下一代互联网实名访问机制研究

汪文勇，黄鹂声

(电子科技大学信息中心 成都 610054)

【摘要】研究互联网主机身份标识和访问控制的相关标准与技术，探讨下一代互联网的实名化策略，提出了一种基于主机标识协议的互联网主机实名化体系架构，并研究如何在此架构中实现基于策略的访问控制，以实现下一代互联网通信各方的身份互信、全局访问控制与授权，防止网络访问的匿名性和自由性。

关 键 词 下一代互联网; 主机标识; 实名标识; 访问控制
中图分类号 TP393 文献标识码 A

Study on Real-Name Access Mechanism in the Next Generation Internet

WANG Wen-Yong，HUANG Li-Sheng

(Information Center, UEST of China Chendu 610054)

Abstract According to the standard and technology of internet host identifying and access controlling and to the strategy of the next generation internet real-name identifying, a host real-name architecture based on the HIP protocol is proposed for implementing peer-to-peer identity trusting, global access controlling and authorizing in the next generation internet, and preventing anonymous and arbitrary network access.

Key words next generation internet; host identity; real-name identity; access control

1 网络实名的提出

由于协议固有的局限性，基于IPv4的信息网络可信程度较低。一方面，互联网主机大多是匿名的，身份无法得到有效验证，助长了用户行为的随意性；另一方面，用户对不同网络资源的访问安全依赖于这些资源本身的访问控制，缺乏统一的授权和访问控制机制。

为了达到更良好的应用效果，下一代互联网应关注如何通过协议和网络构架来实现用户身份透明化、身份认证统一化，以及可集中管理的访问控制，使下一代信息网络更加安全可信。用一句话概括上述目标，就是互联网实名网络访问。

本文提出一种实名网络访问机制，该机制基于主机标识协议(Host Identity Protocol, HIP)实现主机的实名识别[1,2]，并结合基于角色的访问控制(Role-Based Access Control，RBAC)实现集中访问控制[3]。

可以预见，在对移动、多接入等功能有重大需求的下一代互联网中，特别是在安全领域，实名访问将扮演非常重要的角色。

由于独立标识符的引入，可以为互联网中的每一台合法主机统一命名，定义一种认证机制确认上网主机的合法性，并辅以访问控制机制，以实施有效安全控制。这就是本文提出的基于HIP实现实名访问控制机制的核心思路。

2 实名空间与HIP协议

为了解决网络实名访问问题，首先需要一种统一的身份标识和命名机制。互联网工作任务(Internet Engineering Task Force，IETF)的HIP工作组提出了一份草案，建议将现有域名空间进行扩展，采用全称域名(Fully Qualified Domain Name，FQDN)来命名不同的主机，以实现终节点标识符(identifier)与定位符(locator)

收稿日期：2005 – 10 – 14
作者简介：汪文勇(1967 –)，男，硕士，副教授，主要从事网络计算技术、计算机安全理论与技术方面的研究.

的分离。类似于现有的域名，HIP建议为每个FQDN分配一个格式固定的主机标识(Host Identity，HI)来与其对应，由此产生了一个新的命名空间即HI命名空间[2]。

区别于现有的IP协议，HI命名空间要求带有IP栈的任何设备都具有一个HI，HI在统计学上应该是全球唯一的。一个终节点不再与IP地址绑定，而是与HI绑定，如图1所示。

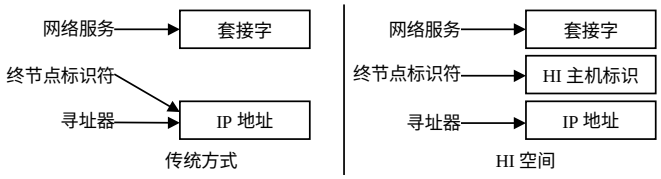

图1 HI命名空间与传统方式在主机标识上的区别

HI命名机制通过HIP协议来实现。HIP协议的主要工作是完成通信双方身份的互相识别与确认。对IPv4协议而言，HIP协议是一种应用层协议，HIP首部作为用户数据报协议(User Datagram Protocol，UDP)载荷被传输；在IPv6环境下，HIP协议首部就是IPv6的一个扩展首部。

3 基于HIP的实名网络模型

在HIP的基础上，本文提出的实名网络模型拟达到以下目的：(1) 以全局的方式命名网络主机即终节点；(2) 保证网络主机名的唯一性和合法性；(3) 有效防止假冒和中间人攻击等。

