ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.2, February 2009, pp.363−374
doi: 10.3724/SP.J.1001.2009.03389

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

互联网命名问题研究*

曹 锐+, 吴建平, 徐明伟

(清华大学 计算机科学与技术系,北京 100084)

Research on Internet Naming

CAO Rui+, WU Jian-Ping, XU Ming-Wei

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

+ Corresponding author: E-mail: mirake@csnet1.cs.tsinghua.edu.cn

Cao R, Wu JP, Xu MW. Research on Internet naming. *Journal of Software*, 2009,20(2):363−374.
http://www.jos.org.cn/1000-9825/3389.htm

Abstract: In this paper, current research issues and the problems of Internet naming are discussed. The existing namespace and key techniques in this field are categorized and introduced. At the end of the paper, the key ideas in research of naming and the possible research trends in the future are discussed.
Key words: naming; namespace; identifier; identity authentication; resolution system

摘 要: 分析了互联网命名问题的研究内容以及当前存在的问题,对命名空间和主要技术的现状进行了分类和介绍.讨论了命名问题研究中的重要思想,以及未来命名问题研究可能的发展方向.
关键词: 命名;命名空间;身份标识;身份认证;解析系统
中图法分类号: TP393 **文献标识码**: A

互联网命名是用一种符号对互联网中的用户、设备、服务或数据进行标识.例如,人们用 E-mail 地址来表示一个用户;用 IP 地址或域名来表示一台网络终端设备;用 URL 表示一个 Web 服务或一个页面.正是因为有了这些符号,人们才可以定位并访问它们.

目前互联网比较常见的命名有 IP 地址、域名、E-mail 地址、URL 等,它们分别标识主机、用户以及 Web 资源.这些标识的出现对于推动互联网的发展曾经起到过积极的作用,但它们也都存在着各自的问题和新的需求.IP 地址既作为端系统的位置标识,又同时充当了它的身份标识.这种 IP 地址过载随着大量移动终端的出现,使得解决移动环境下的访问和互联变得更加困难.基于域名的 E-mail 地址以及字符形式的用户名在 Web 应用中需要解决“一次登录(single sign-on,简称 SSO)”的问题;基于域名格式的 URL 同样无法解决 Web 数据移动后的访问.因此,有关命名方面的研究越来越多,大量新的命名空间和相关的命名技术被提出来.

本文第 1 节对命名问题的概念、研究内容进行阐述.当前主要的命名问题研究成果将在第 2 节介绍.第 3

* Supported by the National Natural Science Foundation of China under Grant Nos.60373010, 90604024 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.2007AA01Z2A2, 2006AA01Z209 (国家高技术研究发展计划(863)); the Foundation for Key Program of the Ministry of Education of Chin under Grant No.106012 (教育部科学技术研究重点项目)

Received 2008-03-28; Accepted 2008-05-14

节对命名问题研究中的一些重要思想进行分析.第 4 节对命名问题研究进行总结,并对未来发展方向进行展望.

1 命名问题的研究内容

命名(naming)就是给互联网的用户、设备、服务和数据(以下统称“网络实体”)分配一个可以代表其身份(identity)的抽象符号,这个符号就是身份标识(identifier,简称 id),对同一类实体分配的身份标识的集合构成了这类实体的命名空间(namespace).命名问题是与命名空间有关的一切问题,包括命名空间中身份标识的定义以及相关的其他技术.

1.1 身份标识的定义

网络实体根据类型的不同主要分成 4 类:用户、设备、服务和数据.用户是指参与互联网活动的人,可以是一个自然人也可以是一群人的集合;设备是发送和接收报文的装置,可以是 PC 机、手机、打印机甚至是未来的智能家电等其他一切可能的电子设备;服务是由网络设备提供的一种功能的抽象,如 WWW 服务、FTP 服务、共享打印服务等,通常由一个规范来描述;数据是信息的具体表现,可以是一个词汇、一个网页甚至是一个超链接等.对于这 4 类不同的实体,命名空间的研究内容和思路也不相同.

1.1.1 用户标识

网络应用程序的最终使用者是用户,所以用户标识通常使用在应用程序中,通常采用简单的字符串或 E-mail 地址.由简单字符串构成的命名空间只在一个应用程序内使用,不能在其他应用程序中使用.而 E-mail 地址构成的命名空间则是全球范围的,可以被任何应用程序使用.

用户身份标识的定义主要遵循两个基本原则:简单和易用.简单是指它的结构简单,而且标识的字符数不会太长.易用包括容易记忆和容易书写,这也正是为什么大多数的用户标识采用字符串的一个原因.

1.1.2 设备标识

网络报文的发送和接收实体都是网络设备,在网络通信活动中起着重要的作用,所以与它有关的研究内容有很多.设备标识的定义主要为了满足以下几个需求:

1. 解决 IP 地址语义过载问题.传统的用 IP 地址作为主机身份的方法不能为移动终端和多宿主主机提供一个稳定的命名,于是如何提出新的命名是网络设备命名的众多研究内容中最先被提出来的,也是最为迫切的需求.这类标识定义的一个特点是引入独立的主机身份的概念,从而将主机标识的语义从 IP 地址中分离出来.
2. 与网络中间件有关的设备标识.网络中间件(如 NAT、代理)的出现,打破了传统的端到端的通信模式,使得端到端的命名和寻址机制也被打破,特别是 NAT 的出现破坏了主机间端到端的访问,扩展现有的主机身份技术是解决网络中间件所带来的问题的一种方法.
3. 异构网络设备的互联.随着三网合一的发展以及新的智能终端的出现,像电视机、电话和 PC 这样本来属于不同类型网络的设备需要互联.由于这些设备各自有不同的设备标识,因而在它们互联的时候,需要对已有的身份标识进行扩展.因而研究如何扩展现有的身份标识,使这些异构网络的设备能够互联,也是一个重要的研究内容.

1.1.3 服务标识

传统的网络服务种类较少,而且大多有统一的标准,对一台主机提供的网络服务的端口进行详细的描述,如提供 SMTP,WWW,FTP 等服务的主机标识加上端口就成为这些服务的标识.但是,随着互联网的发展和各类不同应用的出现,提供更加灵活的服务成为人们的需求,因此,如何描述并使用这些灵活的自定义的服务成为一项研究内容.传统的基于 URL 的服务标识不能满足服务移动、组播任意播等需求,因此 URN 和 URI 等与位置无关的身份标识成为服务标识的一个发展方向.

