下三类。

(1) 国家顶级域名。采用 ISO 3166 的规定,如用 cn 表示中国、us 表示美国、uk 表示英国等。在国家顶级域名下注册的二级域名均由该国家自行确定,如我国将二级域名划分为类别域名和行政区域名。

(2) 国际顶级域名。用 int 表示。各类国际性的组织可以在 int 下注册为二级域名。

(3) 通用顶级域名。目前,通用顶级域名主要有以下几种。com 表示公司企业,net 表示网络服务机构,org 表示非营利性组织,edu 表示教育机构,gov 表示政府部门(美国专用),mil 表示军事部门(美国专用),firm 表示公司企业,shop 表示销售公司和企业,web 表示从事万维网活动的单位,arts 表示从事文化、娱乐活动的单位,rec 表示从事消遣、娱乐活动的单位,info 表示提供信息服务的单位,nom 表示个人。

域名系统的层次结构如图 5-1 所示。

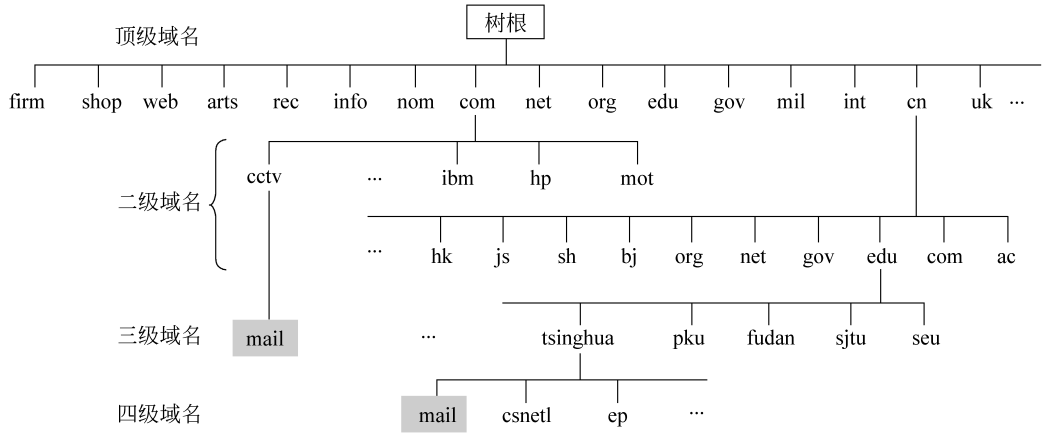

图 5-1 域名系统的层次结构

DNS 的层次结构可以形象比喻为倒立的大树，树根在最上面，树根下面一级的结点就是 DNS 最高一级的顶级域名。树状层次结构最下面的结点就是用户端的单台计算机。

2. 域名服务器

因特网 DNS 是一个联机分布式数据库系统，也是按照域名的层次来安排的。每一个域名服务器都只对域名体系中的一部分进行管辖。现在共有以下三种不同类型的域名服务器。

(1) 本地域名服务器。

本地域名服务器也称为默认域名服务器。本地域名服务器的主要功能是，当一个主机发出 DNS 查询报文时，这个查询报文就首先被送往该主机的本地域名服务器。本地域名服务器离用户较近，一般不超过几个路由器的距离。当所要查询的主机也属于同一个本地 ISP 时，该本地域名服务器立即将所查询的主机名转换为它的 IP 地址，而不需要再去询问其他的域名服务器。

本地域名服务器通常被划分为权威域名服务器和递归域名服务器。对于一个特定的域名空间，如果一个域名服务器存有这个域名空间的所有信息，则将这个域名服务器称为这个域名空间的权威域名服务器，否则称为递归域名服务器。

每一个因特网服务提供商 ISP，或者某个相对独立的单位(如一个公司、一个大学等)都可以拥有一个本地域名服务器。但也并不意味着所有用户都直接使用本地域名服务器，也有些用户使用的是因特网上的一些公共域名服务器，这些公共域名服务器往往是因特网上知名的大型域名服务器，例如国内的百度域名服务器(180.76.76.76)、腾讯域名服务器(119.29.29.29、182.254.118.118)，国外的谷歌域名服务器(8.8.8.8.8.8.4.4)等。这些公共域名服务器从功能上也具有本地域名服务器的功能。

