计算机科学2002Vol. 29№. 4

移动IPv6的一种双向认证机制

A Method of Bi-directional Authentication for Mobile IPv6

何 涛 杨寿保

(中国科学技术大学计算机科学技术系 合肥230026)

Abstract In this paper we analyze the security problems mobile IPv6 faces at the first, then give a method of bi-directional authentication which can be used between the mobile node and the home agent. We also discuss the secure capability of this method.

Keywords Mobile node, Home Agent, Bi-directional Authentication

1 引言

随着网络技术与便携式终端的不断发展,在IP网络中实现对移动性的支持变得越来越重要。象其它台式机用户一样,移动计算机(或者便携式终端)用户希望接入同样的网络,共享资源和服务,而不局限于某一固定区域。且当它移动时,也能方便地断开原来的连接,并建立新的连接。为了支持计算机在移动时仍能保持与因特网的通信,IETF(Internet 工程任务组)开展了一系列研究工作,对移动IP提出了一系列RFC标准。IPv6是下一代的因特网协议,它最终将代替IPv4成为因特网的主要网络层协议,IPv6已经被第三代移动通信合作工程(3GPP, The 3rd Generation Partnership Project)选为下一代移动通信的基本协议。基于IPv6的移动IP(以下称为"移动IPv6")目前是IETF移动IP工作组议程上的主要课题,但移动IPv6目前在安全方面还面临着一些问题。

2 移动IPv6的基本原理及安全问题

为了在移动的时候仍然保持传输层的连接,移动节点必须始终保持一个固定的IP地址,即家乡地址(Home Address)。另一方面,由于移动节点的移动性,要想使通信顺利进行,移动节点还必须绑定另一个IP地址,即转交地址(Care-of Address),发往移动节点的数据包由这个地址来转交。转交地址可以被认为是移动节点拓扑结构意义上的地址。与家乡地址网络部分匹配的子网被称为移动节点的家乡网络(Home Networks),而其余子网称为移动节点的外地网络(Foreign Networks)。家乡网络有一个代理,叫家乡代理(Home Agent)。

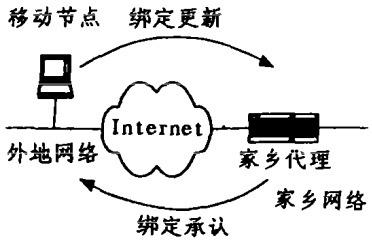

图1 家乡代理的移动绑定

3 移动节点和家乡代理之间的双向认证

针对上述移动IPv6中面临的安全问题,我们提出了移动节点连接在它的家乡网络上时与任何固定的主机一样工作。而当移动节点连接在外地网络上时,它采用IPv6定义的地址自动配置方法得到外地网络上的转交地址,然后移动节点将它的转交地址通知给家乡代理以及通信节点。不知道移动节点的转交地址的通信节点送出的数据包先被路由到移动节点的家乡网络,从那里家乡代理再将它们经过隧道送到移动节点的转交地址。知道移动节点转交地址的通信节点送出的数据包可以直接送给移动节点。在相反方向,移动节点送出的数据包采用特殊的机制被直接路由到它们的目的地。

在移动IPv6中,移动节点的家乡地址与它的转交地址的捆绑称为移动节点的"绑定"。当移动节点离开家乡网络到达外地网络后,它向家乡代理发送绑定信息进行注册。移动节点向家乡代理发送一个包含绑定更新信宿选项的包,家乡代理回送一个包含绑定承认信宿选项的包。如图1所示。移动节点注册的主要目的是让移动节点将它的转交地址通知它的家乡代理,家乡代理根据转交地址把目的地址为移动节点家乡地址的数据包通过隧道转发到移动节点(通信节点知道移动节点转交地址后可以直接把数据包发到转交地址处,而不用再经过家乡代理)。当一个黑客主机发出一个伪造的绑定更新消息,把它自己的IP地址当作移动节点的转交地址时,如图2所示,通信节点发出的所有数据包都会被送到黑客主机。这样会出现两个明显的问题:黑客主机可以看到每一个送给移动节点的数据包,同时移动节点从所有的通信中被断开了,因为它不可能再接收任何数据包了。同样的,黑客主机可以假冒家乡代理与移动节点进行通信。因此,在移动节点向家乡代理注册之前,移动节点和家乡代理必须进行双向认证,移动节点所发送的绑定信息必须进行签名认证。

