基于真实 IPv6地址环境下的安全 DNS系统设计

谢 锐, 顾一众, 汪为农
(上海交通大学网络信息中心, 上海 200030)

摘要:网络的安全保证变得日趋重要,在下一代互联网上这种要求更为迫切. 以真实 IPv6地址接入技术为平台,结合 PKI的证书分发机制对密钥的分发实现安全便捷的管理,利用密钥机制对 DNS全程数据通信进行签名加密保护进而可以实现下一代互联网络体系结构中 DNS系统的安全,包括安全的域名更新、安全的域名查询以及抵御常见的 DNS攻击.

关键词: IPv6; DNS;签名;加密; CNGI
中图分类号: TP 393 **文献标识码**: A **文章编号**: 0438-0479 (2007) S2-0029-03

下一代互联网意味着更大的规模、更广泛的应用、更快的速度、更加安全可信,其中安全性是下一代互联网最重要的标志之一. 相关的研究表明,从 IPv4过渡到 IPv6,网络安全问题并没有消除,只是发生了一些变化,必须从体系结构的角度研究下一代互联网安全的整体解决方案,中国下一代互联网络 CNGI的建设为研究这一体系结构和关键技术提供了机遇.

因此由清华大学牵头,联合国内 10余所重点高校与华为、比威两家网络设备厂商共同组成产、学、研一体化的高水平开发队伍,以中国下一代互联网示范工程 (CNGI)为基础平台,申请了《面向 IPv6的互联网安全体系结构和关键技术研究》的项目. 清华大学提出并实现的基于真实 IP地址的访问的技术大大提高了网络和信息的安全性,保证了在互联网内实现真实 IP源地址访问,即网络中每个分组携带的 IP源地址必须和发送数据源的真实 IP地址一致,将对互联网的安全和应用提供以下便利:可以杜绝基于伪造源地址的攻击;易于追踪网络和信息安全事件;简化身份认证;简化网络管理;支持基于 IP地址的网络计费;报文源地址的真实性.

为构建基于真实 IPv6地址访问的完整的安全体系结构,作为该项目合作单位之一的上海交通大学承担设计开发了支持真实 IP地址访问的 IPv6安全域名服务系统,为上层的各种应用提供统一的安全服务,为整个安全体系提供了安全服务中间件.

收稿日期: 2007-06-15
基金项目: CNGI示范工程 2005年研究开发、产业化及应用试验项目"面向 IPv6的互联网安全体系结构和关键技术研究"资助.
作者简介:谢锐,男,工程师.
Email: sh@sjtu.edu.cn

1 真实地址 IPv6环境下的安全 DNS系统总体框架

本系统以 RFC2535 (Domain Name System Security Extensions)和 RFC 2136 (Dynamic Updates in the Domain Name System)为研究基础,结合 PKI的证书分发机制对密钥的分发实现安全管理. 一方面利用密钥机制对 DNS全程通信进行保护,另一方面也利用 DNSSEC中的密钥技术对域名的解析和动态更新的完整性进行保证,进而实现整个 DNS系统的安全,包括安全的域名更新、安全的域名查询以及抵御常见的 DNS攻击 (域名劫持、缓存污染).

主要设计思路如下:

在网络中的任何用户/应用将对应唯一的一个域名;任何通信体之间的定位将以域名为依据;利用较为成熟的 PKI体系结构,完成对通信单元的证书的管理以及密钥对的发布;采用非对称加密算法对网络中 DNS的数据流进行加密,保证 DNS数据在网络传输中是安全的,不可被窜改;使用签名技术,保证 DNS数据来源是可信的,不可抵赖.

主要的功能模块包括:

- 证书用户 (包含 DNS的服务器和客户端)的证书及公钥安全更新/查询模块;
- 基于 PKI和 DNSSEC技术的 DNS客户端域名/IPv6地址安全注册/更新模块;
- 基于 PKI和 DNSSEC技术的 DNS客户端域名/IPv6地址安全查询模块;
- DNS Server之间的安全迭代查询模块.

