基于 IPSec 的移动 IP 安全体系框架

IPSec-based Mobile IP Security Architecture

顾国飞　朱光宇　张世永　刘松鹏

（复旦大学计算机与信息技术系　上海200433）

Abstract　Mobile IP is one of the key technologies to implement mobile computing. But its security still needs further research. After an introduction to mobile IP, IPSec and the threat to mobile IP security, an IPSec-based mobile IP security architecture is presented in the article. This architecture combines IPSec and some other secure measures with mobile IP so as to give mobile IP stronger security. In the article this architecture is discussed in detail and a method is proposed to traverse firewall using IKE.

Keywords　Mobile IP, IPSec, Security architecture, IKE, Firewall traversal

1. 引言

让人们能够随时、随地访问 Internet，是当前 Internet 研究的一个热点，也是下一代真正的个人通信技术的目标。移动 IP 就是这样的一种技术，它也是目前唯一可以在 Internet 上为移动计算机提供无缝漫游的协议。

由于移动 IP 通信往往既经过有线链路，又通过无线链路，被攻击的概率比普通 IP 通信大大增加，因此面临着更大的网络信息安全方面的威胁。由此可见，考虑在移动 IP 通信环境下的安全体系非常必要，它是决定移动 IP 能否最后真正被接受的最重要因素之一。

很多人都想到采用 IPSec 来加强移动 IP 的安全性[1~3]，但并没有提出一个完整的安全框架来对付移动 IP 环境中的各种安全威胁。本文提出了一种基于 IPSec 的移动 IP 安全体系框架，试图将两者较好地融合，同时加入了其他一些安全措施，以在移动 IP 环境中提供足够的安全性。

2. 移动 IP

在移动 IP[4~6]中，定义了三种新的通信功能实体：移动节点（Mobile Node，以下简称 MN）、本地代理（Home Agent，以下简称 HA）、外地代理（Foreign Agent，以下简称 FA），使用了三个关键技术：代理搜索（Agent Discovery）、注册（Registration）和隧道技术（Tunneling）。下面简述一下移动 IP 的工作原理（如图1所示）。

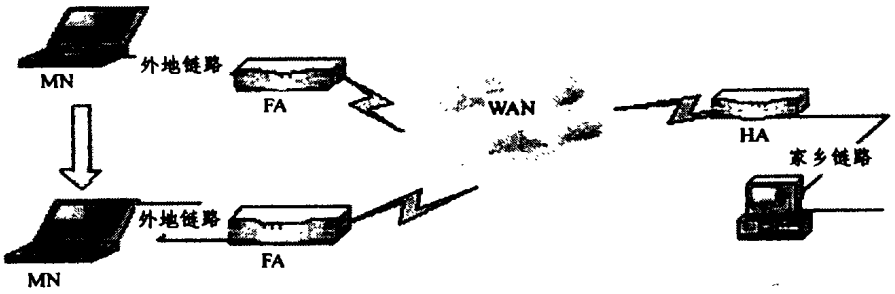

图1　移动 IP 工作原理

1）尽管 MN 可以移动，但每个 MN 都拥有一个固定不变的家乡地址。MN 通过发送代理请求或通过接收 FA/HA 发送的代理广播消息确定自己是连在本地网络还是外地网络上。如果是连在本地网络上，MN 就可像固定节点一样工作，不再利用移动 IP 的其它功能。

2）如果 MN 连在外地网络上，它就通过 FA 的代理广播消息得到转交地址（Care-of Address，以下简称 COA，一般为外地代理地址），并向 HA 注册得到的转交地址。

3）注册完成后，所有发向 MN 家乡地址的数据包被 HA 获得，然后通过隧道向转交地址传送，在 FA 处数据分组被从隧道中取出，送往 MN。可以采用三种隧道技术：IP 的 IP 封装（IP in IP Encapsulation）[7]、最小封装（Minimal Encapsulation）[8]和通用路由封装（Generic Routing Encapsulation）[9]。通过隧道技术，避免了从家乡链路到外地链路上所有路由器的路由信息改动。

