基于移动IPv6的IPSec安全体系

杜小丹[1]，张凤荔[2]，羊裔高[3]，鄢 涛[1]

(1. 成都大学计算机科学系 成都 610106; 2. 电子科技大学计算机科学与工程学院 成都 610054; 3. 成都信息工程学院 成都 610041)

【摘要】对IPSec协议族进行研究，分析了安全联盟、身份认证报头、封装安全负载和因特网密钥交换等协议的结构及其关键技术，并在此基础上提出了一种IPSec 的实现方案，可以有效地保障移动IPv6中数据传输的安全。在具体的实施过程中，可选用传输模式和隧道模式两种实现模式。传输模式只能用于发送方和接收方的系统都应用了IPSec的情况。在大多数情况下，采用隧道模式不需要对所用的系统进行任何修改。

关 键 词 IP安全; 安全联盟; 身份认证报头; 封装安全负载; 因特网密钥交换

中图分类号 TP393.08 文献标识码 A

On the Security Mechanism in Mobile IPv6

Du Xiaodan[1]，Zhang Fengli[2]，Yang Yigao[3]，Yan Tao[1]

(1. Department of Computer Science, Chengdu University Chengdu 610106;
2. School of Computer Science and Engineering, UEST of China Chengdu 610054;
3. Chengdu University of Information Technology Chengdu 610041)

Abstract The paper is dealing with the IPSec Protocols and analysing the structure and key technology of security association , authentication header , encapsulating security payload and Internet key exchange. On the basis of the discussion, it presents the practical design of IPSec, which can effectively ensure the security of data transmission in IPv6. In practice, there are two models can be selected, transmission model and tunnel model, transmission model can only be used on condition that IPSec is applied to the systems of the sender and the receiver. Therefore, in most cases, tunnel model is used because it is not necessary to make any change to the user's system.

Key words IP security; security association; authentication header; encapsulating security payload；Internet key exchange

1 移动IPv6带来的威胁

随着全球Internet用户的迅速增多，数以亿计的用户将通过移动方式接入Internet。因此移动IPv6的设计除了要能够满足节点的移动性外，还应保障通信的安全。但移动通信不同于固定网络的通信，由于其传输媒介的特殊性，使得在移动通信媒介中传输的数据更容易被干扰、监听和篡改，所以安全可靠的数据传输对于移动通信的发展有着至关重要的作用[1~6]。

由移动因特网协议版本6(Internet Protocol Version 6, IPv6)带来的安全问题主要有3类，一是拒绝服务型攻击，如阻止移动节点同其他节点通信或阻止通信者节点同其他节点通信；二是修改绑定缓存表项，在移动节点宿主代理、通信者节点或移动节点前一次访问的路由器上创建未授权的绑定缓存表项，从而发起主动攻击；三是泄露敏感信息，如泄露网络上作为宿主代理的节点等[4]。

收稿日期：2004 – 03 – 22
作者简介：杜小丹(1972 –)，女，硕士，讲师，主要从事计算机网络、多媒体技术方面的研究.

2 IPSec的安全机制

IP安全协议(IP Security Protocol, IPSec)有两个基本目标，一是保护IP数据包的安全，二是为抵御网络攻击提供防护措施[1, 2]。IPSec提供的是开放系统的安全框架，提供认证和加密两种安全机制。认证机制使IP通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭到改动；加密机制通过对数据进行编码来保证数据的机密性。这些机制都是在网络层上实现，对网络层以上的应用是透明的。

2.1 安全联盟

安全联盟(Security Association, SA)是IPSec中最基本的概念。认证报头(Authentication Header, AH)和封装安全负载(Encapsulating Security Payload, ESP)都要用到安全联盟，以后将会述及密钥交换(Internet Key Exchange, IKE) 的一个主要功能就是建立和维护安全联盟。安全联盟是两个应用IPSec实体间的一个单身逻辑连接，决定保护什么、如何保护以及谁来保护通信数据。SA提供的服务通过AH或者ESP两者之一来实现，若传输流中同时需要运用AH和ESP，则可以通过建立两个或者多个安全联盟来实现。两个实体之间的双向通信，也需要建立两个安全联盟来实现[4, 5]。