3.1 命名方式

本文提出的实名网络模型根据IETF草案的建议，对现有的开放源码域名系统进行扩展，增加主机标识符记录HIPHI和实名服务器记录HIPRVS两类域名资源记录，以实现HI的存储、查找定位和有效性验证，并对每个网络实名分配公共密钥基础设施(Public Key Infrastructure，PKI)密钥对，公钥用于主机标识，私钥用于加密签名。扩展后的域名系统提供分配并管理FQDN，可以实现：(1) 实名查找和寻址；(2) FQDN到HI、IP地址的查询和反向查询；(3) HI到IP地址的查询和认证。

采用HI命名空间作为主机实名的实现手段，具有很大的优越性。首先，它可以保证每台主机都有一个得到权威认证的HI，解决目前的大量匿名主机问题；其次，HI取代了IP地址在主机标识方面的用途，意味着一台主机在通讯不中断的情况下可以任意移动和修改IP地址，大大增强了对下一代网络的移动性支持。

3.2 寻址与认证方式

实名模型的寻址过程与传统的域名查询和IP寻址过程有一定差别，表现在以下几个方面。

(1) 动态域名注册

所有移动主机都可以变更IP地址，一旦IP地址变化，主机会立即通知域名服务器，更新IP地址和HI绑定记录。

(2) 基于HI的寻址

所有连接的发起过程必须经过HI查询和定位，不再直接按照IP地址进行查询。同样，应用服务器在向客户机提供服务的同时，也需要反向查找客户机的IP和HI，以确定对方的真实身份。

(3) HI多向认证

完成客户端与服务器之间、客户端与域名系统之间、服务端与域名系统之间的认证，以确保对方身份的合法性和真实性。

客户机访问服务器是一种典型的应用场景。在目前的互联网中，客户机是完全匿名的。希望的模式是，在允许客户访问之前，服务器对客户进行实名认证，其实现过程如图2所示。其他客户对服务器、客户之间、服务器之间的认证原理与此一样，限于篇幅，不再赘述。

图2的应用场景中，客户机在向应用服务器发起实际访问以前，必须经过以下特定步骤来提交自己的实名并接受验证。

(1) 客户机启动一个触发认证(trigger_exchange)过程，向应用服务器发出认证请求，将自己的网络实名和应用服务器的网络实名发送给应用服务器，进行验证。

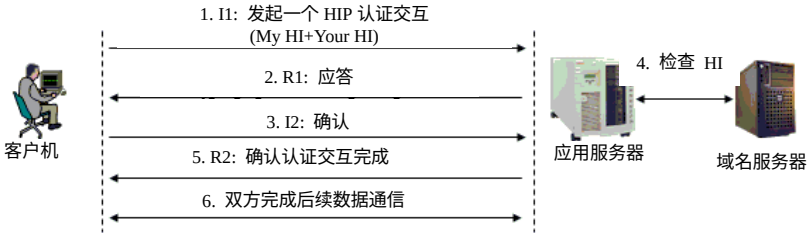

图2　典型应用场景的客户实名认证过程

(2) 应用服务器回复一个puzzle质询，对认证请求进行简单应答，要求协商加密和签名机制(cryptographic solution)。

(3) 客户机启用一个签名方案过程，确定加密和签名机制，开始使用私钥进行签名。

(4) 应用服务器对签名进行检查，并向权威域名机构验证该网络实名是否正活动于客户机所处的IP地址。

(5) 经过以上步骤，应用服务器确定了客户机的网络实名和身份，向客户机发出认证完成确认，双方完成后续的资源请求和响应操作。

3.3　安全性

实名网络模型面临的主要威胁是DOS攻击和中间人攻击。经过分析，最有可能针对HIP协议的DOS攻击共有5种，集中在认证请求、连接重置和应答模拟上。DOS大多在攻击端产生高密度的分组，来迫使服务器端保持大量复杂的协议状态；而攻击端为了节约资源，不保持任何协议状态。可以采用重复协商过程的方式，对第一次协议请求仅进行简单响应，迫使客户端必须首先保持协议状态而且启用签名机制，从而避免大多数DOS攻击。

在缺少第三方认证的情况下，中间人攻击难以防范，但HIP协议强调通信双方都必须与第三方权威域名机构进行认证，而且将PKI证书引入HIP协议，用以产生会话密钥。这就意味着攻击者必须能够同时假冒通信中任意一方的PKI证书、HI名称和IP地址，而实现这些假冒过程是非常困难的。

当然，涉及到安全的因素很多，如针对域名系统的攻击等，限于篇幅本文不详细讨论。

4　RBAC访问控制机制

在下一代互联网中，要实现基于实名的认证和访问控制，只依靠实名命名空间和认证协议是不行的，还需要有一套全局访问控制机制。访问控制是保护资源安全的重要途径，可以限制对关键资源的访问，防止非法用户的侵入或者因合法用户的不慎操作所造成的破坏。