1.1.4 数据标识

传统的互联网数据交换是以报文为单位的,但人们关心得更多的是所需要的信息.根据数据类型的不同,所赋予的身份标识也具有不同的特点.总的来说,数据标识可以从以下 3 个角度来定义:

(1) 基于报文的数据标识.报文仅仅在网络传输中才有意义,因此少数关注这个层面的体系结构(如 I3)会给报文分配标识,以实现一些特殊的功能.

(2) 基于地址的数据标识.也就是根据数据所在的位置分配一个 ID,应用程序通过引用这个标识来得到数据的位置,从而进一步获取其内容,如 URL.

(3) 位置无关的数据标识.以地址来标识数据存在很大的问题,当数据移动或进行备份以后,基于地址的标识不能完全反映数据的最新状态.因此,给数据分配一个与地址无关的数据标识的方法成为当前的一个重要内容.

1.2 命名相关技术的研究内容

与命名空间有关的技术主要包括认证技术和解析技术.认证技术解决网络实体身份标识的真实性验证问题,解析系统的作用是根据网络实体的身份标识获得其内容或一些属性信息(如位置等).

1.2.1 认证技术

在认证技术中使用最多的就是应用程序对用户身份的认证.传统的用户身份标识的认证技术主要基于用户名和口令,但它存在两个问题:一个是不同应用程序之间互相访问时,由于身份的不统一以及认证的独立性,无法保证对方身份的真实性.如 E-mail,其发送者和接受者由各自的应用程序认证,而应用程序之间需要有一种可以保证 E-mail 的发送者身份真实性的机制.另一个是一次登录(SSO)问题.由于目前人们在访问不同的网络应用时经常需要进行很多次登录,既浪费时间又需要记忆不同的用户名和密码.如果让各个应用都能共享用户一次登录的信息从而减少登录次数,那么对用户体验来说将会是一大改善.SSO 是当前用户命名问题的研究热点,也是未来的一个发展趋势.

近几年来,随着人们对主机身份的认识,也出现了针对端系统主机身份的认证技术.在主机身份认证技术中,其研究的重点是报文的接受者如何确定报文的发送者身份是否真实.主要有两类:一类是真实 IP 地址的认证技术,另一类是基于主机身份的认证技术.随着近年来大量出现的新的设备身份标识,针对它们的认证技术会成为一个非常活跃的研究领域.

在服务和数据标识方面,也有相应的认证技术,但目前它们主要是针对互联网中的“网上钓鱼”攻击,因此一般也称作“反钓鱼技术”.反钓鱼技术的研究内容是如何保证用户浏览的网页不是通过 URL 伪造或 DNS 攻击转向的其他页面.反钓鱼技术一般都是通过第三方授权的数字证书来实现.

1.2.2 解析系统

一个命名空间必然有一个解析系统,但是很多命名空间的身份标识具有一些相似性,使得一个解析系统可以为多个命名空间所用.解析系统所关注的研究内容主要有:

(1) 标识规范.一个解析系统如果为一种命名空间提供解析服务,那么这个命名空间的身份标识必须符合解析系统的标识规范,否则解析系统无法工作.例如,ENUM 的标识格式符合 DNS 的层次化字符格式,因而可以使用 DNS 作为解析系统.

(2) 解析和更新的性能.对一个身份标识的解析过程以及更新过程所需要的延迟是解析系统的一项重要指标,延迟越小,性能越高.不同性能的解析系统应用于不同的场合.例如,DNS 的解析性能大约在 1s 以内,对于一般的 Web 应用就足够了.但当考虑在移动环境中使用时,由于对实时性的要求较高,DNS 的解析性能就无法满足它们的要求,因而在 Mobile IP 或 HIP 这些协议中都引入了其他机制,以提高身份标识与 IP 地址匹配关系的解析和更新.

(3) 健壮性和负载均衡特性.由于解析系统对身份标识的使用起着重要的作用,因而其健壮性也是非常重要的.当前网络中的大多数解析系统都是分布式系统,可以避免因为一台服务器的故障而造成整个服务的瘫痪,但有时却会影响一部分标识的解析.另外,当某个解析服务器负载过大时,解析系统能否有效地将这些负载分摊给其他服务器也是解析系统需要研究的问题.

(4) 安全性.解析系统的解析结果应当保证不被第三方篡改或窃取,对于某些机密的数据也应当只有被授权的用户才能解析,而且在更新身份属性的过程中,只有那些有权限的访问者才能修改存储的数据,这些都是解

析系统安全性的表现.目前,大多数系统都能保证更新的安全性,而解析的安全性是研究的重点.

2 命名问题的研究现状

当前互联网中存在各种各样的命名空间,其身份标识、认证技术和解析系统在具有相同点的同时也都有其各自的特点.本节将分别介绍目前互联网中比较常见的身份标识以及相关技术.

2.1 常见的身份标识

2.1.1 用户标识

目前大多数网站采用 3 种形式的用户标识:用户自选的字符串、随机生成的数字串和 E-mail 地址.用户自选的字符串简单,但是只能在一个应用程序内使用,不同的应用之间用户名可能会有重复.以数字串作为用户身份标识也被很多应用程序使用,如微软的 Passport 虽然采用 E-mail 作为可公开的用户名,但实际上该名字对应一个 64 比特长的整数,它才是用户真正的 ID.像 QQ 这类即时通信软件以及部分网站也有很多采用一个随机整数作为用户唯一稳定的身份标识.E-mail 地址的格式是 name@domain,它是一种复合结构,domain 代表 E-mail 服务的命名空间,它是一个 URL.字符串 name 则是用户在这个命名空间中的唯一标识,两者结合起来就是用户的全球唯一身份标识.

E-mail 地址作为用户身份标识相对于数字串来说具有两个优点:首先是便于用户记忆;其次,通过发送 E-mail 可以对用户进行初步的身份认证(如发一封激活信件,由用户激活).所以,我们认为 E-mail 地址会成为未来应用程序首选的用户身份标识.

为了解决漫游和移动环境中的用户注册问题,引入了一种用户身份标识,被称作网络接入标识(network access identifier,简称 NAI)[1].其格式是一个简单的 username 或 realm,也可以是 username@realm.支持 NAI 的设备至少支持长度为 72 字节的 NAI,RFC 建议的是 253 字节.NAI 主要用在移动和漫游环境中用户接入认证的时候.