2.2 身份认证报头

认证报头是IPv6的扩展报头之一，它的作用是在网络应用中确认数据包来源的正确性，并提供密码验证或完整性测试。AH报头格式如图1所示，它通常插在IPv6报头和高一层有效数据之间。

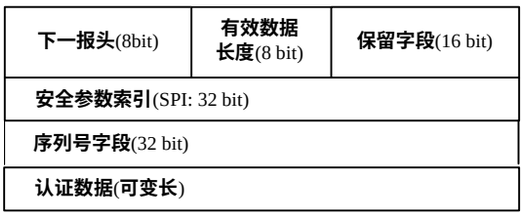

图1　AH报头格式

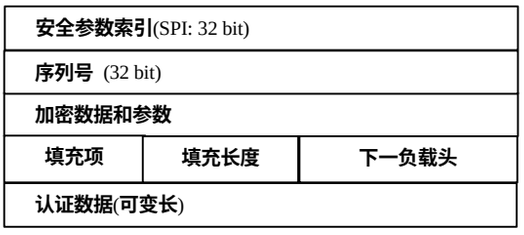

图2　ESP报头格式

AH的作用如下：

1) 为IP数据包提供强大的身份验证，可用于将实体与数据包的内容相关联；
2) 为IP数据包提供强大的完整性服务，验证IP数据包所承载的数据；
3) 如果在完整性服务中使用了公钥数字签名算法，可以为IP数据包提供不可抵赖服务；
4) 通过使用序列号字段来防止重放攻击。

在IPv6中协议采用AH后，因为在主机端设置了一个基于算法独立交换的秘密钥匙，非法潜入的现象可得到有效防止。秘密钥匙由客户和服务商共同设置。在传送每个数据包时，IPv6认证根据这个秘密钥匙和数据包产生一个检验项。在数据接收端重新运行该检验项并进行比较，从而保证了对数据包来源的确认以及数据包不被非法修改。

2.3 封装安全负载

AH报头解决了网络不被黑客潜入和数据包不被修改的问题。但AH并不对数据进行变形转换，数据对于黑客而言仍然是清晰的。为了有效地保证数据传输安全，在IPv6中有另外一个报头——封装安全负载，在网络层实现端到端的数据加密，以对付网络上的监听，其格式如图2所示。

ESP的作用主要有下面几点：

1) 通过加密提供数据包的机密性；
2) 通过使用公共密钥加密对数据来源进行身份认证；
3) 通过由AH提供的序列号机制防止重放攻击；
4) 通过使用安全性网关来提供有限的业务机密性。

ESP是一项在网络层进行加密的技术，对保证数据的安全性和完整性十分有效。AH和ESP可以单独使用，也可以结合使用。前者保证报文来自正确的来源并且未被调包，后者则保证报文不被第三方窃听。这两个扩展报头分别针对认证和加密服务，使IPv6协议的互联网安全性显著提高。