(2) 根域名服务器。

当一个本地域名服务器由于没有保存被查询主机的信息，不能立即回答某个主机的查询时，该本地域名服务器就以 DNS 客户的身份向某一个根域名服务器查询。若根域名服务器有被查询主机的信息，就发送 DNS 回答报文给本地域名服务器，再由本地域名服务器将信息返还给发起查询的主机。但当根域名服务器没有被查询主机的信息时，该根

域名服务器就必须知道哪个权威域名服务器保存了要查询的信息，进而由该权威域名服务器继续发起查询。

需要说明的是，根域名服务器并不直接对顶级域下面所属的所有域名进行转换，它主要负责找到下面的所有二级域名的域名服务器。

目前全世界IPv4根域名服务器只有13台（这13台IPv4根域名服务器名字分别为A至M）。其中1台IPv4根域名服务器为主根服务器，位于美国。其余12台根域名服务器为辅根服务器，其中9台在美国，2台在欧洲（位于英国和瑞典），1台在日本。另外，自2002年启用AnyCast技术以来，根域名服务器的镜像数量近年来也飞速增长。2013年根镜像达到了346个，到2023年底，全球已经有1515个镜像。

（3）权威域名服务器。

权威域名服务器，也简称为“权威服务器”。需要提供互联网服务的每台主机都必须在权威域名服务器处注册登记。为了更加可靠地工作，一个主机最好有至少两台权威域名服务器。一般情况下，该主机的权威域名服务器就是它的本地ISP的一台域名服务器。实际上，许多域名服务器同时充当本地域名服务器和权威域名服务器。权威域名服务器的一项核心功能就是能够准确地将其管辖的主机名转换为该主机的IP地址。

3. DNS查询过程

DNS采用客户端/服务器方式。每一台域名服务器收到其他域名服务器的域名查询信息时，如果自己能够进行域名到IP地址的转换，则直接返回信息。如果自己不能进行域名到IP地址的转换，则必须具有连向其他域名服务器的信息，即能够知道到什么地方去找别的域名服务器。

DNS具体查询过程如下。当某一个应用进程需要将主机名映射为IP地址时，该应用进程就成为DNS的一个客户，并将待转换的域名放在DNS请求报文中，以UDP数据报方式发给本地域名服务器。本地的域名服务器在查找域名后，将对应的IP地址放在回答报文中返回。应用进程获得目的主机的IP地址后即可进行通信。若域名服务器不能回答该请求，则此域名服务器就暂时成为DNS中的一个客户，向DNS中其他域名服务器发起查询请求，直至找到能够回答该查询请求的域名服务器为止。

DNS查询有两种方式：递归和迭代。DNS客户端设置使用的DNS服务器一般都是递归服务器，它负责全权处理客户端的DNS查询请求，直到返回最终结果。而DNS服务器之间一般采用迭代查询方式。

下面举例说明递归查询方式和迭代查询方式的查询过程，如图5-2所示。

在图5-2中，域名为m.xyz.com的主机需要查询域名为t.y.abc.com的主机的IP地址。具体的查询过程如下。

（1）域名为m.xyz.com的主机首先向其本地域名服务器dns.xyz.com查询。如果该本地域名服务器能够解析该域名的IP地址，则直接将结果返还给查询主机。如果无法直接解析，则查询过程进入下一步骤。

（2）由于本地域名服务器dns.xyz.com无法解析该域名的IP地址，本地域名服务器dns.xyz.com就向根域名服务器dns.com（顶级域名服务器）发送查询信息。

