用IPSec提高网络安全性

刘波 黄文学 （南京河海大学网络中心 210098）

摘要：IPSec是作用于IP层的安全协议，可以支持IP级所有流量的加密和认证。IPSec采用鉴别报头（AH）、封装安全有效负荷（ESP）和密钥管理协议来进行IP层的加密与认证。IPSec提供对跨越LAN/WAN，Internet的通信提供安全性。本文介绍了一个基于IPSec的电子商务中网上支付系统的设计。

关键词：IPSec AH ESP IKE 密钥

1 前言

随着网络的高速发展，TCP/IP协议成为大多数计算机和网络供应商所支持的事实标准。网络安全也越来越受到人们的重视。由于TCP/IP发展的最初并没有考虑到安全性，所以TCP/IP存在着很多安全漏洞。IP的最新版本(IPv6)克服了一些IPv4(IPv4是已经存在了20年的协议)安全方面的局限。IP安全协议(IPSec)是IPv6的一部分。虽然IPv6还不成熟，但IP安全机制是独立定义，不需要依靠IPv6部署。所以安全IP的功能首先被广泛使用，比IPv6先流行起来，因为对IP层的安全需求远比增加IPv6功能的需求多得多。

2 IPSec简介

IPSec是一个开放式协议的基本框架,用以保证IP网络上数据通信的安全性。基于Internet工程任务组(IETF)开发的标准，IPSec保证了公共IP网络上数据通信的机密性、完整性和真实性，提供了全网范围内可用的灵活的安全策略解决方案。

在IPSec提出之前，人们通常采用安全套节字层(SSL)为WEB和其他应用程序提供应用层加密，SSL只为那些采用它的应用软件提供数据机密性保护，为了SSL能有效地工作，所有的系统和应用软件都必须加载SSL。而链路层加密在当今几乎不起作用，IP层的认证和加密成为网络安全发展的需求。IPSec正是作用于IP层，可以对所有IP级的通信进行加密和认证，正是这一点才使IPSec可以确保包括远程登录、客户/服务器、电子邮件、文件传输及Web访问在内多种应用程序的安全。

3 IPSec的优点

如果在路由器或防火墙上执行了IPSec，它就会为周边的通信提供强有力的安全保障。IPSec有以下优点：

(1) IPSec在传输层之下，对于应用程序来说是透明的。当在路由器或防火墙上安装IPSec时，无需更改用户或服务器系统中的软件设置。即使在终端系统中执行IPSec，应用程序一级的上层软件也不会被影响。

(2) IPSec对终端用户来说是透明的,因此不必对用户进行安全机制的培训。

(3) 如果需要的话,IPSec可以为特定用户提供安全保障，这样做就可以保护企业内部的敏感信息。

4 IPSec的安全协议

IPSec作为安全网络的长期方向，是基于密码学的保护服务和安全协议的套件。IPSec提供三种协议来保护通过公有或私有IP网络来传送的私有数据: 鉴别报头(AH)提供IP数据报完整性、数据源认证以及防止重发；封装安全有效负荷(ESP)除了提供完整性、数据源认证以外，还提供机密性；IETF选择IKE (Internet Key Exchange)作为IPSec配置安全协定的标准方案。

IPSec有两种操作模式：传输模式和遂道模式（如图1)。这两种模式下，AH和ESP都可以工作，但ESP具有

不同的ESP模型，在传输模式下，只有IP数据被加密，而没有加密IP报头和选项。传输模式具有较好的性能，因为编码通常具有较高的CPU开销。在隧道模式下，整个原始的数据报都被加密，成为一个新的IP包，这时，路由器代表主机完成加密过程，源路由器加密数据包并沿着隧道转发，目的路由器解密数据包并转发到相应的目标系统。面对隧道模式，入侵者只能确定隧道的终端结点，而不是数据包的实际源和目的地址。

图 1　传输模式与隧道模式

5　IPSec在电子商务中的应用设计

在电子商务繁荣发展的今天，网上支付系统的安全性引起了人们的普遍重视。在通常的电子交易中总会有两方：付款方和收款方，商品和货币就在他们之间交换；此外至少还有一个金融机构，它的功能为把交易中传送的电子货币和实际的货币联系起来。在大多数现有的电子支付系统中，金融机构一般分为两部分：发起者（由客户使用的银行）和获取者（由银行使用的银行）。网上银行卡交易就是典型的电子支付系统。

