# 嵌入式 VPN 模型[1]

徐国爱 杨义先 胡正名
(北京邮电大学信息安全中心 北京 100876)

**摘 要** 该文在研究 IP Sec 和 TCP/IP 软件体系结构的基础上，给出了嵌入式 VPN 的模型。该模型可以在不依赖于操作系统网络实现细节的情况下，嵌入 IP Sec 安全机制，从而可以大幅度降低构建 VPN 的成本和周期。

**关键词** 网络安全，VPN, IP Sec, 最大传输单元
**中图号** TN919.3

## 1 引 言

Internet 以 TCP/IP 协议为通信基础，但由于 TCP/IP 协议最初的设计是基于互相信任的通信基础上的，没有考虑安全问题，从而使协议自身存在安全脆弱性。TCP/IP 协议安全脆弱性主要表现在：首先是缺乏有效的认证机制，没有验证通信双方真实性的能力；其次是缺乏保密机制，不能保护网上数据的隐私性；再次是数据在传输过程中有可能被篡改，不能提供对数据流的完整性保护。此外，协议自身设计的某些细节和实现中的一些安全漏洞也会引起各种攻击[1,2]。

为了保护网络数据尤其是私有信息传输的安全性，以往采用的做法是建立企业私有网络，以避免在公共网络上传输数据。但这种做法的问题在于，建立私有网络成本高，建设周期长，灵活性差。VPN(Virtual Private Network) 就是为了解决这个问题而产生的。它通过加密和验证网络流量来保护在公共网络上传输的私有信息不会被窃取和篡改。从而在并不安全的 Internet 上开辟了一个安全的私有网络。

在 TCP/IP 协议族的 IP 层 (网络层) 实现安全机制可以对任何传送协议和应用服务提供“无缝”安全保障。IP Sec 是一组基于 IP 层的安全协议，它也是目前唯一能为任何形式的 Internet 通讯提供安全保障的协议。

## 2 IP Sec 体系结构

IP Sec 是在 IP 包级为 IP 业务提供保护的安全协议标准，其目的是把密码学的安全机制引入 IP，通过使用现代密码学的方法支持保密和认证服务，使用户能够有选择的使用并得到所期望的安全服务。而且，这些安全机制正确实现时，它不对未采用这些机制的其它 Internet 部件有所负面影响。

2.1 IP Sec 的组成 IP Sec 将多种安全技术结合形成一个完整的安全体系，IP Sec 由两大部分三类协议组成：IP Sec 安全协议 (认证头 (AH)/ 封装安全有效负载 (ESP)) 和密钥管理协议 (Internet Key Exchange)[1,3,4]。IP 安全协议 AH 和 ESP 定义了如何通过在 IP 数据包中增加安全扩展头和字段来保证 IP 包的机密性、完整性和真实性；密钥管理协议可以实现不同安全需求的安全策略的协商，和 IP 安全协议一起构建起 IP 层安全体系结构的框架，保护所有基于 IP 的服务或应用。

2.2 两个重要概念 安全联盟 (SA) 和隧道技术 (Tunneling) 是 IP Sec 协议组中两个最为核心的概念。SA 是基于一个单向传输的，它将一个单向传输所需要的各种安全参数有机地整合在一个数据结构，由密钥管理协议进行维护。安全联盟至少包括加密算法、认证算法、密钥、密

[1] 2001-04-13 收到，2001-08-10 定稿
国家重点基础研究发展规划项目 (编号：G1999035805)，国家杰出青年基金项目 (编号：续 69425001)，国家自然科学基金项目 (编号：69882002)

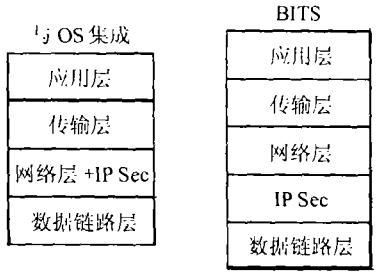


图 1　两种不同的 IP Sec 实施方案

钥生命期和安全联盟的生命期等。安全协议 AH 和 ESP 的实施就依赖于具体的相关的安全联盟。

隧道技术就是把一个包封装在另一个新的数据包里面，整个源数据包作为新的有效负载部分，并在前面添加一个新的 IP 头，其外部的目的地址通常是 IP Sec 的防火墙、安全网关或路由器。通过隧道技术可以对外隐藏内部数据和网络细节，对 IP Sec 而言，IP 隧道的直接目标就是对整个 IP 包提供完全的保护。