（3）根域名服务器dns.com不会直接解析域名信息，而是根据被查询的域名中的abc.com信息，向权威域名服务器dns.abc.com发送查询报文。

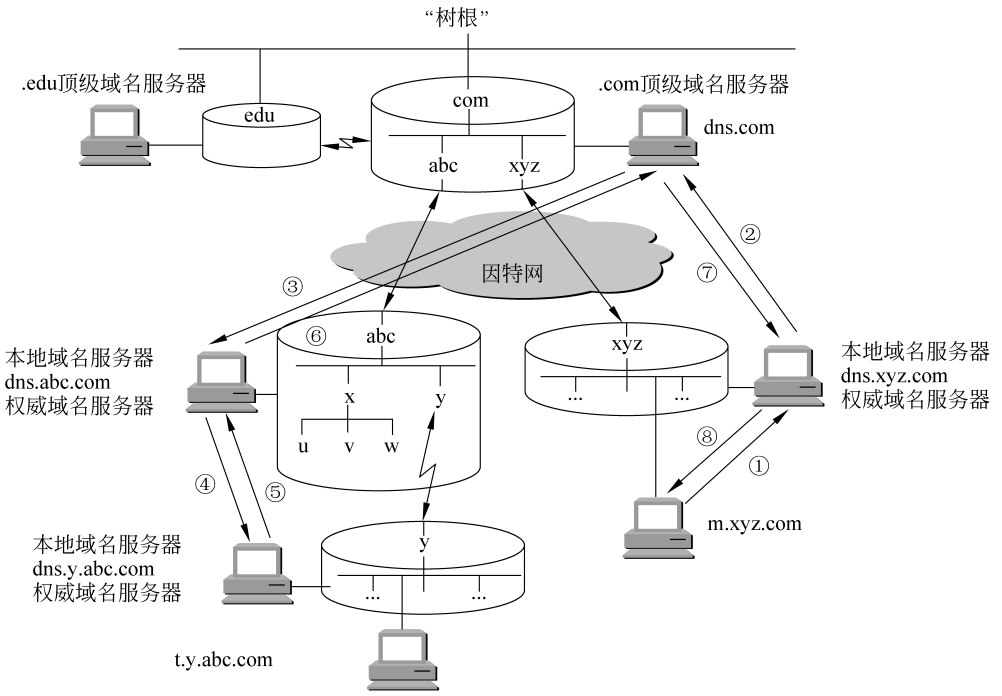

图 5-2　DNS 递归查询过程

(4) 权威域名服务器 dns.y.abc.com 解析得到 t.y.abc.com 的主机的 IP 地址。

如图 5-2 所示，整个域名查询的顺序为①→②→③→④。得到结果后，按照查询过程的相反顺序，将解析结果返回给查询主机，具体顺序为⑤→⑥→⑦→⑧。这种查询方法即为“递归查询”。

在递归查询过程中，根域名服务器充当了 DNS 客户端的作用，向权威域名服务器发送查询报文，并将解析结果返回给本地域名服务器。为了减轻根域名服务器的负担，根域名服务器可以在收到本地域名服务器的查询报文时，直接将域名服务器的 IP 地址返还给本地域名服务器，然后由本地域名服务器直接向权威域名服务器发起查询过程，从而减轻根域名服务器的工作负担。在此期间，根域名服务器发挥了迭代查询的功能，而其他服务器仍然发挥递归查询的功能。这种查询方式就是递归与迭代相结合的查询方式，工作过程如图 5-3 所示。

为了减小 DNS 查询开销，DNS 设计了 DNS 高速缓存机制。每个域名服务器都维护一个高速缓存，用来存放最近查询过的域名与 IP 映射数据，以及从何处获得该映射数据的记录。许多主机在启动时会从本地域名服务器下载域名和 IP 地址的全部数据库，保存在自己最近使用的域名高速缓存中。在主机应用程序需要解析某个域名时，首先会查询自己的域名高速缓存。如果保存有该域名信息则可以直接读取，而不用启用 DNS 服务器域名查询流程。只有当域名信息不在自己的域名高速缓存中，才会启用 DNS 服务器域名查询流程。主机需要定期检查域名服务器以获取新的域名信息。由于域名改动并不频繁，所以保持域名数据库的一致性并不需要太大开销。