2.1.2 设备标识

当前对于网络设备标识的研究较多,根据各自用途的不同,我们分别介绍每种用途的设备标识.

(1) 移动和多宿主设备的标识

IP[2]地址是最早使用的主机身份标识,它本身也是主机位置的标识.IP 地址采用了 32 比特的二进制串格式,层次化的结构使得 IP 地址具有汇聚的特性.但是,由于 IP 地址充当了两种不同的身份(IP 地址的过载),其在移动、漫游和多宿主环境中的使用受到限制.IPv6 地址[3]是 IPv6 网络中的地址和身份标识,有 128 比特.在 IPv6 的配置中,使用的是称为 EUI-64[4]格式的扩展标识符.EUI-64 是 IEEE 定义的一种基于 64 比特的扩展唯一标识符.EUI-64 通过链路层地址生成接口 ID,从而保证了接口 ID 的唯一性,也保证了生成地址的唯一性.

FQDN(fully qualified domain name,完全合格域名)[5,6]也就是我们通常说的域名,是我们目前最熟悉、使用最多的主机身份标识.它是具有层次化结构的字符类型,便于用户记忆,且与设备位置不相关.它在全球范围内唯一,因而被广泛应用于网络应用中,并且很多其他身份标识也都是从 FQDN 扩展而来.

HIP[7−10]采用公钥-私钥对中的公钥作为主机身份(host identity,简称 HI).HIT 是 HI 的一个 128 位哈希值,在报文中携带.TCP 协议[11]不再用 IP 地址绑定 TCP 连接,而是用 HIT 绑定.这种结构可以很容易地解决移动和多宿主的问题[12],还可以解决 v4-v6 互连问题[13].由于引入了密钥机制,HIP 还可以为端系统身份的真实性提供认证手段.HIP 中的主机身份是一个全局唯一标识符,但是由于它的身份与密钥有关,因此并不稳定.由于 HI 是公钥,不便于记忆,因此在实际使用中还要配合域名一起使用.类似于 HIP 这样的保留 IP 地址作位置标识而定义新的主机标识的研究还有 SING[14],ONHS[15],SFN[16].

Shim6[17]与 HIP 类似,也是在网络层之上传输层之下插入一个 Multi6 Sub Layer 的独立层.不同的是,Shim6 采用会话初始的 IPv6 地址作为主机身份标识(identity),当前使用的 IPv6 地址集合作为位置标识(locaters).其优点是对上层应用程序无须作改动,但是由于它采用了 IPv6 地址作为标识,它只是在会话周期内是唯一稳定的.像这样采用初始 IP 地址作为主机身份标识的研究还有 MAST[18].

GSE[19]也采用了分离 IP 双重身份的方法,但是与 HIP 和 Shim6 都不同.它没有在协议栈中引入新的层次,而是将 128 位的 IPv6 地址分成两个部分,前 64 比特作为路由使用的位置标识(routing goop,简称 RG),后 64 位作为端系统的主机身份标识(end-system designator,简称 ESD).与之类似的研究还有 LIN6[20,21].

GUID(global unique identifier,全局唯一标识符)[22]是微软使用的一个标识,是由主机网卡的标识以及 CPU 时钟的唯一数字生成的一个 128 比特的二进制数字.例如,6F9619FF-8B86-D011-B42D-00C04FC964FF 即为有效的 GUID 值,世界上的任意两台计算机都不会生成重复的 GUID 值.GUID 主要用于在拥有多个节点、多台计算机的网络或系统中,分配必须具有唯一性的标识符,也可以作为 P2P 应用中的主机身份标识,微软的产品广泛使用了 GUID,用于识别接口、复制品、记录以及其他对象.如 Office Groove 2007 中,就使用 GUID 作为 P2P 通信时主机的身份标识.

(2) 网络中间件有关的设备标识

IPNL(for IP next layer)[23]是为解决 NAT 穿越问题而提出的主机身份,它在 IP 层之上传输层之下引入新的一层,从而实现公有、私有网络的互联,同时简化了 NAT 网关的信息维护.IPNL 的主要原理是:会话发起方将接收方的域名和共有地址以及自己的域名和私有地址填写在 IP 扩展头中,发起方的 NAT 网关转发报文时填写发起方的共有地址,而当报文到达接收方的 NAT 网关时,网关根据域名查询到目的主机的私有地址,从而进行私有网络的路由.所以,事实上 IPNL 的主机身份是一个集合,包括主机的域名、NAT 的外部 IP 地址以及主机的私有 IP 地址.类似的研究还有 TRIAD[24]协议,它是使用 FQDN 作为主机身份的.

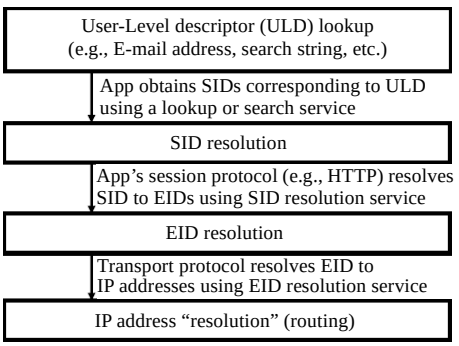

Fig.1 Architecture of LNAI

图 1 LNAI 体系结构

LNAI(layered naming architecture for the Internet)[25]提出了抽象的独立分组命名模型(如图 1 所示),每一层都提出一个独立的标识,彼此之间可以动态关联,它们分别是:应用程序标识,如 E-mail 地址等、服务标识(service identifier,简称 SID)、端系统标识(endpoint identifier,简称 EID)、路由标识(IP 地址).每相邻两层的命名都可以通过解析来获得它们的对应关系.LNAI 引入了重定向的功能,不但可以应用在移动和多宿主环境下,而且还能支持网络中间件,如 NAT、防火墙等.

(3) 不同类型设备互联的标识

在不同类型的设备互联研究中,SIP 和 ENUM 是比较典型的两种技术,SIP 采用域名作为设备的身份标识,而 ENUM 采用了一种新的与域名兼容的格式作为终端的身份标识.

