一种基于MIP路由优化的身份认证方案

张 屹,王 卫,侯整风
(合肥工业大学 计算机与信息学院,安徽 合肥 230009)

摘 要:随着英特网的迅速发展和笔记本电脑的普及,传统方式的Internet已经不能满足人们的需求。移动IP(MIP)由IETF于1992年提出,其中的三角路由问题带来了性能上的缺陷。因此人们提出了多种路由优化方法,其中一种就是引入CA(Communication Agent)来优化路由提高性能,文中正是基于这种优化方法提出了一种新的身份认证方案。它简化了认证过程并且具有很好的安全性。

关键词:MIP;路由优化;CA;认证
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)08-0225-03

A New Authentication Scheme Based on Route Optimization of MIP

ZHANG Yi, WANG Wei, HOU Zheng-feng
(Sch. of Computer and Info., Hefei Univ. of Techn., Hefei 230009, China)

Abstract: Traditional Internet can not meet people's requirements by the rapid development of Internet and the popularization of laptop. Mobile IP(MIP) was designed by IETF in 1992 and its route problem causes the performance deficiency. People put forward many route optimization schemes. One of them uses CA(communication agent) to optimize route perfoamance. Design a new authentication scheme based on this route optimization. It has simple authentication process and reliable security.

Key words: MIP; route optimization; CA; authentication

0 引 言

随着英特网的发展和笔记本电脑的普及,传统的有线网络已经不能够满足人们日益多样的需要,人们需要随时随地地接入Internet,这就需要一种新的网络通讯协议。

移动IP由IETF的移动工作组于1992年6月提出,并于1996年由IESG通过并公布为建议标准[1,2]。因为移动主机(MH)的位置可能会不断地改变,移动IP提供了一种路由机制,使得移动节点可以使用一个固定的IP地址连接到任何的链路上[3]。但是,通信节点(CN)和移动主机之间的数据包需要家乡代理(HA)转发,造成了性能上的缺陷[4]。目前学术界提出了各种路由优化方法[5~8],引入CA(Communication Agent)[6]就是一种很好的路由优化方法。

文中将介绍IETF的MIP思想及一种引入CA的路由优化方法,然后在此方法的基础上,提出了一种新的双向认证方案。

1 IETF的移动IP思想

1.1 相关概念

(1) 移动主机(MH,Mobile Host)。它可以从接入英特网的某一条链路切换到另外一条链路上,并且始终使用其家乡地址(Home Address)而不改变IP地址。

(2) 家乡代理(HA,Home Agent)。它与MH的家乡链路相连接,在移动通信中负责通信节点CN与MH之间直接(MH属于家乡链路)或者间接(MH属于外地链路)的通信。

(3) 外地代理(FA,Foreign Agent)。它与MH移动到的某个外地链路相连,负责与家乡代理协作,帮助目前处于所辖链路的MH与CN之间的通信。

(4) 通信节点(CN,Communication Node)。就是与MH进行通信的节点。

(5) 隧道技术(Tunneling)。如图1所示,当一个数据包被当成另外一个数据包的载荷数据的时候,它所经过的路径被称作隧道。当MH处于外地链路且使用FA的IP地址作为COA时,HA将CN要发给MH的数据包封装进另外一个数据包发给FA,FA获取数据包后将数据包拆封,把载荷内的原始数据包发给MH。

(6) 转交地址(COA,Care Of Address)。COA是MH移动到外地链路时所提交的转交IP地址。COA又分为两种:第一种是外地代理转交地址,即MH使用外地代理的IP地址作为COA;第二种是配置转交地址,MH通过静态分配(如手工配置)或者动态分配(如使用DHCP服务器)获得一个暂时的IP地址作为COA。

