DNSSec

1.简介

DNSSEC依靠数字签名保证DNS应答报文的真实性和完整性。权威域名服务器用自己的私有密钥对资源记录(Resource Record, RR)进行签名，解析服务器用权威服务器的公开密钥对收到的应答信息进行验证。如果验证失败，表明这一报文可能是假冒的，或者在传输过程、缓存过程中被篡改了。

1. 原理
2. 一个支持DNSSEC的解析服务器向支持DNSSEC的权威域名服务器请求域名[www.test.net](http://www.test.net/).时，它除了得到一个标准的A记录(IP 地址)以外，还收到一个同名的RRSIG记录，其中包含test.net这个授权域的数字签名，它是用test.net.的私有密钥来签名的。
3. 为了验证这一签名的正确性，解析服务器可以再次向test.net的域名服务器查询响应的公开密钥，即DNSKEY资源记录。
4. 假设解析服务器开始并不信任test.net.的公开密钥， 它可以到test.net.的上一级域名服务器net.那里查询test.net.的DS(Delegation Signer， 即DS RR)记录，DS RR中存储的是test.net. 公钥的散列值(比如用MD5算法计算得到的128比特数据，再用base64编码得到的一个字符串)。
5. 假设解析服务器由管理员手工配置了.net的公钥(即Trust Anchor)，它就可以验证test.net.公钥(DNSKEY)的正确与否了。就不用询问根节点.net.的公钥真实性。

(5)然后解析服务器就可以用其中的公钥验证上述记录的真实性与完整性。

3.DNSKEY记录

DNSKEY资源记录存储的是公开密钥

example.com. 86400 IN DNSKEY 256 3 5 ( AQPSKmy…..aNvv4w== )

其中256是标志字段(flag)，它是一个16比特的数，如果第7位(左起为第0位。这一位是区密钥(Zone Key)标志, 记为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(example.com.)必须是区的名字。第十五称为安全入口点(Security Entry Point，SEP)标志

下一个字段“3”是协议(protocol)字段，它的值必须是3 ，表示这是一个DNSKEY，这是为了与以前版本DNSSEC兼容而保留下来的。其他的值不能用于DNSSEC签名的验证。

下一个字段“5”是算法(Algorithm)字段，标识签名所使用的算法的种类。其中常用的几种：1：RSA/MD5; 3：DSA/SHA-1; 5:RSA/SHA-1。

最后括号中的是公开密钥(Public Key)字段，它的格式依赖于算法字段。

在实践中，权威域的管理员通常用两个密钥配合完成对区数据的签名。一个是Zone-Signing Key(ZSK)，另一个是Key-Signing Key(KSK)。ZSK用于签名区数据，而KSK用于对ZSK进行签名。这样做的好处有二：

(1)KSK的密钥签名的数据量很少，被破解(即找出对应的私钥)概率很小，因此可以设置很长的生存期。这个密钥的散列值作为DS记录存储在上一级域名服务器中而且需要它的数字签名，较长的生命周期可以减少密钥更新的工作量。

(2)ZSK签名的数据量比较大，因而破解的概率较大，其生存期应该小一些。因为有了KSK的存在，ZSK可以不必放到上一级的域名服务中，减少了管理的开销。

4.RRSIG记录

RRSIG资源记录存储的是对资源记录集合(RRSets)的数字签名。

host.example.com. 86400 IN RRSIG A 5 3 86400 20030322173103  
　　 (  
 　　20030220173103 2642 example.com.  
 　　oJB1W6WNGv+ldvQ3WDG0MQkg5IEhjRip8WTr  
　　 …  
 　　J5D6fwFm8nN+6pBzeDQfsS3Ap3o= )

从第五个字段(“A”)开始各字段的含义如下：

　　类型覆盖(The Type Covered Field)：表示这个签名覆盖什么类型的资源记录，本例中是A。

　　算法：数字签名算法，同DNSKEY记录的算法字段；本例中5表示RSA/SHA-1。

　　标签数量(The Labels Field)：被签名的资源域名记录所有者(host.example.com.)中的标签数量，如本例中为3，\*.example.com.为2，“.”的标签数量为0。

　　接下来的几个字段分别是被签名记录的TTL、有效期结束时间、开始时间。

2642是密钥标签(Key Tag)，它是用对应公钥数据简单叠加得到的一个16比特整数。如果一个域有多个密钥时(如一个KSK、一个ZSK)，Key Tag可以和后面的签名者字段(example.com.)共同确定究竟使用哪个公钥来验证签名。

5.DS记录

DS(Delegat ion Signer)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。DS记录存储在上级域名服务器(Delegation)中，比如example.com的DS RR存储在.com的区中。

dns.example.com. 86400 IN DS 60485 5 1 (  
　　 2BB183AF5F22588179A53B0A  
 　　98631FAD1A292118 )

DS 之后的字段依次是密钥标签(Key Tag)、算法和散列算法(1代表 SHA-1)。后面括号内的内容是dns.example.com.密钥SHA-1计算结果的16进制表示。

　　6.NSEC记录

　　NSEC记录是为了应答那些不存在的资源记录而设计的。为了保证私有密钥的安全性和服务器的性能，所有的签名记录都是事先(甚至离线)生成的。服务器显然不能为所有不存在的记录事先生成一个公共的“不存在”的签名记录，因为这一记录可以被重放(Replay)；更不可能为每一个不存在的记录生成独立的签名，因为它不知道用户将会请求怎样的记录。

　在区数据签名时，NSEC记录会自动生成。