SIP(session initiation protocol,会话初始化协议)[26]是一种基于文本的应用层控制协议,可用来创建、修改或终止多媒体会话,如因特网电话呼叫.在 SIP 协议中,端系统使用类似 E-mail 地址作为身份标识,其格式为 sip:userID@gateway.com,SIP 终端将自己的地址信息在本地区的注册服务器上进行注册.当呼叫时,SIP 终端可以通过 Proxy Server 或 Redirect Server 获得被呼叫终端的 IP 地址,从而建立会话.

ENUM(telephone number mapping,电话号码映射)[27]采用符合 E.164 标准的电话号码作为终端的身份标识,通过 DNS 的解析完成定位.例如电话号码"+86-10-66023626"将会被翻译成"6.2.6.3.2.0.6.6.0.1.6.8.e164.arpa"保存在 DNS 的资源记录中,记录中还可以保存该终端的不同通信方式(如 E-mail,SIP)的地址,这样,用户只需通过 DNS 解析这个电话号码就能访问到这台终端或者它能够使用的所有网络服务的地址.

UIA(user information architecture)[28]提出了一种未来不同电子设备之间的互联体系结构.它要求不同类型的电子设备终端自己指定一个"公钥-私钥"对,并将公钥的哈希值作为该设备的标识(endpoint identifier).可以使用类似域名的表示形式,如 Phone.Bob,iPod.Alice 等.UIA 通过统一的命名空间使得不同类型的电子设备可以直接点对点(peer-to-peer)地传输数据,而不再需要以电脑作为中转站,建立了一个应用层的逻辑上的不同类型设备信息交互平台.

2.1.3 服务标识

目前,互联网广泛使用的服务标识是基于 URL,URN 和 URI 的,它们本身也都是数据标识.

URL(统一资源定位符(uniform resource locator))[29]是 Internet 上用来描述信息资源的字符串,主要用于各种 Web 应用中,可以用一种统一的格式来描述各种信息资源,包括服务、文件、服务器地址等.URL 的格式由 3 部分组成:第 1 部分是协议(或称为服务方式);第 2 部分是存有该资源的主机 IP 地址或域名(有时也包括端口号);第 3 部分是主机资源的具体地址(如路径和文件名).例如,http://www.sina.com.cn/就表示了新浪网提供的 Web 服务,我们通过它来访问这个服务.URL 最大的缺点是与被标识资源的位置有关,因而当信息资源的存放地点发生变化时,必须对 URL 作相应的改变.

URN(统一资源名(uniform resource name))[30]提出了对互联网资源的统一命名方案.URN 的格式为“urn:⟨NID⟩:⟨NSS⟩”.其中,⟨NID⟩表示命名空间标识,⟨NSS⟩表示命名空间中的特定标识.URN 与资源所处的位置无关,使用时,URN 会先解析成与位置相关的域名,然后再定位.

URI(通用资源标识符(uniform resource indicator))[31]是以某种统一的(标准化的)方式标识资源的简单字符串.事实上,URL 和 URN 是 URI 的一个子集.语法是[scheme:]scheme-specific-part.scheme 代表资源类型,例如“http”,“mailto”等.scheme-specific-part 的语法和语义由 URI 的命名空间决定.URI 有绝对和相对之分.

```
[city = Washington [building = whitehouse
                    [wing = west
                    [room =oval-office]]]]
[service = camera   [data-type = picture
                        [format = jpg]]
                    [resolution = 640×480]]
[accessibility = public]
```

Fig.2 Service identifier in INS

图 2 INS 中的服务标识

INS(intentional naming system)[32]提供了一种用户访问移动服务的资源发现和服务定位系统.它可以描述服务也可以描述数据.它采用“属性-值”作为服务或数据的标识,称为 Name-Specifiers,如图 2 所示.Name-Specifiers 被 INR(intentional name resolver)解析.它可以跟踪资源位置的变化,支持移动,还可以实现任意播和组播等服务的发现.

2.1.4 数据标识

(1) 基于报文的数据标识

I3(Internet indirection infrastructure)[33]是一种建立在 IP 网络上的应用层报文转发体系结构.它将报文收发的过程分成两个步骤,通过给报文一个 id 标识来完成匹配,可以很好地支持移动、组播等各种环境和应用.I3 中的每个报文都被赋予一个 m 比特长的二进制数字,在文献[33]中,m 是 256.接收端为了接收报文需要向 I3 网络中插入 Trigger,Tigger 中包含一个 trigger 标识和自己的 IP 地址.I3 规定了 Trigger 中的标识 id_t 和报文标识 id 的匹配规则:如果有至少前 k 个比特可以匹配,且不存在比 id_t 具有更多前缀匹配的标识,则 id_t 匹配 id 成功.I3 的转发机制会将报文转发给可以匹配的 trigger 中的主机.I3 还可以与 HIP 结合成 Hi3[34],在 I3 的基础上支持主机身份的认证.Secure-I3[35]在 I3 的基础上提供了更好的安全性.

(2) 基于地址的数据标识

这类标识目前通常采用前面已经介绍的 URL,这里不再赘述.

(3) 位置无关的数据标识

位置无关的数据标识用来表示不同的数据,标识与数据所在的位置无关,只反映了数据本身的身份.除了前面介绍的 URN,URI 以外,还有 PURL,URC,DONA 以及 Handle.此外,XML 系列中 XPath 和 XPointer 的数据标识不仅与位置无关,而且还能反映数据内容的特征.

PURL(persistent uniform resource locator)[36]对 URL 进行了改进.PURL 看上去和 URL 是一样的,但它并不指向数据的实际位置,而是一个 PURL Server,PURL Server 中保存了当前数据资源的实际位置.因此,只要 PURL Server 的位置不发生变化,用户就可以用 PURL 作为数据资源的稳定标识.

URC(统一资源引用符(uniform resource citation))[37]是一个还在讨论的新命名,它是描述对象的一些“属性/值”的集合,提供了资源对象的一些“元信息”.URC 基本上被认为是一个字符串,但也可以被设计成其他格式.URC 可以支持对一个资源的多个拷贝的标识.

Handle[38]是 Handle System 中定义的数据标识,其格式为“权威域/本地名”.权威域(handle naming authority)要求注册申请,且它是全球唯一的.权威域可以分层次,在书写规则上,权威域类似于 URL,但是它的顺序不同,如 loc.ndlp 中,loc 是父亲域,ndlp 是子域.本地名(handle local name)由用户自己选择.Handle 可以作为一个数据的全球唯一身份标识,且与数据的位置无关.