DNS 高速缓存机制的存在，实际上大大减轻了域名服务器的计算负担，使得域名服

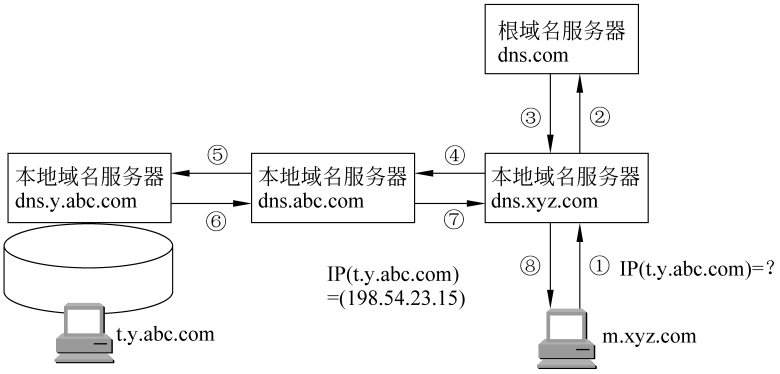

图 5-3　递归与迭代相结合的查询方式

务器可以为更多主机提供服务。

5.1.2　DNS 面临的安全威胁

DNS 工作机制是建立在互信模型的基础之上的，是一个完全开放的协议体系。DNS 协议中没有提供数据加密和认证机制，没有对各种查询进程准确识别，对网络基础设施和核心骨干设备的攻击没有考虑防护措施。DNS 面临常见的安全威胁包括以下几种。

1. 域名欺骗

域名欺骗是最常见的攻击方式，攻击者通常伪装成客户可信的 DNS 服务器，然后将伪造的恶意信息反馈给客户。常见的域名欺骗主要包括事务 ID 欺骗和缓存投毒。

（1）事务 ID 欺骗。

事务 ID 欺骗是针对 DNS 数据报首部的事务 ID 进行的。由于客户端会用该 ID 作为响应数据报是否与查询数据报匹配的判断依据，因此攻击者伪装成 DNS 服务器提前向客户发送与查询数据报 ID 相同的响应报文，只要该伪造的响应报文在真正的响应报文之前到达客户端，就可以实现域名欺骗。

对事务 ID 的获取主要采用网络监听和序列号猜测两种方法。其中，网络监听比较简单，由于 DNS 数据报文都没有加密，因此只要攻击者能够监听到 DNS 服务器之间的网络流量即可获得事务 ID。序列号猜测的方法指直接对 DNS 查询报文的事务 ID 进行猜解。从理论上来讲，由于事务 ID 字段为 2 字节，限制了其 ID 值只能是 0～65535，大大降低了猜测成功的难度。

（2）缓存投毒。

在 DNS 查询机制中，为了减少不必要的带宽消耗和客户端延迟，DNS 设计了高速缓存机制。缓存投毒是指攻击者将“污染”的缓存记录插入正常的 DNS 服务器的缓存记录中。所谓“污染”的缓存记录指 DNS 解析服务器中域名所对应的 IP 地址不是真实的地址，而是由攻击者篡改的地址，这些地址通常对应着由攻击者控制的服务器。

高速缓存的存在虽然减少了访问时间，却是以牺牲一致性为代价的，同时也使得服务器发生缓存中毒的可能性增大，极大削弱了 DNS 系统的可用性。同时攻击者可以利用 DNS 协议中缓存机制中对附加区数据不做任何检查的漏洞，诱骗域名服务器缓存具有较大 TTL 的虚假资源记录，从而达到长期欺骗客户端的目的。

缓存投毒的具体实现过程如下。

① 用户 A 向解析器 R 请求查询 xxx.baidu.com 的 IP 地址。

② 如果 R 中没有缓存 xxx.baidu.com 的域名与 IP 数据，R 将会转向 baidu.com 的权威域名服务器。

③ 假设 R 合法解析得来的地址是 IP1，但是攻击者会在该响应到达前，伪造大量解析地址为 IP2 响应包发送给 R。而 IP2 是攻击者控制的服务器，通常为钓鱼网站等。