图 1为系统总体设计结构图.

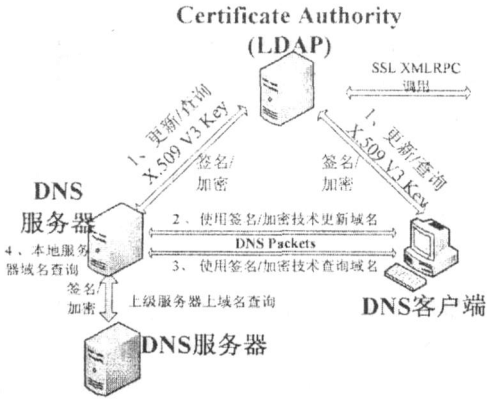

图 1 设计框架总图

通过 4个模块的设计来保证真实地址 IPv6环境下 DNS的通讯是足够安全可信的.

2 模块基本功能介绍

2.1 证书用户安全更新/查询 LDAP服务器上的公钥

整个系统中与通信相关的安全功能的实现都必须依赖存放在 CA-LADP系统中所提供的非对称密钥,因此应用系统通信双方在真正发起 IP通信之前,必须首先获得并存储自身的密钥对和对方的公钥.

所有的用户 (包含 CA-LDAP服务器)可在本地使用 openssl的 openssl-0.9.8d.tar.tar或 Win32OpenSSL-0_9_8d.exe中提供的密钥对生成函数来产生用于非对称加密算法的密钥对,并存储在本地以方便自身各种应用程序的调用.为了使各通信体间能够互相知道各自的域名和公钥,每个通信体应将自身的公钥和域名使用 CA-LDAP的公钥经过加密后安全地上传至 LDAP数据库,供他人查询.

作为信任链的起始点,CA-LDAP服务器的公钥应放在一个所有通信体都可以访问到的公共地方.

2.2 DNS客户端安全注册更新

为了构建可信的网络,在整个安全 DNS系统中,用户的域名将被用来作为标识该用户身份的唯一标志存在 (IP地址不再是身份的标识),要求每个用户必须将自己的 IP与个人的域名在 DNS系统中进行唯一定义.

一旦发现地址发生改变,客户应当立刻发起基于证书的安全的域名注册请求.在通讯过程将对 DNS数据流进行数字签名和加密,保证 DNS通信系统的可信性.

安全的域名注册过程如图 2所示.

DNS Clien端 (简称 DC,下同)发起注册的过程:

1) 用户在本地网络环境中,静态或动态获得当前 IPv6地址及所属地 Local DNS信息.

2) 用户通过 Local DNS以匿名递归查询的方式获得 Home DNS的 IP地址 (此过程也应当使用安全的 DNS查询).

3) 客户端软件使用新的线程向 Home DNS注册用户域名信息、用户新获得的 IPv6地址、资源记录类型以及其他辅助信息,如许可查询范围列表 {匿名,限制查询域和/或限制 ID列表}.详细如下:

- 从缓存中或 CA服务器中获得 Home DNS服务器的证书并做有效性验证 (图 1中 1所完成的工作);