选择开放系统互连开放系统安全框架(ISO/IEC 10181 1996)作为网络实名访问控制模型[4]，它定义了访问控制系统设计时所需要的一些基本访问控制功能(access control functions)组件，并且描述了各功能组件之间不同的通信状态。访问控制功能组件包括initiator、访问控制执行功能(Access Enforcement Function，AEF)、访问控制决策功能(Access Decision Function，ADF)、目标(target)资源几个部分。以上组件在实际应用环境中的关系如图3所示。

在一般的应用架构中，AEF一般部署在负责提供资源的应用服务器上，接受客户的访问请求，向ADF提出决策请求，并根据决策结果限制服务提供范围；ADF则部署在专门的访问控制服务器上，对访问控制的规则进行决策。

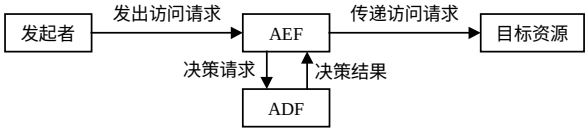

图3　RBAC访问控制功能组件关系

5 基于HIP和RBAC的实名认证与访问控制框架

本文综合应用了HIP协议模型和RBAC访问控制模型的工作机制，提出了实名认证和授权技术方案构架，如图4所示。

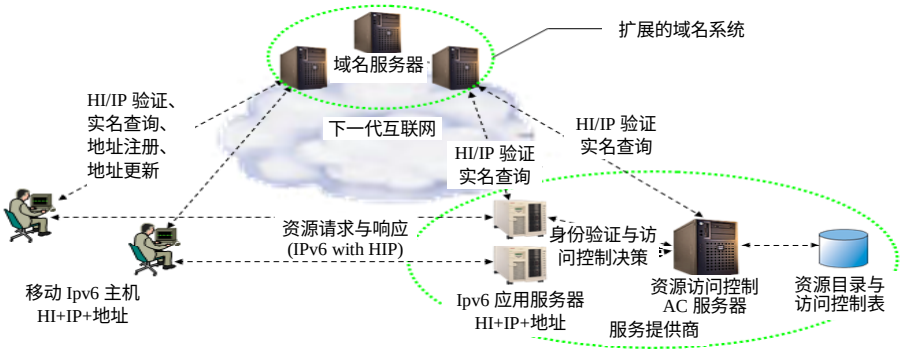

图4 下一代可信网络实名身份认证、访问控制工作框架

在总体应用场景中提出了多种参与角色，包括移动主机、扩展域名服务器、HIP服务器、应用服务器、资源访问控制服务器等等，以上角色互相作用，共同完成彼此的实名身份认证和访问控制过程。

在图4的构架中，移动客户机需要访问某个商业网站服务器，可以通过如下步骤来完成。

(1) 客户机首先必须拥有自己的合法主机标识，标识可能来自于权威机构颁发的PKI证书，也可能来自于服务商提供的下级域名扩展域名，客户机可以将标识存放在本地硬盘，也可以临时从颁发机构获取。

(2) 客户机向域名服务器发出请求，按照实名来获取该网站的标识和当前IP地址。

(3) 客户机与服务器互相认证网络实名。

(4) 客户机发出资源访问请求。

(5) 服务器启用基于角色的访问控制体系，将客户机的网络用户实名和访问资源情况提交给本地(或可信认证机构)的访问控制服务器，检查该用户在本网站系统内的权限角色，决定是否应该向客户机提供服务，或是提供何种级别的服务。

6 结 束 语

HIP是下一代互联网络的主机身份标识手段，RBAC作为流行的访问控制模型，也已经得到了广泛应用，本文对以上两种技术进行了综合分析和利用，提出了一个针对下一代互联网的实名认证和访问控制构架，并分析了其主要工作过程。

参 考 文 献

[1] Moskowitz R, Nikander P, HendersonT. HostIdentityprotocol[EB/OL]. http://www.ietf.org/internet-drafts/draft-ietf-hip-base-04.txt, 2005-10-24.

[2]Moskowitz R, Nikander P. Host identity protocol architecture[EB/OL]. http://www.ietf.org/internet-drafts/draft-ietf-hip-arch-03.txt , 2005-8-1.

[3] Sandhu R, Coyne E, Feinstein H, et al. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38-47.

[4] ISO/IEC 10181-3:1996. Information technology: open systems security frameworks for open systems: Access control framework[S].1996.

编 辑 熊思亮