④ R 很难检测来源响应的真实性，并且根据 DNS 接收策略，当接收到第一个响应包后会丢弃随后的响应，随后 R 会将该条记录存入自身缓存中，这样就完成了缓存投毒的过程。

⑤当其他合法用户查询时，R 由于缓存中已经存入 IP2 且尚未过期，会直接将 IP2 响应给用户，致使用户访问被攻击者控制的站点，从而达到缓存投毒的目的。

2. 拒绝服务攻击

针对 DNS 的拒绝服务攻击(Denial of Service，DoS)分为两类：一类是直接对域名服务器或客户端进行攻击，另一类是利用 DNS 系统作为反射点来攻击其他目标。

(1) 针对 DNS 系统客户端的 DoS 攻击。

针对 DNS 系统客户端的 DoS 攻击主要通过发送否定回答显示域名不存在，从而制造黑洞效应，对客户端造成事实上的 DoS 攻击。对域名服务器的攻击则是直接以域名服务器为攻击目标。

(2) 反射式 DoS 攻击。

反射式 DoS 攻击中，攻击者利用域名服务器作为反射点，用 DNS 应答对被攻击目标进行洪泛攻击，很显然反射式 DoS 攻击的目标不是 DNS 系统本身。由于 DNS 协议设计上的原因，查询报文通常很小，而响应报文在采用 UDP 传输情况下最大可达 512 字节，因而能够产生放大式的攻击效果。超过 512 字节的报文又采用 TCP 传输，更增加了分布式拒绝服务攻击(Distributed Denial of Service，DDoS)攻击成功的概率。

3. 域名解析过程劫持攻击

在域名解析过程劫持攻击中，攻击者通常伪装成客户可信任的实体对通信过程进行分析和篡改，将客户请求重定向到假冒的网站等与请求不符的目的地址，从而窃取客户的账户和密码等机密信息，进行金融欺诈和电子盗窃等网络犯罪活动。

在因特网中，运营商的 DNS 解析服务器一直受到质疑(由于植入广告等原因)，而公共 DNS 服务器(如百度的 180.76.76.76)由于其良好的安全性与稳定性被越来越多的互联网用户所信任。发起域名解析过程劫持攻击的攻击者，正是利用用户对公共 DNS 服务器的信任，将用户发往公共 DNS 的请求劫持，并转发到其他的解析服务器。除此之外，劫持者还会伪装成公共 DNS 服务的 IP 地址，对用户的请求进行应答。从终端用户的角度来看，这种域名解析路径劫持难以被察觉。域名解析过程劫持攻击过程如图 5-4 所示。

正常情况下，用户使用公共 DNS 服务器进行 DNS 解析的路径如图 5-4 中的实线所示。如果该 DNS 请求流量被网络上监控设备监控到，攻击者就可以将满足预设条件的 DNS 请求转发到中间盒子，并使用其他替代的 DNS 服务器处理用户的 DNS 请求。最终，中间盒子通过伪造 IP 源地址的方式将 DNS 应答包发往终端用户。此时的解析路径如图 5-4 中的虚线所示。

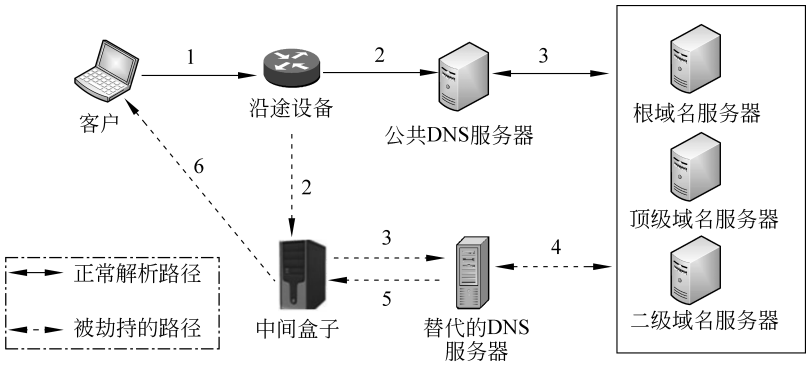

图 5-4　域名解析过程劫持攻击

4. 域名配置攻击

域名配置攻击是指攻击者利用 DNS 协议配置的随意性弱点来实施攻击。这种攻击方法的典型代表是对 DNS 通配符的滥用，攻击者通常利用通配符条目来混淆其要真正攻击的目的主机，垃圾邮件也会利用这点向主机名嵌入跟踪信息来验证真实的邮件账号，从而避开反垃圾邮件系统的检测。