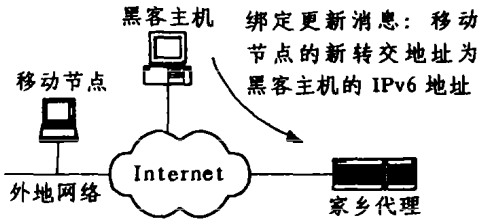

图2 假冒移动节点的转交地址

节点和家乡代理之间的一种双向认证机制,可以防止会话替换,还可以防止重发攻击。首先假设移动节点和家乡代理都拥有由认证机构(Certifying Authority)颁发的证书(Certifica-

何 涛 硕士研究生,研究方向:IPv6以及移动IP;杨寿保 教授,博导。

te)。移动节点拥有一个签名方案,由签名算法 Sig_{mn}、验证算法 Ver_{mn}、公有密钥以及私有密钥组成。认证机构提供公开的对其签名进行验证的算法 Ver_{ca}。移动节点拥有一个证书 $C(MN)$:

$$C(MN)=(ID(MN),K_{mn},Sig_{ca}(ID(MN)(K_{mn}))$$

其中 $ID(MN)$是移动节点的身份信息,K_{mn}是移动节点的公有密钥,Sig_{ca}是认证中心的签名算法。同样的家乡代理也拥有一个证书 $C(HA)$:

$$C(HA)=(ID(HA),K_{ha},Sig_{ca}(ID(HA),K_{ha}))$$

下面给出具体的认证过程,如图3所示:

(1)移动节点生成一个随机数 N_{mn},发送给家乡代理。

(2)家乡代理生成一个随机数 N_{ha},用家乡代理的私有密钥对 N_{mn}以及 N_{ha}计算签名 $Sig_{ha}(N_{mn},N_{ha})$。然后把 $C(HA)$、N_{ha}、$Sig_{ha}(N_{mn},N_{ha})$发送给移动节点。

(3)移动节点使用 Ver_{ca}来验证 $C(HA)$,然后使用经过认证的家乡代理的公有密钥 K_{ha}对 $Sig_{ha}(N_{mn},N_{ha})$进行验证。

(4)移动节点用自己的私有密钥 N_{mn}以及计算签名 $Sig_{ha}(N_{mn},N_{ha})$,并且对绑定更新消息 BM 计算签名 $Sig_{mn}(BM)$,然后把 $C(MN)$、$Sig_{mn}(N_{mn},N_{ha})$、$Sig_{mn}(BM)$发送给家乡代理。

(5)家乡代理使用 Ver_{ca}来验证 $C(MN)$,然后使用经过认证的移动节点的公有密钥 K_{mn}对 $Sig_{mn}(N_{mn},N_{ha})$进行验证。如果证实是移动节点发送过来的,再用移动节点的公有密钥 K_{mn}解开 $Sig_{mn}(BM)$,得到经过认证的绑定更新消息,从而可以完成移动节点的注册。

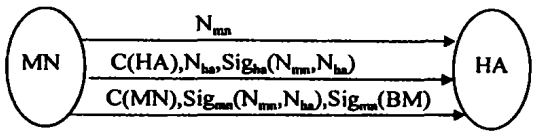

图3 移动节点和家乡代理之间的双向认证示意图

下面分析一下这种认证机制是如何防止中间人攻击以及重播攻击的。

(1)假如有黑客伪装成移动节点与家乡代理进行认证,黑客发出随机数 N 给家乡代理,家乡代理把 $C(HA)$、N_{ha}、$Sig_{ha}(N,N_{ha})$返回给黑客,这时该轮到黑客发送 $C(MN)$、$Sig_{mn}(N,N_{ha})$、$Sig_{mn}(BM)$给家乡代理了,然而计算 $Sig_{mn}(N,N_{ha})$需要用到移动节点的私有密钥,黑客将无法得逞。即使黑客主机随便用一个密钥计算 $Sig_{any}(N,N_{ha})$,家乡代理收到后发现不能对此进行认证而丢弃它,从而也就不会按照黑客的要求对之进行注册。