(7) 家乡地址(Home Address)。就是移动主机MH

收稿日期:2005-11-14
作者简介:张 屹(1982-),男,安徽合肥人,硕士研究生,研究方向为网络安全;侯整风,副教授,研究方向为网络安全。

固定使用的处于家乡链路的 IP 地址。

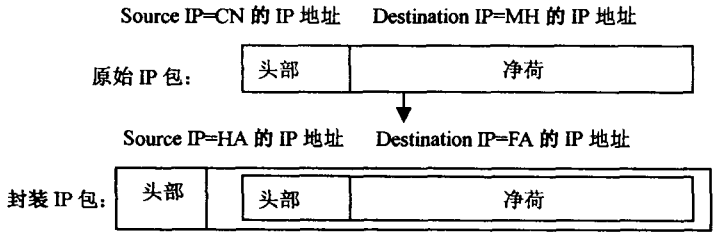

图 1 隧道技术

1.2 工作机制

家乡代理和外地代理周期性地发出广播消息,当 MH 收到消息后,就可以判断自己是处于家乡链路还是外地链路,如果是处于家乡链路,则按照常规进行工作;如果处于外地链路,则可以通过 FA 发来的消息,把 FA 的 IP 地址作为 COA,也可以通过 DHCP 或手工配置一个 COA。然后 MH 通过 FA 向 HA 注册新的 COA, HA 确认 MH 的身份后进行地址的绑定更新(Binding Update),将 MH 的家乡地址和新的 COA 一起绑定到路由表中。HA 将注册确认消息发送给 MH,通知 MH 注册完成。

当 CN 打算发送数据给 MH 时,由于 MH 的 IP 地址是家乡地址,CN 发送到 MH 的数据包会被 HA 所截获。如果 HA 发现 MH 不在家乡链路上,就分两种情况处理:如果 COA 是一个配置转交地址,就直接发给这个地址;如果这个 COA 是一个外地代理转交地址,则需要通过隧道技术封装数据包发送给 FA,再由 FA 打开封装,把原始数据包发送给 MH。而 MH 发送给 CN 的数据包则直接路由到目的地。

由于 HA 对 MH 的认证机制,MH 的身份是可以确认的,这就可以有效地防止不怀好意者的 DoS 攻击。此外,移动 IP 在注册请求消息中还使用了标识域来防止不怀好意者通过重新发送截获的认证消息来进行重发攻击。

1.3 三角路由问题

从以上可以看出,当 CN 需要向 MH 发送数据时,必须通过 HA 转发给 FA,这大大增加了通信代价。特别地,当 CN 和 MH 处于同一个网络中,消息却要绕一个大圈子才能传送到目的地,这对于实时性较强的业务是很不利的。

针对这个问题,IETF 又提出了优化路由方案 ROMIP。其思想是:让 CN 直接与 MH 通信,但这不但加大了移动 IP 实施的复杂度(因为需要升级 CN,使其具有隧道功能),而且会造成安全上的隐患。一个不怀好意者很容易发送假消息声称自己是 MH,让 CN 发送消息给假的 MH。

2 使用 CA 的路由优化方案

2.1 工作原理

为了解决三角路由问题,有人提出了使用通信代理 CA[1]来优化路由。当 COA 为外地代理转交地址时,通信方式如图 2 所示。

CA 作为 CN 把数据包发向移动主机 MH 的中转,和 HA,FA 一样,CA 也会向本地网络发出广播消息声明自己的存在。假设 MH 不在家乡链路,HA 截获 CN 发来的数据包后,就发送应答消息告诉 CN 当前 MH 的 COA。然后 CN 向本地的 CA 发送消息要求建立绑定表,之后就可以通过 CA 发送数据包给 MH。如果 COA 是外地代理转交地址,CA 会用隧道把数据包送到 FA;如果是配置转交地址,则直接把数据包发给 MH。