DONA(data-oriented network architecture)[39]采用了一种扁平结构且能够自认证的名字格式.它的命名基本单位称为 principal,可以是一个网站或网页,也可以是网页里的一张图片等,并与一个“公钥-私钥对”关联.DONA 中标识的格式为 *P*:*L*,其中,*P* 是这个 principal 的公钥的哈希值,*L* 是由 principal 自己选择的全球唯一标签.DONA 的优点在于其标识与应用无关、与位置无关且全球唯一.而且标识自认证的特点使得能够判断数据是否被篡改,可以保证数据的完整性.

XML(extensible markup language)[40]近些年来得到了广泛的应用.它是一种严格规范的标记语言.XML 文档中的标记集合可以构成一个命名空间(NameSpace),由 Schema 或 DTD 进行类型定义.通过指定文档的 URI 或 URL 可以获取一个 XML 文档的命名空间.如 xmlns:n1=“http://www.domain1.com”xmlns:n2=“http://www.domain2.com”定义了 n1 和 n2 两个命名空间,因此,⟨n1:node⟩和⟨n2:node⟩就是两个不同的节点.XML 文档的节点可以用它的命名空间的 URI 加上该节点的 XPath 作为唯一的身份标识.

XPath[41]是基于 XML 文档的一条路径,如/main/node/subnode.XPath 的每两层之间由“/”分割开的部分称作一个定位步长,其格式是“轴::节点检测[谓词]”.如“child::para[position()=1]”表示当前节点的子节点中第一个名字叫 para 的节点.XPath 代表了 XML 文档中的节点路径,但由于谓词的存在,XPath 也反映了文档内容,因此是基于内容的数据标识.XPointer[42]是 XPath 的扩展,并能够在 URI 中使用,用来标识全球任何一个 XML 文档中的任何片段,从而成为文档数据片段的标识.如 http://www.foo.org/bar.xml#xpointer(article/section [text()=“abc”])”就标识了在 www.foo.org 上的 bar.xml 文档中 article 根节点下内容为“abc”的 selection 子节点,可见它具有描述数据内容的能力.

2.2 命名相关技术的研究现状

2.2.1 身份认证技术

用户标识的认证通常采用的是用户自己选择用户名和口令的方式.这种方法相对简单,容易在一个网站内维护用户身份的信息,因此身份真实性的认证结果也只是在网站内部有效.

不同应用程序之间的用户身份认证主要是在 E-mail 服务中验证源用户身份的真实性.主要包括 Sender ID[43]和 DKIM[44]两种技术.Sender ID 技术是微软整合 SPF[45]和 Caller ID[46]提出的反垃圾邮件技术,其基本思想通过查询 DNS 的反向记录来发现邮件的源地址是否属于用户源身份所属的 E-mail 服务商的 IP 地址段.DKIM(domain keys identified mail)在使用 E-mail 地址作为用户身份的同时引入了密钥机制,通过查询 DNS 获得用户身份的密钥从而验证邮件中的签名是否正确.

一次登录问题的研究是与用户身份有关的命名问题研究的热点.微软的 Live ID[47]是其原有的.Net Passport[48]的改进,Live ID 服务是一个联合身份系统(federated identity system),它使用 E-mail 地址作为用户身份,通过各个联盟伙伴(federated partner)的协作完成 SSO 的身份认证.当用户访问联盟服务时,服务将用户重定向到用户身份提供商进行认证,从而获得正确的令牌,身份提供商在认证通过之后,把用户浏览器再重定向到服务商,服务商根据令牌来实现对用户的授权.除了微软的 Live ID 之外,类似的认证技术还有自由联盟的 Liberty Alliance[49]规范和 DIX[50]等.

在端系统身份真实性的研究中,前面介绍的 HIP 是一个代表,端系统在会话协商期间进行密钥的认证,由于 HIP 的主机身份本身也是公钥,因此公钥的认证过程也就是主机身份的认证过程.HIP 与 I3 结合后是 Hi3[34],它在 I3 网络中支持对端系统的身份认证.

目前大多数情况下,IP 地址仍然充当了端系统身份的角色.SAVA(基于真实 IPv6 源地址的网络寻址体系结构(IPv6 source address validation architecture))[51]设计和实现了一种包括接入第一跳、域内、域间 3 个层次的真实 IPv6 源地址网络寻址系统.在第一跳接入的层次中,SAVA 通过端系统的认证,建立端系统 IP 地址和接入交

换机端口的对应关系.当接入交换机接收到报文后,根据报文中的IP地址是否和交换机端口的匹配来判断IP地址是否伪造,从而保证了在互联网上转发的报文中携带的源IP地址都是真实的.

2.2.2 解析技术

本节将分两部分介绍当前解析系统的研究成果,第1部分主要介绍DNS系统以及针对DNS的改进技术,第2部分是其他解析系统.

• DNS及其改进技术

当前被广泛使用并最为大家所熟悉的大规模分布式解析系统就是DNS(domain name system)[5,6].DNS系统由域名服务器(name server)和解析器(resolver)构成.域名服务器采取层次化的结构相连,每一层的服务器都负责它所属域的域名存储和解析.DNS还引入Cache来缓存之前对域名的解析结果,以提高平均查询性能.DNS主要提供与FQDN格式兼容的身份标识的解析服务,因此很多身份标识如HIT,SIP,ENUM,ONHS等都能使用DNS为自己提供解析服务.

DNS在实际使用中还存在一些不足:系统可能出现单点故障和负载不均衡的情况,对于域名的解析和更新延迟也不能满足一些应用的需求,此外,DNS在安全性方面还不够好,对数据的完整性和机密性没有保证,容易被篡改或侦听.针对DNS的这些不足,提出了许多方案,大致可以分成以下4类:

1. 单独提高DNS的性能.例如,CoDNS[52]利用服务器故障一般比较集中的特点,在解析延迟超过一定阈值时向另一服务器重新发起解析请求.Renewal[53]在DNS中引入了主动更新的思想,根据域名的受欢迎程度来调整更新的主动性,提高了在域名超时被动访问时的效率.