4）当 MN 向外发送数据包时，照常处理，无需隧道技术。对 MN 的数据分组来说，FA 完成默认路由器的功能。

3. 移动 IP 环境中的安全威胁

在移动 IP 环境中存在着许多威胁（其实普通 IP 环境中也存在着这些威胁，不过在移动 IP 环境中更易受到攻击），种类虽然很多，但概括起来可以归纳为以下五种：窃取机密攻击、恶意攻击、假冒攻击、抵赖、篡改。

1）窃取机密攻击　是指未经授权的攻击者非法访问网

顾国飞　硕士研究生，主要研究方向为计算机网络应用、网络安全、网络与分布式计算。朱光宇　硕士研究生，主要研究领域为计算机网络、Internet 应用。张世永　博士生导师，主要研究领域为计算机安全、计算机网络应用。刘松鹏　硕士，主要研究领域为计算机网络、安全、分布计算。

络、窃取信息的情况，一般是通过在不安全的传输通道上截取正在传输的信息或者利用协议或网络的弱点来实现的。由于移动 IP 中的无线链路是非常脆弱的，为得到链路上传送的信息，攻击者甚至并不需要物理地连接到网络上，因此这类攻击要引起高度重视。

在移动 IP 环境中，窃取机密攻击有两种：一种是被动偷听(Passive Eavesdropping)，即在网络上监听传送的数据包，另一种是会话窃取攻击(Active Session Stealing，也称 Takeover)，即在一个合法用户经认证后开始通信时，攻击者冒充合法用户的身份(如 IP 地址)将正在进行的通信窃取过去。

2)恶意攻击　在当今最为突出的就是拒绝服务攻击 DoS (Denial of Service)了。典型的拒绝服务攻击有如下两种形式：资源耗尽和资源过载。当一个对资源的合理请求大大超过资源的支付能力时就会造成拒绝服务攻击。拒绝服务攻击的手段有 Smurf[10]、Land[11]、TCP SYN Flooding[12]等等。

在移动 IP 中具体的拒绝服务攻击形式有两种：(1)攻击者向 HA 发出伪造的注册请求，把自己的 IP 地址当作 MN 的 COA。这样在成功注册后，通信对端节点(Correspondent Node，CN)的数据包都会被 HA 通过隧道送给了攻击者，而真正的 MN 则被拒绝了服务，再也收不到任何数据了。(2)攻击者以 TCP SYN Flooding 攻击服务器，使服务器无法响应其它有用信息，从而使得合法的 MN 被拒绝服务。

3)假冒攻击　重放攻击(Replay)是最常见的假冒攻击。它利用身份验证机制中的漏洞先把消息记录下来，然后再发送出去。在移动 IP 中，最常见的重放攻击是：攻击者将一个有效的注册请求消息保存起来，过了一段时间后再重发这个消息，从而注册一个伪造的 COA。

4)抵赖(Repudiation)　就是否认自己做过的事，在移动 IP 中无法防止攻击者的抵赖。

5)篡改　其实和窃取机密攻击是连在一起的。在移动 IP 中，恶意的攻击者能够篡改通信信息，更严重的是篡改注册信息。

由上分析可见移动 IP 环境中存在着比普通 IP 环境更大的安全威胁，移动 IP 本身并没有完全解决这些问题，它的安全弱点在于没有提供强的认证、加密和完整性检查(特别是在注册过程中)，同时也没有一个密钥管理的机制，而这些又正好是 IPSec 所能提供的，所以下面先介绍一下 IPSec，再提出基于 IPSec 的移动 IP 安全体系框架。

4. IPSec

IPSec 提供了一种标准的、健壮的以及包容广泛的机制[13,14]，可以用它为 IP 及上层协议(如 TCP 和 UDP)提供安全保障。IPSec 由一系列协议组成，图2显示了 IPsec 的体系结构、组件及各组件间的相互关系。

IPSec 可以有两种工作模式：传输模式(Transport Mode)和通道模式(Tunnel Mode)。两者的区别在于传输模式只保护 IP 的载荷，安全协议头插在 IP 头和上层协议头(如 TCP 或 UDP 头)之间，而通道模式保护整个 IP 包，要对整个 IP 包封装，安全协议头位于内外 IP 头之间。