2.3 IP Sec 的实施　IP Sec 可在终端主机上、网关 / 路由器或两者中间进行实施和配置，具体选择与用户对安全保密需求有关。IP Sec 在主机上实施分成两类情况：一是与操作系统集成，一是在网络层与数据链路层之间实施，后者也称为堆栈中肿块 (BITS)[1]。

与操作系统集成的方法是将 IP Sec 当作网络层的一部分来实现，它的优点是与操作系统紧密结合实施的效率高，支持所有的 IP Sec 模式；缺点就是需要提供较多操作系统网络实现细节，而对一般的商用操作系统来说，这点是很难做到的。BITS 方案的优缺点基本与前者相反。

## 3 IP Sec 在 IP 层的嵌入

IP Sec 的与操作系统集成的实现方法本身就是 IP Sec 在 IP 层的嵌入实现方法。但本文以下讨论的嵌入方法特指利用操作系统驱动程序机制，截获 TCP/IP 软件 IP 协议栈的几个关键接口，嵌入 IP Sec 的安全协议，从而在绕过操作系统 TCP/IP 软件实现细节的基础上在主机上实现 IP Sec 安全功能的一种模型。

3.1 操作系统中的 TCP/IP 软件结构　TCP/IP 协议软件是操作系统中的一部分 [5]。它使用进程的概念使各个协议软件模块独立，以便于理解、设计和修改，以协议堆栈的形式在系统内存中存在。每个协议软件模块独立执行，并提供明确的并行的机制。TCP/IP 软件在系统中包括有：IP 进程、TCP 输入进程、TCP 输出进程等。从概念上来说，TCP/IP 软件包含有以下几个的层次：应用层、传输层、网络层、网络接口层和硬件。其中网络接口层负责硬件的封装，通过它，IP 层的数据包可以完成最终的发送过程，来自硬件的数据可以封装成具有指定网络设备特性的 IP 包，从而提交给 IP 层和最终到达的应用程序端口。不同功能层次网络分组在 TCP/IP 协议栈间传输示意过程如图 2 所示：

3.2 IP 数据包的接收与发送过程　IP 协议栈是 TCP/IP 协议软件中最核心的，它完成上层数据包的组装、分片、路由选择等多项基本功能，IP 包是 IP 协议栈和网络接口层交互的数据格式。IP 数据包到达网络接口层之前可能需要分片，而网络接口层提交数据包时则可能需要将分片的数据包进行重组。我们将 IP 协议栈提交 IP 包给网络接口层的操作接口叫做 IP 数据包的发送过程，IP 协议栈从网络接口层接收和重组 IP 包的过程叫做 IP 包接受过程。

如果一个主机连接在两个 MTU(网络最大传输单元) 不一样的网络上，IP 协议栈发送过程之前经常需要对数据包进行分片处理。但是，我们这里讨论的 VPN 实施主体是终端主机，所以很多时候只与一个网络相连，同时在这里我们也假定主机不与不同 MTU 的网络相连 (实际上这种假设并不失去应用的广泛性)，因而，主机 IP 协议栈的数据发送过程相当于不存在数据包

分片问题；因为 IP 包在传输过程可能经过更小 MTU 的网络，所以 IP 包接收过程仍然可能需要数据包重组。从而可以理解为，主机 IP 包接收接口所接收的 IP 包就是源主机所 IP 发送过程所发送的 IP 包，反之亦然。

3.3 IP Sec 在 IP 层部分嵌入 通过操作系统的驱动程序 (网卡驱动程序即是一种) 的设计机制可以实现对 IP 协议栈 IP 包接收和发送过程接口的截获，这相当于在 IP 协议栈原有的 IP 发送和接收操作之前可以嵌入适当的数据处理操作，这是 IP Sec 在网络层嵌入实现的基础。将 IP Sec 的加密和认证操作嵌入到 IP 协议栈的输出接口， IP Sec 的解密和验证操作嵌入到 IP Sec 的输入接口，而通信双方主机的 IP 包接收接口所接收的 IP 包就是对方主机 IP 发送过程所发送的 IP 包，这样就可以使 IP Sec 的安全协议在 IP 层部分接口嵌入，实现 IP Sec 的安全策略，这就是 IP Sec 在 IP 层的部分嵌入，如图 3 所示：