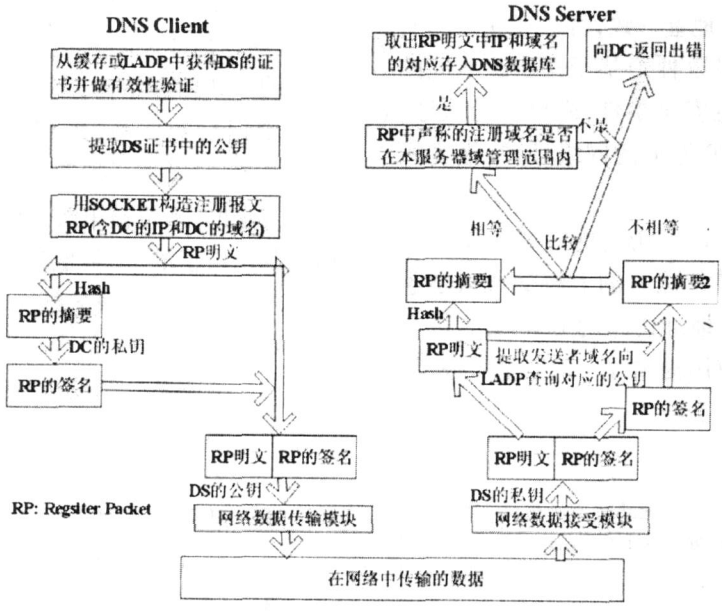

图 2 DNS客户端向服务器端注册域名及 IP地址的过程

- 从有效的证书中取出 Home DNS服务器的公钥;
- 通过 Socket编程构造含 DC域名与 IP地址的注册报文 (简称 RP,主要包含 UserName、RecordType、IPv6地址 /别名、TTL等 DNS资源记录必须的一些类型,这些格式需要与 DNS服务器端相一致);
- 通过特定的 Hash算法生成 RP的摘要,并对该摘要使用自身的私钥和非对称算法加密,产生签名;
- 将 RP和签名打包,然后通过 HomeDNS服务器的公钥进行非对称算法加密,形成注册请求的密文;
- 通过数据发送模块将该密文发往 DNS服务器.

4)等待 DNS Server端发回认可或拒绝回应报文,如果返回正确报文,则结束注册过程,否则尝试重新注册请求过程.

DNS Server端 (简称 DS,下同)处理注册的过程:

1) DS通过其数据接受模块收到 DC发来的注册请求密文;

2) DS使用自己的私钥打开次密文,分离出注册请求的明文 RP和签名;

3) DS从明文中提取域名信息,并以此信息为根据查询 CA的 LDAP服务器 (图 1中 1所完成的工作),获得该域名所对应的公钥;同时对该明文运用和客户端一致的 hash算法计算出 RP的摘要,记为 RPD1;

4) 使用该公钥将 RP的签名打开,得出 RP的摘要,记为 RPD2;

5) 比较 RPD1与 RPD2的值;如果两者不等,通过签名 /加密的方法直接返回出错信息给 DC,结束;

6) 如果相等,则判断 RP中所声称的域名是否在本服务器的域管理范围内;

7) 如果属于本管理范围,服务器在对 RP明文中的域名注册请求信息如 {用户域名,用户 IP,许可列表和其他属性信息 }做出必要的检查,如果符合 DNS系统的规范,则存入本地数据库,如判断列表长度是否超过管理规定 (超长列表可能过渡消耗服务器资源);否则通过签名 /加密的方法直接返回出错信息给 DC,结束;

8) 将域名 /IPv6地址 /资源类型填入 DNS的 LDAP数据库.

通过上述通信过程,可以保证:

- 通过签名,注册请求的内容确实是该域名所有者发出的;伪造的域名注册信息到达 DNS服务器端后,服务器由于无法获得匹配的公钥,根本就无法验证签名,因而不会对伪造报文作出应答;
- 通过 DS公钥对数据的加密,由于其他任何主机不具备与该公钥相对应的私钥,即使报文被截获,也无法打开密文,所以可以在保证网络传输时通信过程是安全的.

2.3　DNS安全查询

对于 DNS安全查询,系统设计时将考虑两个方面的情况:

- 客户端与 DNS服务器之间的安全查询;
- 服务器与上级服务器之间的递归查询;

(1)客户端安全查询模块

在本系统中,我们更多的是考虑 DNS数据在互连网传输中的安全性,因此我们对于客户端本地的域名缓存信息将不予考虑.即每当应用程序按照域名访问的时候,都会触发一个 DNS域名查询过程的产生.