IPSec 有三个最主要的部分：验证头(Authentication Header，AH)[15]、封装安全载荷(Encapsulating Security Payload，ESP)[16]和密钥交换(Internet Key Exchange，IKE)[17~19]。

1)验证头 AH 为 IP 包提供数据完整性检查和验证服务。通过使用数据完整性检查，可判定数据包在传输过程中是否被修改；通过使用验证机制，终端系统或网络设备可对用户或应用进行验证，过滤通信流，还可防止地址欺骗攻击及重放攻击。完整性检查的 MAC 计算至少要支持 HMAC-MD5-96和 HMAC-SHA-96，实践中也常用加密 SHA-1算法。

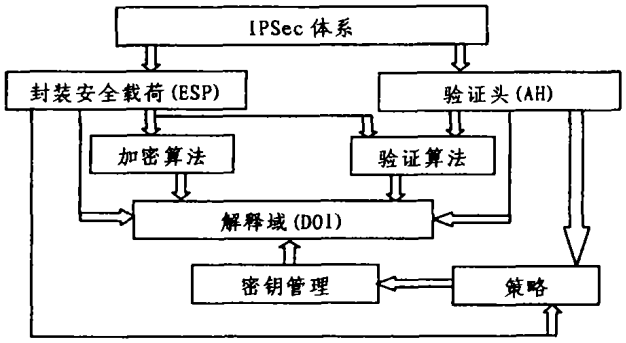

图2　IPSec 体系结构、组件及各组件间的相互关系

2)封装安全载荷 ESP 与 AH 相比，除了完整性检查和验证服务外，最主要的是增加了加密机制，它的加密算法至少要支持 CBC 模式的 DES 算法，实践中往往可以采用更强的加密算法如 IDEA、三重 DES、CDMF 算法等。

3)IKE 是 IPSec 默认的自动密钥管理协议，可以自动进行密钥的确定和分配。IKE 规定了自动验证 IPsec 对等实体、协商安全服务和产生共享密钥的标准，使得用户可以协商认证方式、加密方式和要使用的密钥(包括其生存时间)等。作为一种混合型协议，它是由 Internet 安全关联和密钥管理协议(ISAKMP)和两种密钥交换协议 OAKLEY 与 SKEME 组成。IKE 使用了两个阶段的 ISAKMP，此外还定义了5种交换模式。正是因为 IKE 的诸多特性，使得它能够实现机密性保护、完整性保护及身份验证、抵抗拒绝服务攻击、防止中间人攻击和实现完美向前保密(PFS)等。

5. 基于 IPSec 的移动 IP 安全体系框架

基于以上分析，这里提出了一个基于 IPSec 的移动 IP 安全体系框架，它不仅融合了移动 IP 和 IPSec，还采用了一些其他的安全措施，从而给移动 IP 环境以极大的安全性。

5.1　基本框架和简单的工作过程描述

本安全体系框架是针对 IPSec 环境中的安全威胁而提出的，因此下面描述一下本安全体系框架如何对付本文第三部分所分析的安全威胁。

首先给出一张与原先的移动 IP 的简要对比表(表1)，下面再进一步解释。

1)对于窃取机密攻击在移动 IP 中的两种主要形式，移动 IP 本身并没有采取任何对付措施。一般的策略是采用链路加密或端对端加密等方式对付，但数据链路层加密不能贯穿通信全程，在不同的通信介质交汇处易被攻击，而移动 IP 经过的链路比较多，因此最好的方法是采用端到端加密。这样，不论链路是有线还是无线，在网络的任一点上，数据均得到保护，而不是只能对网络的一部分有效；同时只在目的地对数据解密，既保证了安全性，又降低了传输时延。本框架中采用了 IPSec 的 ESP 通道模式提供端到端的加密功能。