(2)假如黑客伪装成家乡代理与移动节点进行认证,黑客接收到移动节点发送过来的随机数 N_{mn}后,必须返回 $C(HA)$、N_{ha}、$Sig_{ha}(N_{mn},N_{ha})$给移动节点,然而计算 $Sig_{ha}(N_{mn},N_{ha})$必须知道家乡代理的私有密钥,黑客同样将不能得逞。

(3)假如黑客进行的是重发攻击,黑客第一次窃取到移动节点发送给家乡代理的认证消息 $C(MN)$、$Sig_{mn}(N_{mn},N_{ha})$、$Sig_{mn}(BM)$时把它保留下来,当其第二次窃取到移动节点发送给家乡代理的认证消息 $C(MN)$、$Sig_{mn}(N_{mn'},N_{ha'})$、$Sig_{mn}(BM')$时,企图用 $C(MN)$、$Sig_{mn}(N_{mn},N_{ha})$、$Sig_{mn}(BM)$代替 $C(MN)$、$Sig_{mn}(N_{mn'},N_{ha'})$、$Sig_{mn}(BM')$发送给家乡代理。然而 M_{mn}与 N_{ha}是随机数,只一次有效,家乡代理在用本地保存的 $N_{mn'}$以及 $N_{ha'}$验证 $Sig_{mn}(N_{mn},N_{ha})$时认证失败。

从上面的分析可以看出,这种双向认证机制是安全的可靠的。

结束语 本文设计了一种移动 IPv6中移动节点和家乡代理间的双向认证机制,这种机制引入了认证证书,可以有效地防止会话替换,包括假冒移动节点与家乡代理进行通信,假冒家乡代理与移动节点进行通信等。由于这种机制采用了随机数,还可以有效地防止重发攻击。采用这种认证机制,当移动节点移动到不安全的外地网络时(特别是无线环境下的网络),可以安全地向家乡代理进行注册,从而可以安全地与其它 IPv6节点进行通信。移动 IPv6是一门非常有前途的技术,其安全问题的解决将有助于加速其投入实际运用的进程。

参 考 文 献

1 Solomon J. Mobile IP: The Internet Unplugged. Prentice Hall: 1998. 161～178

2 Johnson D B, Perkins C. Mobility Support in IPv6. INTERNET-DRAFT, 2000-11

3 Perkins C. IP mobility support. IETF RFC 2002, 1996-10

4 Diffie W, Oorschot P C, Wiener M J. Authentication and Authenticated Key Exchanges. Designs, Codes and Cryptography. 1992, 107～127

5 Diffie W, Hellman M E. New Directions in Cryptography. IEEE Transactions on Information Theory. 1976, 645～654

(上接第105页)

15 Chan M C, Lazar A A. Designing a CORBA-Based High Performance Open Programmable Signaling System for ATM Switching Platforms. IEEE J. on Selected Areas In Communications, 1999, 17 (9): 1537～1548

16 Vinoski S. CORBA: Integrating Diverse Applications Within Distributed Heterogeneous Environment. IEEE Communication Magazine, 1997(Feb): 46～55

17 Maffeis S, Schmidt D C. Constructing Reliable Distributed Communication System with CORBA. IEEE Communication Magazine, 1997(Feb): 56～60

18 Schmidt D C, et al. A High-Performance End System Architecture for Real-Time CORBA. IEEE Communication Magazine, 1997 (Feb): 72～77

19 Sunaga H, Yamada T. NOSES Distributed Communication Switching Software Structure Based on CORBA. IEEE Intl. Conf. on Communications, 1997. 760～764

20 Sunaga H, Yamada T. NOSES Distributed Communication Switching Software Structure Based on CORBA. IEEE Intl. Conf. on Communication (ICC' 97 8-12 June 1997. Montreal, Quebec, Canada) 1997. 760～764

21 方亮,张淑芳. CORBA 技术在 TMN 中的应用及相关问题. 数字通信, 2000, 27(8): 65～68

22 沈桥,易萍,徐琼,寿国础. CORBA 和 TMN 综合技术的研究. 北京邮电大学学报, 2000, 23(1): 71～75

23 胡健,刘锦德. 基于 CORBA 的网络管理技术研究. 计算机科学, 2000, 27(12): 30～33

24 毛云峰,董金祥. 基于分布环境的电信网络管理系统的设计和实现. 计算机应用研究, 2000, 17(5): 51～53, 106