5. 区域传送信息泄露攻击

大多数 DNS 系统的运行至少需要两台 DNS 服务器：一台主服务器和一台用来容错的辅助服务器。DNS 服务器之间通过复制数据库文件进行同步，这一过程称为“区域传送”。辅助服务器既可以从主服务器装载数据文件，也可以从其他辅助服务器装载。在传送过程中，攻击者非法获取区域传送信息，从而窃取内部网络拓扑、主机名和操作系统等信息，进而从这些信息中判断其功能或发现其他具有漏洞的其他主机，为进一步发起网络攻击提供可能。

5.1.3　DNSSEC 的工作原理及解析流程

1. 解决 DNS 安全问题的基本思路

DNS 面临诸多安全威胁的核心原因是 DNS 协议中没有提供数据加密和认证机制，没有对各种查询进程准确识别，无法对网络基础设施和核心骨干设备的攻击采取防护措施。解决 DNS 安全问题的基本思路包括以下两方面。

(1) DNS 对域名进行解析过程中，必须对 DNS 服务器的响应信息进行源端鉴别，避免篡改或伪造响应信息；

(2) 对 DNS 查询信息进行完整性检测，只有通过源端鉴别和完整性检测的 DNS 响应消息才会进行处理，避免服务器或客户端受到伪造或篡改 DNS 消息的攻击。

因此在 DNS 原有功能的基础上，DNSSEC 提供了以下 3 项安全服务。

(1) 提供数据来源验证，保证 DNS 数据来自正确的域名服务器。

(2) 提供数据完整性验证，保证数据在传输过程中没有任何更改。

(3) 提供否定存在验证，对否定应答报文提供验证信息。

2. 新增资源记录类型

为实现上述安全服务，DNSSEC 新增加了 4 种类型的资源记录：DNSKEY（DNS

Public Key)、RRSIG(Resource Record Signature)、DS(Delegation Signer)和 NSEC(Next Secure)。

(1) DNSKEY 资源记录。

DNSKEY 资源记录用来存储 DNS 服务器的公开密钥。DNSKEY 记录协议的格式如图 5-5 所示。

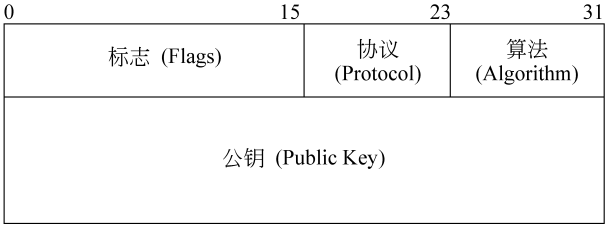

图 5-5 DNSKEY 协议格式

其中,标志(Flags)字段,16 位。第 7 位(左起为第 0 位)是区密钥(Zone Key)标志,记为 ZK。如果 ZK 为 1,则表明它是一个区密钥,该密钥可以用于签名数据的验证,而且资源记录的所有者必须是区的名字。

协议(Protocol)字段,8 位,其值必须是 3,表示这是一个 DNSKEY,该字段其他的值不能用于 DNSSEC 签名的验证。

算法(Algorithm)字段,8 位,指明签名所使用的算法的种类。DNSKEY 支持的签名算法包括 RSA/MD5 算法、DH 算法、DSA/SHA-1 算法、Elliptic Curve 算法和 RSA/SHA-1 算法。