表1

安全威胁		移动IP的对策	本安全体系框架下的对策
窃取机密攻击	被动偷听	无	IPSec的ESP通道模式实现端端加密
	会话窃取攻击		
恶意攻击(主要是拒绝服务攻击)	伪造注册请求	弱认证算法	IPSec的强认证算法
	TCP SYN Flooding	入口过滤技术和反向隧道	入口过滤技术和双向IPSec隧道
假冒攻击	重放攻击	采用时间标签或Nonce	IPSec中的序列号等验证机制
抵赖		无	IPSec数字证书
篡改		无	完整性检查

2)对于拒绝服务攻击中伪造注册请求的有效方法是对MN和HA之间交互的所有注册信息进行有效的强认证,移动IP中移动节点是采用Keyed MD5(Message Digest5)算法进行认证的,但这种认证很弱,而且没有密钥管理的策略。因此我们采用IPSec的强认证算法,而且用IKE提供完善的密钥管理技术。

对于TCP SYN Flooding,目前为止,还没有较好的技术方法解决,可以采用入口过滤技术(Ingress Filtering)[20]减轻威胁。但入口过滤技术的采用也带来了新的问题,因为一个连接在外地链路上的MN发出的数据分组以家乡地址为源地址,而路由器认为该地址应位于移动节点的家乡链路上,因此将其丢弃。对这个问题,移动IP采用了反向隧道技术[21,22]来解决:当移动节点注册时,可以申请反向隧道服务,将自己产生的数据分组进行隧道封装后再送到家乡代理,封装后的数据分组的源地址和目的地址在拓扑上都是正确的,不会被过滤机制丢弃。本安全体系框架也用到了入口过滤,但并不需要反向隧道技术,因为我们这里采用的是双向IPSec隧道(Bi-directional IPSec Tunnel),数据已经过封装,所以地址在拓扑上都是正确的。

3)对于重放攻击,移动IP的策略是移动节点为每一个注册消息标识域产生一个唯一值,使家乡代理能够知道下一次注册请求的值是多少。移动IP共定义了两种标识域的填写方法,第一种是利用时间标签,第二种采用Nonce。而我们的框架中采用了IPSec,其中的序列号等验证机制就能够抗重放攻击。

4)对于抵赖,移动IP没有办法,而本安全体系框架采用了IPSec数字证书以防抵赖。

5)对于篡改,移动IP也没有特别好的措施,而本安全体系框架提供了完整性检查以防篡改。

接下来简单描述一下在这个安全体系框架里移动IP的工作过程。这里,也和普通移动IP的工作过程作了比较,对比情况如表2。

表2

普通移动IP	新的安全体系框架下
1)MN在外地链路上监听FA的广播消息	1)MN在外地链路上监听FA的广播消息
2)MN发送注册请求给FA	2)MN通过DHCP、PPP的IPCP或手工配置来获得一个配置转交地址(Collocated Care-of Address)
3)FA转发MN的注册请求给HA	3)MN建立一条直接到HA的IPSec隧道
4)HA返回注册应答,通过FA转发给MN	4)MN发送注册请求直接到HA
5)这样在MN-FA和FA-HA之间分别建立起了隧道	5)HA发送回注册应答
6)FA在MN和HA之间中继所有的信息,从CN的信息先到HA,再送到FA,再到MN;从MN的信息送到FA,然后可以直接送到CN(可以不经过HA)	6)这样在HA和MN之间建立起了一条双向的IPSec隧道,以后MN和CN之间的所有通信信息都要经过这条隧道

需要指出的是,在上面的两种情况中,FA所起的作用并不完全相同:在普通移动IP下,FA需要转发(不是简单的中继)MN和HA之间的注册信息,而在新的安全体系框架下,就不需要FA的转发了。

5.2 用IKE穿越防火墙

在现在的安全设备中,防火墙是必不可少的,虚拟私用网(VPN)技术也用得越来越多,在采用VPN技术的环境中,移动节点如何穿越防火墙而又不牺牲网络的安全性是一个问题,对此,文[23]提出了用SKIP穿越防火墙,但这种方法在隧道上的每个数据包都加上了一个额外的SKIP头,这可能会更加加重网络的负担,此外在SKIP头中还标示了采用的加密和认证的算法,可能会更易受到攻击,因此本文论述一种用IKE穿越防火墙的方法,避免了以上的不足。之所以称之为用IKE穿越防火墙是因为这里认证方式、加密方式和要使用的密钥都由IKE来自动协商。该模型如图3所示(FW表示防火墙,其他缩写前面已经提过)。