2. 针对Web应用提高DNS的解析性能.由于当前DNS更多地用在对Web服务器的解析上,因此有一类研究主要利用Web服务的一些特点改进DNS.如SV机制[53]利用了服务器位置相对稳定的特点,DEW[54]和Active Name[55]在返回域名结果的同时也返回一些数据信息量较少的数据内容.而PRN[56]利用解析延迟主要是因查询远端服务器造成的这一特点,采用预测的方式提前获得接下来可能要查询的域名结果,从而避免查询远端服务器的延迟.

3. 提出新的体系结构.这类研究主要是引入P2P和DHT的思想引入,提出新的体系结构完成域名解析.由于DHT具有健壮性、负载均衡、主动更新的优点,也可以通过一些技术提高解析的性能,因此这类研究是目前解析系统研究的一大热点,如Active Name,SFR[57],PDNS[58],CoDoNS[59]等都将域名服务器构成了一个P2P的网络,通过这个网络完成域名定位.

4. 提高DNS的安全性.DNSSEC(DNS security extensions)[60,61]在普通DNS服务的基础上提供了两种功能:数据认证和事务交互认证功能.数据认证是保证解析器收到的应答中的资源记录是完整的,事务交互认证是保证解析器收到的消息是从请求的服务器返回的,并且该应答是与请求相对应的.但是,DNSSEC不能拒绝对服务器的非法访问,即如果一个非法的客户端向服务器发送请求,服务器是不能认证也不会拒绝的.

• 其他解析系统

Rendezvous机制.由于DNS解析系统不能满足快速移动的需求,因而对于那些需要实时更新自己当前位置的移动节点来说,需要一种新的机制来完成其身份标识到IP地址的解析.于是,Rendezvous机制被广泛采用,它和DNS一起可以作为一个可以给移动节点(MN)提供快速解析的解析系统.在Mobile IP[62]和Mobile IPv6[63]中,Rendezvous Server(RVS)是一台在家乡网络的服务器,其IP地址在DNS中注册.当用户解析MN的IP地址时,DNS返回RVS的地址,用户再通过RVS获得MN的地址.当MN移动时,其域名和IP的对应关系则只需在RVS中更新.很多协议采用了类似的机制完成移动节点的解析,如HIP,SING,LIN6.只是在SING中RVS被称作Locater Agent,而在LIN6中称作Mapping Agent,但它们的原理都是一样的.

I3[33]的解析本质上也是Rendezvous机制,但是与前面介绍的几种协议不同,它是一种建立在IP网络之上的应用层报文转发体系结构.I3节点负责完成Trigger和报文ID的定位并转发报文,全体I3节点构成了一个基于Chord的Overlay网络,该网络通过报文的ID标识以及Trigger中的主机身份来完成报文的应用层路由.每一个报文在发送端被赋予一个 m 比特长的id,报文的结构为(id,$data$),而接收方发送的Trigger格式为(id_t,$addr$),id_t是

Trigger 的 id,*addr* 是接收主机的 IP 地址或域名.I3 节点要匹配这两个标识,即看它们的前 *k* 个比特是否一致(在文献[33]中,*m*=256,*k*=128),如果匹配,则将报文转发给 *addr*.因此 I3 节点充当了 Rendezvous 服务器的角色,它将一个报文标识解析成了一个主机地址,而解析是根据匹配原则进行的.I3 的报文转发示意图如图 3 所示.

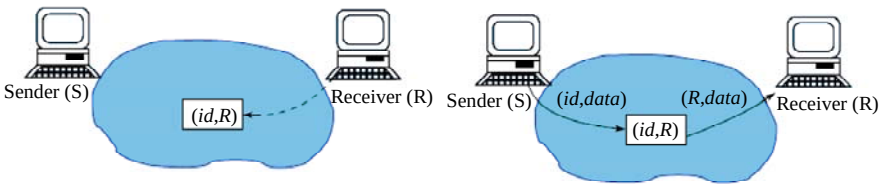

Fig.3 Packet identifier and send and receive procedure of packet in I3

图 3 I3 中数据报文的标识以及报文的发送和接收过程

Handle System[38]采用了分层的解析服务结构.顶层是 Global Handle Registry(GHR),它的下层是 Local Handle Services(LHS).一个 LHS 可以维护多个本地域的 handle 命名空间,但这些信息都要在 GHR 中进行注册.Handle System 的解析服务采用了分布式的结构,由多个子解析服务组成,每个子解析服务由 1 个或多个服务点(service site)组成,每个服务点都是其他服务点的完全备份,由多台服务器组成.因此,Handle System 的解析系统具有很好的健壮性和负载均衡的特点.Handle System 还实现了一定的安全性,当客户端访问一些机密的 handle 或对 handle 进行更改时,Handle 服务器会对客户端进行认证,认证通过后才能返回结果或进行操作.同时服务器和客户端的通信可以经过数字签名,也可以用会话密钥进行加密,从而既保证了数据的完整性,也保证了数据的机密性.

3 命名问题研究中的重要思想

在命名问题的研究过程中,一些有价值的思想和技术被引入这个领域,可以给我们一些启发.这些思想和技术概括起来主要有:

1. 分层思想.这是命名研究中一个重要的思想,通过前面的介绍可以看出很多身份标识都体现了这个思想,例如定义独立的应用层标识、服务资源标识、主机标识和主机位置标识等.分层思想本身也是互联网体系结构的一个重要思想.它可以将问题划分成彼此独立不相关的几个不同的问题,问题之间只需要有统一的接口即可.体现分层思想的解决方案具有较大的灵活性和可扩展性,便于未来的升级,且在维护中成本较低,是我们在命名问题研究中最应重视的思想.

2. Peer-to-Peer 的思想和技术.未来 P2P 应用会有较大的发展,因而基于 P2P 应用和 P2P 安全的身份标识会越来越多(如 GUID 和 HIT).在解析系统中,P2P 的技术被应用得更多,它可以使系统的参与者更加自主,协作性更强,而系统的健壮性也会有所提高.DHT 在目前命名解析技术中使用得较多.它的结构化特点使资源的定位和更新更加快速、有效,成为提高解析系统性能的一个重要手段.P2P 的思想和相关技术随着 P2P 应用和解析系统的发展将越来越受到这个领域研究者的重视.