最后一个字段是公钥(Public Key)字段,它的格式依赖于算法字段。

在 DNSSEC 的认证和加密机制中,使用两对密钥来配合完成签名信任链的建立。第一对密钥用来对区内的 DNS 资源记录进行签名,称为区签名密钥(Zone Signing Key,ZSK),由权威认证服务器生成、签名。权威认证服务器在每次 DNS 查询的时候都会使用 ZSK 对查询结果(资源记录)进行数字签名,并将数字签名放在 RRSIG 记录中。ZSK 可以通过 DNSKEY 记录获取。

为了防止 ZSK 被修改,DNSSEC 还使用了另一对被称为密钥签名密钥(Key Signing Key,KSK)的公私钥对,用来对包含密钥(如 ZSK)的资源记录(DNSKEY)进行签名,并将签名结果放在 DNSKEY 的 RRSIG 记录中。在 DNSKEY 记录中,会同时包含 ZSK 和 KSK。因此,在一个区(zone)中,除 DNSKEY 记录外,其他的记录均由 ZSK 签名。

(2) RRSIG 资源记录。

RRSIG 资源记录用来存储对资源记录集合(RR Sets)的数字签名,协议格式如图 5-6 所示。

其中,类型覆盖(Type Covered)字段,16 位,表示这个签名覆盖什么类型的资源记录集合。

算法(Algorithm)字段,8 位,指明采用的数字签名算法,同 DNSKEY 记录的算法字段。

标签(Label)字段,8 位,指明被签名的资源域名记录(RRSIG)所有者中的标签数量。

起始 TTL、签名过期(有效期结束)时间、签名开始时间,均为 32 位。其中,有效开始

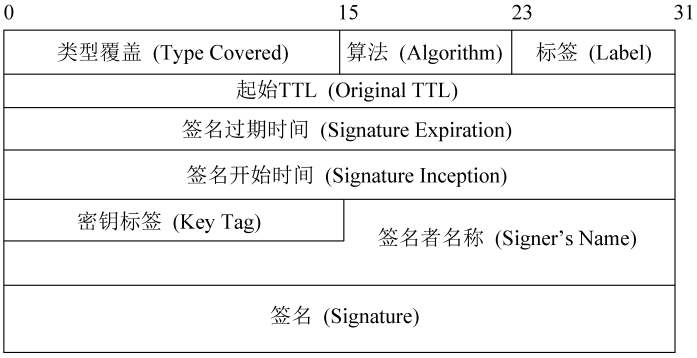

图 5-6　RRSIG 协议格式

时间和结束时间均是从 1970 年 0 时 0 分 0 秒(UTC 时间)开始的秒数。签名必须在开始时间和结束时间之间才有效。

密钥标签(Key Tag)字段,它是用对应公钥数据简单叠加得到的一个 16 位整数(采用网络字节序)。

签名者名称(Signer's Name)字段,表明 DNSKEY RR 记录的所有者的名称。

签名(Signature)字段,包含产生的签名值。

(3) NSEC 资源记录。

NSEC 记录是为了应答那些不存在的资源记录而设计的。

(4) DS 资源记录。

DS 记录存储 DNSKEY 的散列值,用于验证 DNSKEY 的真实性,从而建立一个信任链。不同于 DNSKEY 存储在资源记录所有者所在的权威域的区文件中,DS 记录存储在上级域名服务器(Delegation)中。

3. DNSSEC 解析过程

下面举例说明 DNSSEC 域名解析过程,如图 5-7 所示。终端 A 配置的本地域名服务器为 a.com 域名服务器,且终端 A 已经具有该本地域名服务器的公钥 PK_{AC}。假设终端 A 中某应用程序欲解析域名为 www.b.edu 的 IP 地址。与该解析过程相关的 edu 域名服务器的 IP 地址为 192.2.2.7,b.edu 域名服务器的 IP 地址为 192.2.3.7。

具体解析过程如下。

(1) 终端 A 向其本地域名服务器(a.www 域名服务器)发送域名 www.b.edu 的解析请求。

(2) a.www 域名服务器接收到终端 A 的域名解析请求后,首先查找其高速缓存中是否存在相关解析记录。如果有相关记录,则直接向终端 A 返回域名 www.b.edu 的 IP 地址,解析过程结束。