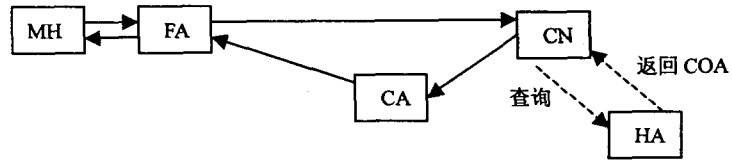

图 2 引入 CA 的路由优化方案

由于 CA 处于 CN 所在网络上,数据包传输时不像三边路由需要经过 MH 的家乡代理 HA,不同位置的 CN 有各自的本地 CA 去帮助自己最佳路由到 MH。这种路由方案缩短了传输路径,而且实现起来比较简单,不用对每一个打算和 MH 通信的 CN 进行改造,具有较好的可行性。尽管如此,它却没有解决 MH 对于 CN 的身份认证问题,这在需要身份认证的系统中应用是远远不够的。

2.2 认证问题

无论是最初的移动 IP 路由方法还是这个引入了 CA 的优化路由方法,都只考虑了 CN 对于 MH 的身份认证(HA 对于 MH 具有认证的能力,CN 通过 HA 得到确认身份的 MH 的转交地址),没有 MH 对 CN 的认证,即身份的认证是单向的。如果需要双方都能够相互鉴别身份,就需要我们使用传统的认证机制来确认彼此身份。

考虑到 HA 已经确认了 MH 的身份,如果再进行 CN 对于 MH 的身份认证就显得有点多余。是否能够利用移动 IP 协议中 HA 对于 MH 的身份认证,仅增加 MH 对 CN 的身份认证就能达到双向的身份认证。下面给出新的认证方案。

3 新的认证方案

3.1 认证机制

在新的认证方案中,增加了可信认证中心(AC, Authentication Center)来认证 CN 的身份。至于 AC 如何对于 CN 进行认证,可以视具体的情况而定。同样,家乡代理也可以采取各种认证算法来验证 AC 发来的信息,但是根据移动 IP 的规范,建议使用 MD5 为缺省算法。

为了方便讨论,假设 AC 与 CN 之间共享密钥 Kac, AC 与 HA 之间共享密钥 Kah,CN 与 HA 之间临时会话密钥为 Ks,而 HA 对于 MH 进行认证的共享密钥设为 Km。其中,Km 是原本的移动 IP 协议中 HA 对 MH 进行身份鉴别的密钥。

当 CN 打算与 MH 通信时,先发送认证请求信息 Kac

(CN)让认证中心AC验证。AC利用共享密钥Kac解密,确认CN的身份后,发送Kac(Ks)给CN让它得到临时会话密钥Ks。同样,AC还会发送Kah(CN,Ks)给HA,告诉HA通信节点CN已经通过认证,让HA发送MH的COA给CN。HA用Kah解密后,使用刚接收到的Ks发送Ks(COA,Km(CN))。CN用Ks解密后,向CA请求绑定路由表,把Km(CN)发送给MH,让MH知道这个CN的身份是经过认证的。至此认证工作结束,CN可以按照先前的优化路由方案发送数据包给MH了。

具体步骤如下所示:

(1) CN: Kac(CN)→AC

(2) AC: Kah(CN,Ks)→HA, Kac(Ks)→CN

(3) HA: Ks(COA,Km(CN))→CN

(4) CN: Km(CN)→MH

3.2 认证的安全性及相关讨论

当CN的身份被AC确认后,AC会让HA发送MH的COA给CN(HA对于MH的认证已经由移动IP协议所确保),CN完全可以相信这个MH的转交地址COA是真实可信的,从而相信这个MH的身份是已经确认的。而MH收到了用自己和HA之间的共享密钥加密的CN的身份信息,也可以据此相信CN的身份已经被家乡代理确认了,进而相信这是一个经过认证的CN。此外,通过时间戳可以防止不怀好意者通过截获Km(CN)来进行重发攻击;通过使用可信的AC分发的会话密钥Ks,使得CN可以确认HA的真实身份,防止了一个假冒的HA把伪造的MH的转交地址COA发给CN。