2.4 密钥交换

密钥交换是IPSec默认的自动密钥管理协议，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。

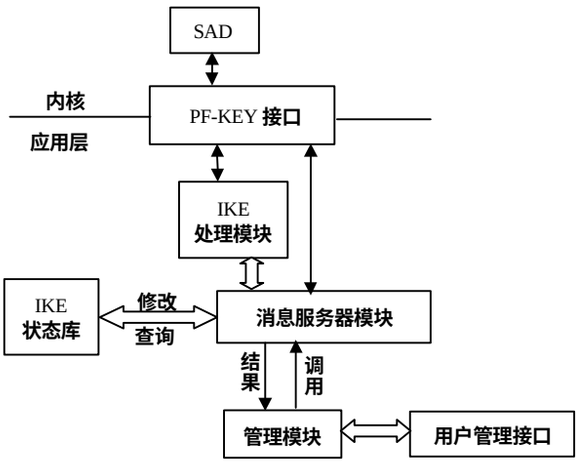

图3 IKE实现的基本框架

IKE通过两阶段的协商来完成SA的建立：在第一阶段，由IKE交换的发起方发起一个主模式交换，交换的结果是建立一个名为安全联盟和密钥管理协议(InternetI Security Association & Key Management Protocol, ISAKMP)的安全联盟，这个安全联盟的作用是保护安全协议协商SA的后续通信，主模式将SA的建立和对端身份的验证以及密钥协商结合起来，能抵抗中间人攻击。为了给ISAKMP SA提供一更快捷的方式，IKE还提供了另一种野蛮模式，它可使协商更为快捷，但抵抗攻击的能力较差，也不能提供身份保护。第二阶段可由通信的任何一方发起一个快捷方式的消息交换序列，完成用于保护通信数据IPSec SA的协商，这种模式为快速模式。

图3给出了IKE在Linux下实现的基本框架。整个系统按照功能划分为管理模块、处理模块、消息服务器模块等，IKE状态库模块可实现数据共享，PF-KEY协议作为内核和IKE守护进程的接口，提供IKE协议与内核安全联盟数据库(Security Association Data base, SAD)进行SA消息的传递。

3 IPSec模式的实现

IPSec可以作为一个独立的协议层次在IP层和数据链路层的中间实现，也可在IP协议内部实现。前一种实现不需要IP层的源代码，将特殊的IPSec代码插入到网络栈中，截获从IP栈向本地链路层接口传送的数据包，对这些数据包进行一些必要的安全性处理，然后再交给数据链路层。

3.1 IPSec实现方案

依据通信保密性要求，IPSec可在终端主机、网关、路由器或在两者中同时实施和配置，通常有3种实现方案，即与操作系统集成实施；插入网络层和数据链路层之间实施；在一个直接连接路由器的专用设备中实施。不论哪一种实施方案，完成IP安全保护的IPSec基本实现都是相同的。本文在分析研究IPSec协议族的基础上，提出一种IPSec实现方案，如图4所示。本方案中，实现IPSec包括IPSec协议处理、策略管理、IKE密钥交换和密码算法4个模块。其中IPSec协议引擎位于操作系统的内核中，实现安全协议AH和ESP，功能包括外出和进入数据包的处理、同因特网协议(IP)层和传输控制协议(Transfer Control Protocol, TCP)层的接口等，它是数据流程的核心；策略管理模块也位于操作系统的内核中，管理安全策略数据库(Security Policy Data base, SPD)和安全联盟数据库(SAD)，对数据包的安全保障起决定作用；IKE密钥交换用于动态管理SAD，功能包括IKE间的交互、同SPD和SAD的接口；密码算法是达到安全的基本工具，它至少应实现高级加密标准(Advanced Encryption Standard, AES)、数据加密标准(Data Encryption Standard, DES)、3DES等。

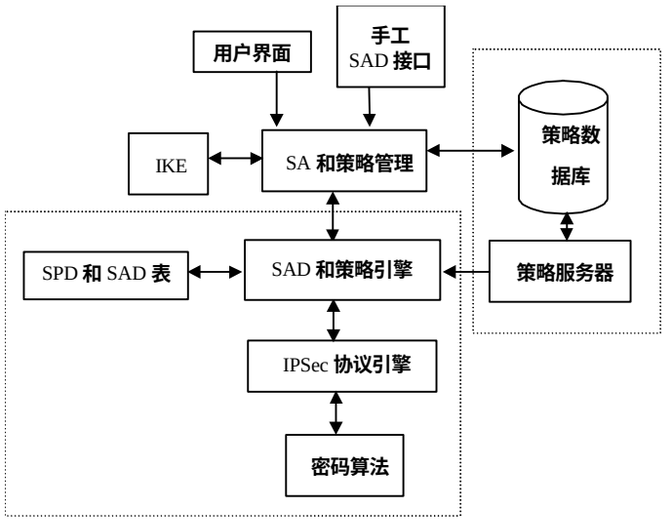

图4 IPSec实现方案

3.2 IPSec实现模式

IPSec协议支持两种实现模式，即传输模式和隧道模式。

3.2.1 传输模式的实现

在传输模式中，IP包头保持原样不变，只对IP数据部分进行加密。传输模式的优点是只需要对每个包加入几个字节。由于IP包头不加密，这种方式允许在网络中间节点上，根据IP包头信息进行特殊处理，网络上的其他设备可以识别此包的发送方和接收方，它可以通过观察发送方的IP包头，对通过的信息量进行分析。