DNS Clien端发起安全查询的过程:

1) DC软件侦听域名解析请求 (如 WWW访问);

2) 查询本地证书缓存或远端 CA-LDAP服务器以便获得自身的密钥对以及 Local DNS Server的公钥;

3) 构造查询报文 (含自身的域名,被查询者的域名、资源记录类型),记为 QP;

4) 使用特定的 hash算法生产 QP的摘要;并用自己的私钥使用 RSA算法生成签名;将查询报文和签名合并,并用 DS的公钥进行加密,生成密文;

5) 将密文发出,到 DS的 UDP53端口,等待服务器返回的结果;

6) 如果服务器返回的是对应的 IP地址,则查询结束,如果返回的是上一级 DNS服务器的地址,则继续构造查询报文,进入循环步骤 3).下图 3为具体的报文构造过程:

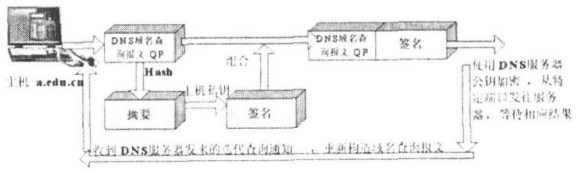

图 3　客户端域名查询报文构造过程

DNS Server端对安全查询的响应过程:

1) 服务器端将侦听在 53端口上;

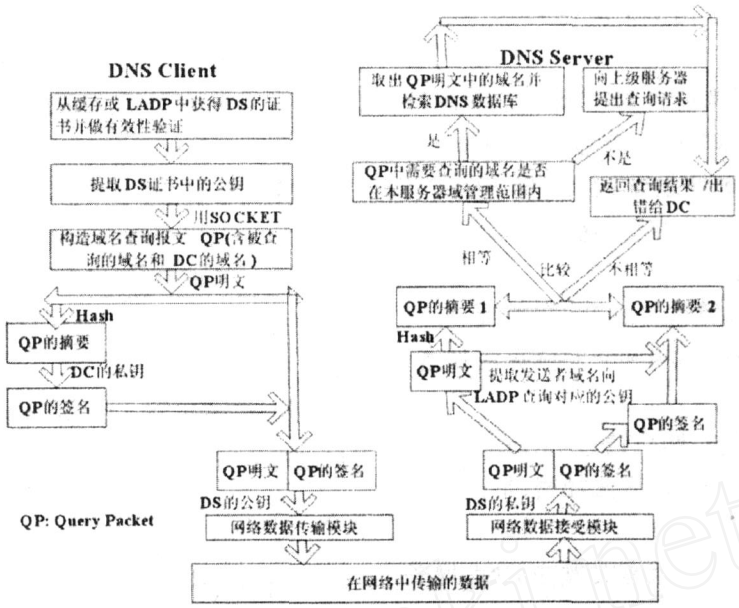

图 4 NDS客房端向服务器端查询域名对应 IP地址的过程

2) 收到密文后;使用自己的私钥将密文解开;

3) 识别出 QP明文和 QP的签名;从 QP明文中取出发出查询请求者的域名,以此为根据查询本地缓存或 CA-LDAP获得其公钥;同时对 QP明文用相应的 hash算法生产摘要记为 QPD1;使用查询到的公钥对 QP的签名进行 RSA非对称算法生成 QPD2;

4) 比较 QPD1与 QPD2是否相等;如果不相等,返回错误结果给查询者,结束;

5) 如果相等,则检查被查询的域名是否在本服务器的域管理范围之内;

6) 如果是,则利用域名查询 IPv6地址,并返回结果给查询者,结束;如果不是,则向上级服务器提出安全的查询请求;并等待上级服务器返回查询结果;

具体的流程图见图 4.

(2)服务器之间的递归查询请求

在系统的具体设计中,目前支持服务器之间的递归查询.

当前服务器所做的操作如下:

1) 服务器根据域名查询对应的根服务器,获得相应的根服务器域名 / Ipv6地址;

2) 服务器查询该服务器所对应的公钥,如果没有查询到,则结束循环;如果有则

3) 根据域名使用签名 加密查询该服务器上的次级域名服务器的 IPv6地址,

4) 如果当前查询到的域名服务器是所要查询域名的域服务器,则进行直接域名 / IPv6对应关系的查询,跳出循环;否则转 3);

5) 使用签名 加密查询向客户端的查询者返回最终的查询信息;

如果收到的是服务器发来的递归请求则,上级服务器所做的操作如下:

1) 收到下级服务器发来的查询请求密文;

2) 查询下级服务器的公钥;

3) 解开密文,获得签名和原文,如果正确;

4) 直接查询 DNS-LDAP,并将查询结果返回给上级服务器.