本方案并没有直接让移动主机MH对CN进行认证,原因在于:对于一个常规密钥系统,每一对MH和CN的双向认证都需要MH和AC有共享密钥,这使得密钥分发变得十分繁琐。而在本方案中,AC和MH之间分发密钥变成了AC和家乡代理HA之间分发密钥,而只要有这样一个密钥,HA就可以利用移动IP固有的HA和MH之间的共享密钥发送CN的身份认证信息给MH。换句话说,AC和HA之间的密钥代替了AC与HA所属的多个MH之间的密钥,一个密钥分发达到了多个密钥分发的认证效果,从而简化了密钥的分发复杂度,同时也有利于密钥的统一管理。

4 结束语

文中介绍了移动IP基本思想,根据使用CA的移动IP路由优化方法,提出了一种新的身份认证方案并对其进行了讨论。此方案利用了移动IP协议中HA对MH进行认证的特性,同时结合了引入CA的优化路由,简化了双向认证的复杂性,且具有较高安全性和可行性。当然,这种方案也存在一些问题,比如:方案的实施很大程度依赖家乡代理HA的可靠性,如果HA作假或者受到攻击变得不可靠,认证将面临新的挑战,这也是今后需要解决的问题。

参考文献:

[1] Perkins C. IP Mobility Support[S]. RFC2002. 1996.

[2] Perkins C. IP Encapsulation within IP[S]. RFC2003. 1996.

[3] Johnson D B, Perkins C. Route Optimization in Mobile IP[EB/OL]. draft-ietf-mobileip-optim-05.txt, 1996-10.

[4] Solomon J D. 移动IP[M]. 北京:机械工业出版社,2000.

[5] Stallings W. 密码编码学与网络安全:原理与实践(第2版)[M]. 北京:电子工业出版社,2001.

[6] 岑　巍. 关于移动IP的进一步研究[J]. 电信科学,1992(2):15-17.

[7] 朱　健,杨　庚. 移动IP路由方案研究[J]. 中国数据通信,2003(4):82-85.

[8] 蒋海林,张丽娟,谈振辉. Mobile IP路由优化协议中存在的一些问题[J]. 电力系统信息,2002(2):49-51.

(上接第224页)

对角色进行定位是先把主体(用户、线程、进程)的行为类型(消息类型)与角色对应起来,形成一个角色表,即,只有请求执行某种类型行为的主体才能够被分派相应的角色,此时,角色的分派不是直接与主体相关联,而是与主体的请求行为有关。事实上,在CIST中,一个主体能够请求执行的行为,已经在主体形成的时候与主体关联起来了。这是一个简单灵活的RBAC实现方式。

5 结束语

在CIST中,资源对象和对象属性只能由指定的程序访问,通过控制程序的访问权限,就可以控制对对象及其属性的安全访问。把安全内核的体系结构定义为正交体系结构,便于安全内核的功能扩展。把每个子系统定义为一个对象,便于子系统的改进。通过RBAC保证安全内核中每个对象的安全访问,既提高了系统的安全性,也加强了系统的独立性。由于没有增加程序执行过程的复杂度,所以不会降低系统效率。

参考文献:

[1] 訾小超,张绍莲,茅　兵,等. 访问控制技术的研究与进展[J]. 计算机科学,2001(7):26-28.

[2] Ferraiolo D F, Kuhn D R. Role-Based Access Controls[A]. Proceedings of the 15th NIST-National Computer Secuity Conference[C]. Baltimore, Maryland:[s.n.],1992.

[3] Ferraiolol D F, Cugini J A. Role-Based Access Control(RBAC): Features and Motivations[A]. 11th Annual Computer Security Appilcations Procceedings[C]. Maryland:[s.n.], 1995.

[4] 张友生. 几种新型软件体系结构[EB/OL]. URL: http://www.opentest.51.net/softeng/newstru.htm, 1999.

[5] Barkley J. Implementing Role-Based Access Control using Object Technology[A]. First ACM Workshop on Role-Based Access Control[C]. Gaithersburg, Maryland:[s.n.],1995.