3. 重定向(redirection)思想.随着大量新的网络服务的不断涌现,很多应用会因为使用这些服务而打破了原有的端到端通信模式.例如,服务器对用户的认证演变成了 SSO 中服务器要求用户 ID 提供商提供认证服务,端到端的互联模式在 Mobile IP 中被家乡代理打破,以及 I3 中提到的 Service Composition[33],都需要一种服务使用另一种服务提供支持,这时重定向技术就不可避免地被使用.因而未来无论研究身份标识的认证技术还是解析系统,都需要考虑重定向带来的变化.同时,重定向的思想也能帮助我们通过利用已有服务的优点简化问题的实现复杂度(如 SSO 和 Rendezvous 机制),因而也是命名领域中的重要思想.

4 总 结

命名问题是当前互联网研究中的一个重要问题.它涉及到了互联网实体(用户、设备、服务、数据)的表示

和使用.研究内容包括身份标识定义和与之有关的认证和解析技术.当前广泛使用的 IP 地址、域名、E-mail 地址、URL 等身份标识都无法满足当前和未来一些应用的需求,因此,人们在这个领域里进行了很多的研究,也提出了许多新的命名空间和命名技术.

目前命名问题的研究热点主要有:用户身份标识的一次登录问题;移动和多宿主环境下主机的身份表示问题;主机身份认证问题;网络融合带来的不同类型设备互联时的身份表示问题;网络服务及网络数据资源的稳定命名;身份解析系统的研究等.

尽管当前已有很多研究,但是还有很多工作需要做.例如,有关 IP 地址过载的问题还没有完全解决,很多新技术在实际中应用中还存在一些困难.随着许多新的互联网体系结构的提出以及新的网络服务的出现,如 LNAI,I3 中的 Service Composition 等,一些新的命名空间也被提出来,但是它们怎样从已有的命名空间过渡也是需要研究的内容.而在身份标识的定义,如是否应该全球统一、是否为字符类型、是否需要划分很多层次等问题上,学术界本身还无定论,这都需要我们作进一步的分析和研究.此外,对身份标识的认证技术还需要发展,而随着解析系统在未来应用中的地位越来越重要,大规模分布式高性能的解析系统研究也必然成为这个领域中重要的研究课题.

References:

[1] Aboba B, Beadles M, Arkko J, Eronen P. The network access identifier. RFC4282, 2005.

[2] Internet protocol, DARPA Internet program, protocol specification. RFC791, 1981.

[3] Deering S, Hinden R. Internet protocol, version 6 (IPv6) specification. RFC 2460, 1998.

[4] 64-Bit global identifier format tutorial. http://standards.ieee.org/regauth/oui/tutorials/EUI64.html

[5] Mockapetris P. Domain names—Concepts and facilities. RFC 1034, 1987.

[6] Mockapetris P. Domain names—Implementation and specification. RFC 1035, 1987.

[7] Moskowitz R, Nikander P. Host identity protocol architecture. RFC 4423, 2006.

[8] Moskowitz R, Nikander P, Jokela P, Henderson T. Host identity protocol. RFC5201, 2008.

[9] Nikander P, Arkko J, Jokela P. End-Host mobility and multihoming with host identity protocol. RFC 5206, 2008.

[10] Nikander P, Laganier J. Host identity protocol (HIP) domain name system (DNS) extensions. RFC 5205, 2008.

[11] Postel J. Transmission control protocol. RFC 793, 1981.

[12] Ylitalo J, Nikander P. A new name space for end-points: Implementing secure mobility and multi-homing across the two versions of IP. In: Proc. of the 5th European Wireless Conf. on Mobile and Wireless Systems Beyond 3G (EW2004). Barcelona: SCI UPC, 2004. 435−441.

[13] Jokela P, Nikander P, Melen J. Host identity protocol: Achieving IPv4-IPv6 handovers without tunneling. In: Proc. of the Evolute Workshop 2003: Beyond 3G Evolution of Systems and Services. Guildford: University of Surrey, 2003. A-2/1-5.

[14] Folke M. Implementing a new naming system for IP mobility called SING [MS. Thesis]. Luleå Universtity of Technology, 2003.

[15] O'Donnell MJ, A proposal to separate handles from names on the Internet. 2003. http://people.cs.uchicago.edu/~odonnell/Citizen/Network_Identifiers/Proposal_to_Separate/proposal_to_separate/

[16] Andreas J, Mats F, Bengt A. The split naming/forwarding network architecture. In: Proc. of the 1st Swedish National Computer Networking Workshop. Arlandastad, 2003.

[17] Nordmark E. Shim6: Level 3 multihoming shim protocol for IPv6. Internet Draft: draft-ietf-shim6-proto-10, 2008.

[18] Cocker D. Internet working multiple address service for transport (MAST). In: Proc. of the 2004 Symp. on Applications and the Internet (SAINT 2004). IEEE Computer Society, 2004. 4.

[19] Matt Crawford, Thomas Narten, John W. Stewart, Zhang LX. Separating identifiers and locators in addresses: An analysis of the GSE proposal for IPv6. Internet Draft, draft-ietf-ipngwg-esd-analysis-05, 1999.

[20] Ishiyama M, Kunishi M, Teraoka F. An analysis of mobility handling in LIN6. In: Proc. of the Int'l Symp. on Wireless Personal Multimedia Communication (WPMC). 2001.

[21] Kunishi M, Ishiyama M, Uehara K, Esaki H, Teraoka F. LIN6: A new approach to mobility support in IPv6. In: Proc. of the 3rd Int'l Symp. on Wireless Personal Multimedia Communications. 2000.

[22] GUID. http://msdn2.microsoft.com/en-us/library/ms679021.aspx

[23] Francis P, Gummadi R. IPNL: A NAT-extended Internet architecture. In: Proc. of the ACM SIGCOMM Conf. New York: ACM, 2001. 69−80.

[24] Sheriton DR, Gritler M., TRIAD: A new next-generation Internet architecture. Technical Report, Stanford: Computer Science Department, Stanford University, 2000. http://www-dsg.stanford.edu/triad/triad.ps.gz

[25] Balakrishnan H, Latshminarayanan K, Ratnasamy S, Shenker S, Stoica I, Walfish M. A layered naming architecture for the Internet. In: Proc. of the ACM SIGCOMM Conf. New York: ACM, 2004. 343−352.

[26] Rosenberg J, Schulzrinne H, Camarillo G, Johnston A, Peterson J, Sparks R, Handley M, Schooler E. SIP: Session initiation protocol. RFC 3261, 2002.