3.2.2 隧道模式的实现

如果终端主机不支持IPSec，一般通过采用一个专门的设备(安全网关或路由器)来提供数据包的安全保障，而且该设备并不是数据包的始发点，它只对数据包进行加密保护，并把它传送到另一个目的地，对于这种情况，采用的就是IPSec的隧道模式。

在隧道模式中，安全网关为自己转发的数据包提供安全服务，即对数据包重新封装，在原来数据包的基础上增加一个IPSec头。这个头既可是AH头(但一般不使用)，也可是ESP头。ESP头对整个IP数据包进行封装，并作为IP报头的扩展将数据包定向到安全网关。图5是IPSec隧道模式下的IP数据包格式的一个实例。

IP头	ESP头	原来的IP头	网络载荷

图5　隧道模式下的IP数据包式示例

可以看到在隧道模式下的IP数据包有一个内部头和一个外部头两个IP头。其中，内部IP头由始发点的主机创建，而外部IP头由提供安全服务的设备根据具体情况创建。这样经过IPSec隧道模式安全处理的数据包，在到达隧道的另一端时，再按照要求去掉外部IP头，然后把数据包起始点创建的数据包传送到目的地。

传输模式是由主机使用而不是网关使用，网关甚至可以根本不支持传输模式。其优点在于额外开销较小，缺点是无法对可变字段进行保护。隧道模式的主要优点是在实现IP安全性的过程中，不需要对用户系统进行任何改变，还可避免传输模式中网络攻击者对信息流量的分析，使网络攻击者只能跟踪隧道的端点，甚至在发送方与接收方即为隧道的两端点的情况下，网络攻击者也不能判定隧道内包的发送方和接收方。但是，隧道模式带来了额外的开销。一般情况下，传输模式只能用于发送方和接收方的系统都应用了IPSec的情况。因此，在大多数情况下，IPSec采用隧道模式，这种方式不需要对所用的系统进行任何修改。

4 结 束 语

本文提出的IPSec的实施方案，在IP层上对数据包进行高强度的安全处理，提供了诸如数据源地验证、无连接数据完整性、数据机密性、抗重播和有限业务流机密性等安全服务和密钥管理，能为企业局域网与拨号用户、域、网站、远程站点以及Intranet之间的通信提供强有力且灵活的保护，使得各种应用程序可以享用IP层提供的安全服务和密钥管理，而不必设计和实现自己的安全机制。可以预料，IPSec必将成为网络安全的产业标准。

本文研究工作得到电子科技大学青年基金(No.YF020202)资助，在此表示感谢！

参 考 文 献

[1] Kent S, Atkinson R. Security architecture for the Internet protocol[S]. RFC2401, 1998

[2] Deering S, Hinden R. Internet protocol, version 6(IPv6) specification[S]. RFC2460, 1998

[3] 王　路, 袁宏春, 万里冰. 基于IP的点对点分布式VPN系统[J]. 电子科技大学学报, 2004, 33(1): 67-70

[4] 夏士雄, 王东明, 常　征. 移动IPv6与网络安全[J]. 计算机工程与设计, 2002, 24(12): 13-16

[5] 王　玲, 钱华林. IPv6的安全机制及其对现有网络安全体系的影响[J]. 微电子学与计算机, 2003, 26(1): 50-51

[6] 沈　莉. IPv6安全协议研究[J]. 电子科技大学学报, 2002, 31(1): 72-75

编　辑　熊思亮