为了简化讨论,这里忽略了MN和HA之间有多个防火墙的情况,而只考虑如图所示只有一个防火墙的情况(多个防火墙的情况可以依理类推),并假设HA和FW之间只需进行访问控制,即HA和FW之间只需采用AH就可以了。此外,MN和CN之间的端到端加密也可能存在,但它在MN和FW之间安全隧道的上层,下面的论述把它忽略掉,因为加入它们可能会使讨论变得较为繁琐、不清晰(事实上,加上它们就是在数据包上多加几个头部)。

注册过程的数据包格式如下:(以下RegRqst表示注册请求信息,RegReply为注册应答信息,src表示源IP地址,dst表示目的IP地址)

1)MN->FW:IP[src=COA,dst=FW]|ESP|IP[src=COA,dst=HA]|UDP|RegRqst

2)FW->HA:IP[src=FW,dst=HA]|AH|IP[src=COA,dst=HA]|UDP|RegRqst

3)HA->FW:IP[src=HA,dst=FW]|AH|IP[src=HA,dst=COA]|UDP|RegReply

4)FW->MN:IP[src=FW,dst=COA]|ESP|IP[src=HA,dst=COA]|UDP|RegReply

数据传输阶段的数据包格式如下(以MN发HTTP请求

为例):

1)MN 产生的原始包为:IP[src=MN,dst=CN]|TCP|HTTP(这里源地址 MN 为家乡地址)

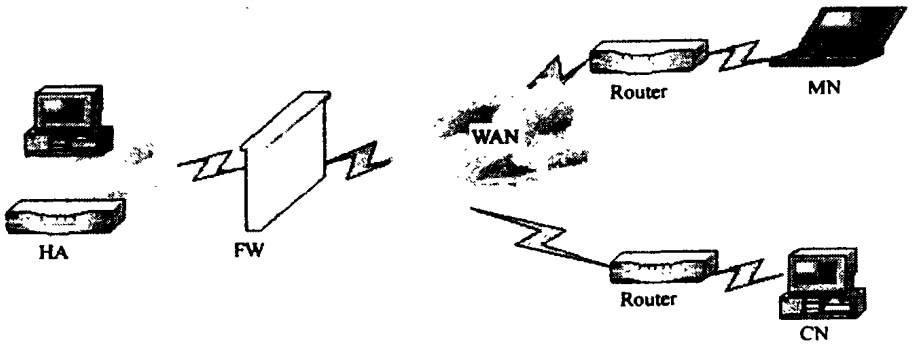

图3 用 IKE 穿越防火墙模型图

2)MN->FW: IP[src=COA,dst=FW]|ESP|IP[src=MN,dst=CN]|TCP|HTTP

3)FW->CN(经过认证、解密、恢复): IP[src=MN,dst=CN]|TCP|HTTP

4)CN->HA: IP[src=CN,dst=MN]|TCP|HTTP(下面该 IP 包被封装传送)

5)HA->FW: IP[src=HA,dst=FW]|AH|IP[src=HA,dst=COA]|ESP|IP|TCP|HTTP

6)FW->MN: IP[src=FW,dst=COA]|ESP|IP[src=HA,dst=COA]|ESP|IP|TCP|HTTP

7)最后 MN 得到数据包后认证、解密,恢复出:IP[src=CN,dst=MN]|TCP|HTTP

值得指出的是,这里我们对完全的双向 IPSec 隧道做了一个小小的变通,数据传到 FW 后并未传给 HA,而是直接路由给 CN,应该说这样做减轻了一些网络负担,而且未给网络添加额外的安全威胁。

5.3 本安全体系框架对移动 IP 的一点改变

采用本安全体系框架后,原有的移动 IP 协议的一些细节需要有所改变,在下面列出:

1)不再需要原来的安全手段(注册时的 MD5、时间标签和 Nonce),因为本安全体系已经提供了更强的安全措施。

2)不再采用原有的隧道方式,代之以 IPSec 的 ESP 通道模式建立双向 IPSec 隧道。

3)FA 的作用有所改变,MN 发出的注册信息不需要经过 FA 转发。

总结和展望 移动是未来网络技术的发展方向之一,作为一种可以在 Internet 上为移动计算机提供无缝漫游的协议,移动 IP 有着很好的前景,但安全问题也在困扰着它。本文提出了一个基于 IPSec 的移动 IP 安全体系框架,它克服了移动 IP 环境的安全威胁,存在着以下优点:1)为 IP 通信提供了强的认证。2)提供了完善的加密和完整性检查。3)用 IKE 自动协商进行密钥管理。4)可以穿越防火墙,支持 VPN。但同时,它也存在着缺点,最大的不足就是对实时应用(如视频点播等)来说,由于隧道需要加上许多头部,增添了开销,使得网络负担加重,影响实时性能;其次它依赖于 IPSec 技术的广泛部署;此外 IPSec 和 NAT 的共存还存在着一些问题。

总而言之,本文提出的安全体系框架能够为移动 IP 环境提供很强的安全性,有很好的优点,但也存在一些缺陷,需要进一步研究和完善,这正是下一步的研究方向。我们期待着在不久的将来,安全的移动 IP 能够从研究走向应用,为人们的生活服务。

参 考 文 献

1 Condell Z. Use of IPSec in Mobile IP. Internet Draft, 1997
2 Patil B, Narayanan R, Qaddoura E. Security Requirements/Implementation Guidelines for Mobile IP using IP Security. Internet Draft, 1999
3 Binkley, Jim, McHugh J. Secure Mobile Networking: Final Report. June 1999. http://www.cs.pdx.edu/research/SMN/index.html
4 Perkins C. IP Mobility Support. RFC 2002, Oct. 1996
5 Solomon J. Applicability Statement for IP Mobility. RFC 2005, Oct. 1996
6 James S. Mobile IP The Internet Unplugged. Prentice Hall publication, 1999
7 Perkins C. IP Encapsulation within IP. RFC 2003, Oct. 1996
8 Perkins C. Minimal Encapsulation within IP. RFC 2004, Oct. 1996
9 Generic S H. Routing Encapsulation (GRE). RFC 1701, Oct. 1994.
10 CERT Advisory CA-98. 01. "smurf" IP Denial-of-Service Attacks; January 5, 1998. http://www.cert.org/advisories/CA-98.01.smurf.html
11 CERT Advisory CA-97. 28; "Teardrop/Land" IP Denial-of-Service Attacks; December 16, 1997. http://www.cert.org/advisories/CA-97.28.Teardrop_Land.html
12 CERT Advisory CA-96. 21; TCP SYN Flooding and IP Spoofing Attacks, September 24, 1996. http://www.cert.org/advisories/CA-96.21.tcp_syn_flooding.html
13 Kent, Atkinson. Security Architecture for the Internet Protocol. RFC 2401, Nov. 1998
14 Thayer R, Doraswamy N, Glenn R. IP Security Document Roadmap. RFC2411, 1998
15 Kent S, Corp B, Atkinson R. IP Authentication Header. RFC2402, 1998
16 Kent S, Corp B, Atkinson R. IP Encapsulating Security Payload (ESP). RFC2406, 1998
17 Piper D. The Internet IP Security Domain of Interpretation for ISAKMP. RFC2407, 1998
18 Maughan, Schertler, Schneider, Turner. Internet Security Association and Key Management Protocol (ISAKMP). RFC 2408, Nov. 1998
19 Harkins, Carrel. The Internet Key Exchange (IKE). RFC 2409, Nov. 1998
20 Ferguson P, Senie D. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Jan. 1998
21 Montenegro G. Reverse Tunneling for Mobile IP. RFC2344, 1998
22 Montenegro G. Reverse Tunneling for Mobile IP, revised. RFC3024, 2001
23 Montenegro G, Gupta V. Sun's SKIP Firewall Traversal for Mobile IP. RFC2356, 1998