[27] Bradner S, Conroy L, Fujiwara K. The E.164 to uniform resource identifiers (URI) dynamic delegation discovery system (DDDS) application (ENUM). RFC 3761, 2008.

[28] Ford B, Strauss J, Lesniewski-Laas C, Rhea S, Kaashoek F, Morris R. User-Relative names for globally connected personal devices. In: Proc. of the 5th Int'l Workshop on Peer-to-Peer Systems (IPTPS). 2006.

[29] Masinter L, McCahill M. Uniform resource locators (URL). RFC 1738, 1994.

[30] Moats R. URN syntax. RFC2141, 1997.

[31] Fielding R, Masinter L. Uniform resource identifier (URI): Generic syntax. RFC 3986, 2005.

[32] Winoto WA, Schwartz E, Balakrishnan H, Lilley J. The design and implementation of an intentional naming system. Operating Systems Review, 1999,34(5):186−201.

[33] Stoica I, Adkins D, Zhuang S, Shenker S, Surana S. Internet indirection infrastructure. In: Proc. of the ACM SIGCOMM 2002. New York: ACM, 2002.

[34] Nikander P, Arkko J, Ohlman B. Host identity indirection infrastructure (Hi3). IETF Draft, draft-nikander-hiprg-hi3-00, 2004.

[35] Adkins D, Lakshminarayanan K, Perrig A, Stoica I. Towards a more functional and secure network infrastructure. Technical Report, UCB/CSD-03-1242, Berkeley: University of California, 2003.

[36] Weibel S, Jul E, Shafer K. PURL: Persistent uniform resource locators. http://purl.org/

[37] URC. Uniform resource characteristics, uniform resource citation. http://www.auditmypc.com/acronym/URC.asp

[38] Sun S, Lannom L, Boesch B. Handle system overview. RFC 3650, 2003.

[39] Koponen T, Chawla M, Chun BG, Ermolinskiy A, Kim KH, Shenker S, Stoica I. A data-oriented (and beyond) network architecture. In: Proc. of the Sigcomm 2007. New York: ACM, 2007. 181−192.

[40] W3C. Extensible markup language (XML) 1.0 (4th ed.). W3C Recommendation, 2006. http://www.w3.org/TR/REC-xml

[41] W3C. XML Path language (XPath) version 1.0. W3C recommendation, 1999. http://www.w3.org/TR/1999/REC-xpath-19991116.16.html

[42] W3C. XML Pointer language (XPointer) version 1.0. W3C Recommendation, 2001. http://www.w3.org/TR/WD-xptr.html

[43] Lyon J, Wong M. Sender ID: Authenticating e-mail. RFC 4406, 2006.

[44] Fenton J. Analysis of threats motivating domainkeys identified mail (DKIM). RFC 4686, 2006.

[45] Wong M, Schlitt W. Sender policy framework (SPF) for authorizing use of domains in e-mail. RFC 4408, 2006.

[46] Caller ID for e-mail. http://www.microsoft.com/downloads/details.aspx?familyid=9a9e8a28-3e85-4d07-9d0f-6daeabd3b71b

[47] Microsoft Corporation. Windows live ID. http://msdn2.microsoft.com/en-us/library/cc287610.aspx

[48] Microsoft passport.. http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/10704d52-639b-4ffd-a6f4-90f3e1a2e119.mspx

[49] Liberty alliance. http://www.projectliberty.org/

[50] Merrells J, Rowley P, Sermersheim J, Pohlman M. DIX: Digital identity exchange. Internet Draft, draft-merrells-dix-02, 2006.

[51] Wu J, Ren G, Li X. Source address validation: Architecture and protocol design. In: Proc. of the IEEE Int'l Conf. on Network Protocols. 2007. 276−283.

[52] Park K, Wang Z, Pai V, Peterson L. CoDNS: Improving DNS performance and reliability via cooperative lookups. In: Proc. of the 6th Symp. on Operating Systems Design and Implementation (OSDI 2004). Berkeley: USENIX Association, 2004. 14.

[53] Cohen E, Kaplan H. Proactive caching of DNS records: Addressing a performance bottleneck. In: Proc. of the Symp. on Applications and the Internet. San Diego-Mission Valley: Elsevier, 2001. 707−726.

[54] Krishnamurthy B, Liston R, Rabinovich M. DEW: DNS-Enhanced Web for faster content delivery. In: Proc. of the 12th Int'l World Wide Web Conf. Budapest, 2003.

[55] Vahdat A, Dahlin M. Active names: Flexible location and transport of wide-area resources. In: Proc. of the 2nd USENIX Symp. on Internet Technologies & Systems. Berkeley: USENIX Association, 1999. 14.

[56] Shang H, Wills CE. Piggybacking related domain names to improve DNS performance. Computer Network: The Int'l Journal of Computer and Telecommunications Networking, 2006,50(11):1733−1748.

[57] Walfish M, Balakrishnan H, Shenker S. Untangling the Web from DNS. In: Proc. of the 1st Conf. on Symp. on Networked Systems Design and Implementation (NSDI). Berkeley: USENIX Association, 2004. 17.

[58] Handley M, Greenhalgh A. The case for pushing DNS. In: Proc. of the 4th ACM Workshop on Hot Topics in Networks (Hotnets-IV). College Park, 2005.

[59] Ramasuramanian V, Sirer EG. The design and implementation of a next generation name service for the Internet. In: Proc. of the 2004 Conf. on Applications, technologies, architectures, and protocols for computer communications. New York: ACM, 2004. 331−342.

[60] Cohen B. DNSSEC: Security for essential network services, enterprise networking planet. 2003. http://www.enterpriseitplanet.com/security/features/article.php/2206241

[61] Eastlake D. Domain name system security extensions. RFC 2535, 1999.

[62] Perkins C. IP mobility support for IPv4. RFC 3344, 2002.

[63] Johnson D, Perkins C, Arkko J. Mobility support in IPv6. RFC 3775, 2004.

曹锐(1978－),男,北京人,博士生,主要研究领域为互联网体系结构.

吴建平(1953－)男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为计算机网络体系结构,计算机网络协议测试,形式化技术.

徐明伟(1971－)男,博士,教授,博士生导师,CCF 会员,主要研究领域为计算机网络体系结构,形式化方法,协议一致性测试.