如果本地域名服务器中不存在域名 www.b.edu 的相关记录,则本地域名服务器在数据库中检索名字为 b.edu,类型为 NS 的资源记录。如果存在相关记录,则由此确定根域名服务器。

如果不存在上述的资源记录,则检索名字为 edu,类型为 NS 的资源记录。根据资源记录确定根域名服务器。

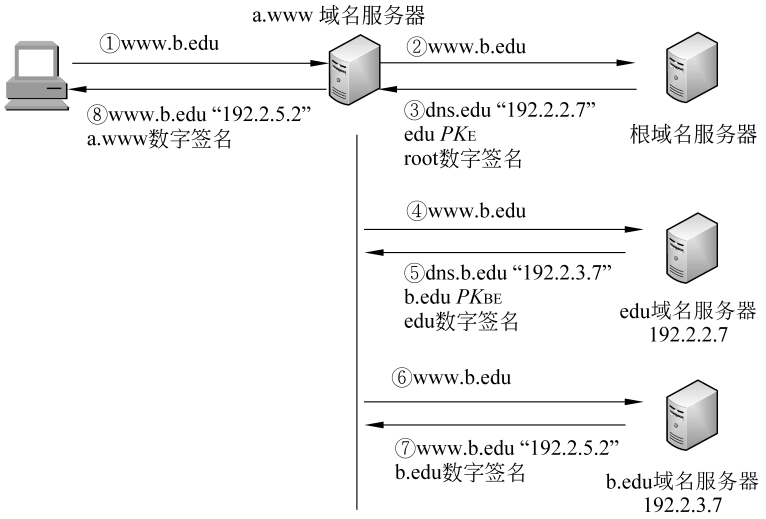

图 5-7 DNSSEC 解析过程

本地域名服务器根据上一步确定的根域名服务器地址，向根域名服务器发送域名 www.b.edu 的解析请求。

根域名服务器依次检索名字为 www.b.edu、类型为 A 的资源记录，名字为 b.edu、类型为 NS 的资源记录，名字为 edu、类型为 NS 的资源记录。根据资源记录确定 edu 域名服务器。

(3) 根域名服务器向本地域名服务器回送 edu 域名服务器的 IP 地址 192.2.2.7、edu 域名服务器的公钥 PK_E、用 root 域的私钥 SK_R 产生的数字签名 D_{SK_R}。

(4) 本地域名服务器接收到根域名服务器的 DNS 响应消息后，首先用 root 域的公钥 PK_R 验证根域名服务器的数字签名，记录下 edu 域的公钥 PK_E。然后向 edu 域名服务器发送域名 www.b.edu 的解析请求。

(5) edu 域名服务器向本地域名服务器回送 b.edu 域名服务器的 IP 地址 192.2.3.7、b.edu 域名服务器的公钥 PK_{BE} 和用 edu 域名服务器的私钥 SK_E 产生的数字签名 DS_{KE}。

(6) 本地域名服务器用 edu 域名服务器公钥 PK_E 验证用 edu 私钥加密的数字签名 DS_{KE}，获取 b.edu 域名服务器的 IP 地址。

本地域名服务器向 b.edu 域名服务器发送域名 www.b.edu 的解析请求。

(7) b.edu 域名服务器接收到本地域名服务器发送的解析请求，向本地域名服务器回送域名 www.b.edu 的 IP 地址 192.2.5.2、用 b.edu 域名服务器私钥 SK_{BE} 产生的数字签名 D_{SKBE}。

(8) 本地域名服务器用根域名服务器发送的 edu 域的公钥 PK_E 验证 edu 域名服务器的数字签名。

本地域名服务器接收到 b.edu 域名服务器发送的解析结果后，用 edu 域名服务器发送的 b.edu 域的公钥 PK_{BE} 验证 b.edu 域名服务器的数字签名。

本地域名服务器完成对 b.edu 域名服务器发送的解析结果的源端鉴别和完整性检测后，向终端 A 发送解析结果。

本地域名服务器向终端 A 发送解析结果时，用 a.com 域的私钥 SK_{AC} 产生解析结果