图 5为具体的报文构造过程:

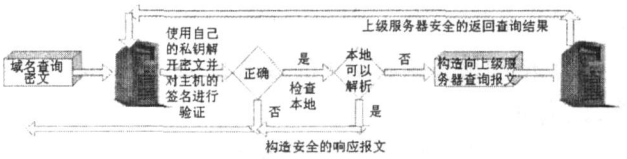

图 5 服务器域名迭代查询报文构造过程

3 系统的实际部署

我们将上述系统部署在 CERNET2基于 IPv6源地址的网络内,如图 6所示拓扑.

使得在整个域内的用户可以实现:

- 查询信息的可信与加密:服务器可以通过 PKI技术,利用服务器证书对信息加数字签名,也可以配合客户端证书对查询信息作加密,确保信息确实由服务器签发且只能由指定客户察看.
- 该功能保证服务不被中间人攻击:服务器使用自己的数字证书,对于客户端请求安全的

查询做数字签名,客户端通过验证该签名即可得知报文是否完整的由指定服务器签发.

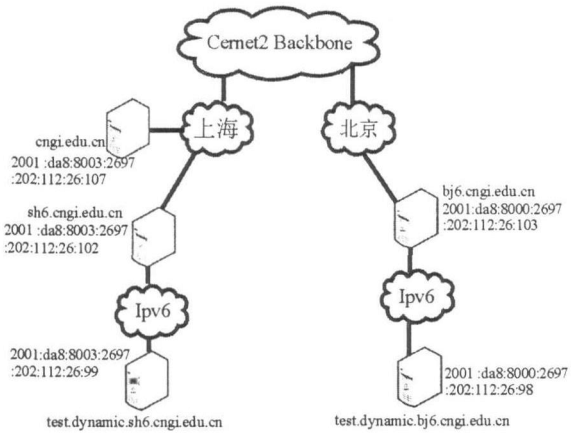

图 6　基于真实 IPv6地址访问的域名服务系统拓扑图

通过实际部署大大提高了真实 IPv6地址情况下域名访问的安全性,为整个《面向 IPv6的互联网安全体系结构和关键技术研究》的安全体系提供了安全服务中间件.

参考文献:

[1] http://www.cisco.com/.

[2] Andew S Tanenbaum. 计算机网络 [M]. 熊桂喜,王小虎,译. 北京: 清华大学出版社, 2002.

[3] 伍海桑,陈茂科,陈名华,等. IPv6原理与实践 [M]. 北京: 人民邮电出版社, 2000.

[4] Sam Brown, Brian Browne, Neal Chen. Configuring IPv6 for Cisco IOS [M]. 北京: 电子工业出版社, 2003.

[5] Eastlake D. RFC2535 Domain Name System Security Extensions [S]. IETF, 1999.

[6] Vixie P, Thomson S. Dynamic Updates in the Domain Name System [S]. IETF, 1997.

Design of a Secure DNS System Based on Real IPv6 Address Network

XIE Rui, GU Yi-zhong, WANG Wei-nong

(Network Information Center, Shanghai Jiaotong University, Shanghai 200030, China)

Abstract: Network security guarantee has become increasingly important in the next generation Internet, such a request is more urgent than ever. Based on real IPv6 accessing technology, integrating with the PKI certificate distribution mechanism to achieve safe and convenient management on key distribution mechanism and using key mechanism to signature and encrypt the entire DNS data communications can protect the security of Next Generation DNS system, including the security of the domain name updates, security of domain lookup and withstanding common DNS attacks.

Key words: IPv6; Domain Name System; signature; encryption; China Next Generation Internet Project