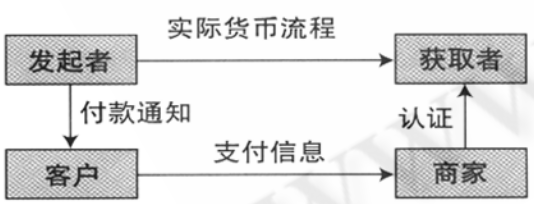

图 2　银行卡交易过程

支付信息的传输和认证可以说是支付系统中最为重要的一个环节，其安全性是商家和客户最关心的方面。在这里我们采用IPSec的隧道模式来确保支付信息的安全传输，隧道模式的优点是两个隧道端点之间的数据是安全的，而不管最终目的地如何。针对隧道模式配置IPSec时，网络之间所有通信都是安全的，而不要求在各个计算机上配置IPSec。目前，Windows 9x/NT、Solaris和其他一些UNIX平台的IPSec软件均已发布，Linux目前仍在测试当中。基于IPv6的IPSec for Linux目前仍在测试当中。有几家销售商正在致力于在路由器中实现IPSec。Windows 2000为实现IPSec服务提供了基于策略的管理能力，为实现隧道模式，要求“路由和远程访问”（Routing and Remote Access）服务。

在Windows 2000中启用隧道模式的步骤如下：

（1）打开“IP安全性策略管理”（IP Security Policy Management）。

（2）在详细资料窗格中，用鼠标右键单击你想修改的策略，然后单击“属性”（Properties）。

（3）单击你想修改的规则，然后单击“编辑”（edit）。

（4）在“隧道设置”（Tunnel Setting）选项卡下，单击“隧道端点由这一IP地址指定”（The tunnel endpoint is specified by this IP Address），然后指定隧道端点的IP地址。

Windows 2000支持建立多个隧道模式连接，但是每次只能有一个隧道。各个隧道连接都要求独立的规则。下面以商家和银行系统的保密通信过程来说明IPSec的应用（其中路由器Ra和路由器Rb已配置了IPSec，IP隧道创建于两个路由之间）：

① 商家局域网的一台计算机A收到客户的信用卡信息后，试图与银行局域网中的计算机B通信，A发送一个IP包，目的地址是银行局域网的主机B。

② A一侧的路由器——边缘路由器Ra接收到数据包，Ra把所有出去的包过滤，如果这个从A到B的包需要使用IPSec，Ra就进行IPSec的处理，并把网包打开，添加外层IP包头。这个外层包头的源地址是防火墙，而目的地址可能是主机B的网络边缘的防火墙，对于这种情况，网络入侵者只能确定隧道的终端节点，而不是数据包实际的源和目的地址。

③ 路由器Ra查寻它与B一侧的路由器——边缘路由器Rb之间的IPSec是否存在，如果没有，它即向IKE提出申请。如果两个路由器之间已有共享IKE SA（安全协定）存在，IPSec SA会立即产生，否则，必须先建立一个，之后才可以进行IPSec SA协商。

④ IKE会话激活后，两个路由器就在加密算法（如DES）和鉴别算法（如MD5）上取得了一致，并获得共享的会话密钥。这时，路由器Ra就可以加密A的数据包，放入一个新的IPSec分组并发送到路由器Rb上。

（下转第77页）

(上接第 37 页)

⑤路由器 Rb 收到 IPSec 分组后，查寻 IPSec SA，进行相应的处理并解开原始的数据包，转发给 B。至此，IPSec 建立了 A 与 B 之间的安全通信过程。

IPSec的一个最基本的优点是它可以在共享网络访问设备，甚至是在所有的主机和服务器上完全实现，这在很大程度上避免了升级任何网络相关资源的需要。在客户端，IPSec架构允许使用在远程访问介入路由器或基于纯软件方式使用普通MODEM的PC机和工作站。在客户支付信息的传输过程中同样可以采用 IPSec 实现安全传输。

6 结束语

综上所述，IPSec 可以保证局域网、专用或公用的广域网及 Internet 上信息传输的安全。相信 IPSec 在保证 Internet 上各分支办公点的安全连接、通过外部网或内部网建立与合作伙伴的联系，以及提高电子商务的安全性方面会发挥重要的作用。■

参考文献

1 *RFC2401. Security Architecture for the Internet Protocol[S] November 1998 全文。*

2 *RFC2402. IP Authentication Header [S] November 1998全文。*

3 *RFC2403. IP Encapsulating Security Payload (ESP) [S] November 1998 全文。*

4 *RFC2409. The Internet Key Exchange (IKE) [S] November 1998全文 。*