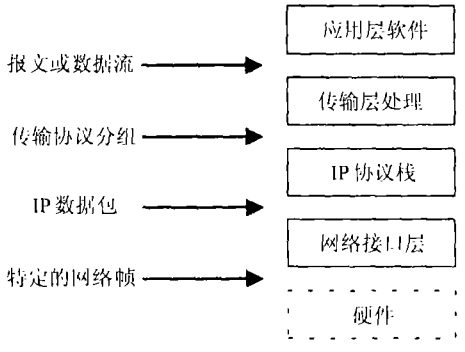


图 2 网络分组在不同协议栈间的传输

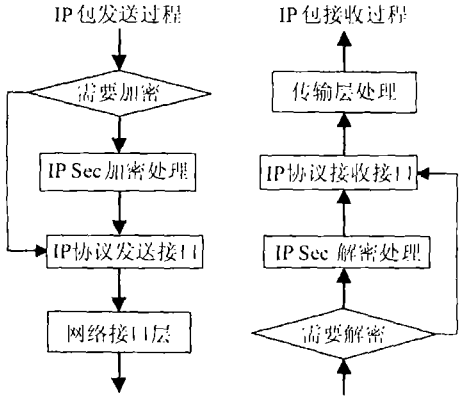


图 3 IP Sec 在 IP 层部分嵌入

3.4 MTU 问题 IP 包发送接口所发送的数据包相当于是经过分片之后的数据包，加密认证处理之前，它的最大长度不操作 MTU[2,5]，可以顺利提交给网络接口层进而发送出去。而 IP 数据的加密和认证必然带来数据的扩展，一旦新 IP 包长度超过 MTU，网络接口层肯定不能将 IP 包发送出去 (数据分片过程已在 IP 层处理过)，甚至可能导致系统崩溃。

事实上，TCP/IP 协议软件初始化的时候，操作系统会通知 TCP/IP 相关协议栈系统当前所连接各网络的 MTU，为 TCP/IP 正常工作做准备。通过类似 IP 包接收和发送过程的截获手段，可以欺骗 TCP/IP 协议栈，将操作系统通知的 MTU 减少，使得即使加密扩展，也不影响 IP 的正常分片操作过程，从而解决 MTU 问题进而实现 IP Sec 在 IP 层的部分嵌入。

## 4 嵌入式 VPN 模型的意义

虽然嵌入式 VPN 模型要求主机所有连接的网络的 MTU 相同，但事实上绝大多数终端主机、甚至网关都符合这个条件，因而这种模型具有很广大的实际应用环境。

4.1 可以实现 IP Sec 的全部安全功能 IP 包的发送过程是包含完整的 IP 包结构，在妥善解决 MTU 问题的基础上，首先对整个 IP 进行认证和加密处理是没有问题的；其次，通过分析 IP 包的头信息和数据信息可以提取传输层数据和头信息，从而实现通道模式的认证和加密，从而可以实现 IP Sec 的所有情况的安全机制，保证 IP 包的保密性、完整性和真实性。

4.2 对操作系统透明 嵌入式 IP Sec 实现机制的关键技术在于通过操作系统标准的驱动程序开发机制，截获 TCP/IP 协议栈的 IP 包接收和发送接口，而驱动程序开发机制是商用操作系统基本的接口功能，比如 Windows 系列操作系统。这样 IP Sec 的嵌入就可以完全避开操作系统网络实现的细节，对操作系统透明，几乎不依赖于操作系统开发商。

4.3 实现方式灵活 从嵌入式 IP Sec 的实现过程可以看出，它的加解密部分即适合于一般的硬件方式，也可接收纯粹的软件方式。同时，这种方式特别适合于终端主机上实现，这样往

往可以实现对已有 VPN 系统的扩充，显然，如果网关所连接的网络的 MTU 一致的情况下，嵌入式 IP Sec 也适合网关上实现。

## 5 结 束 语

事实上，IP Sec 已成为 VPN 实现的事实标准，怎样降低 IP Sec 实现的成本，这对普及 VPN 的使用、提高网络的安全性始终具有相当重要的意义。嵌入式 IP Sec 可以在保证 IP Sec 实现全部安全功能的同时，又不依赖于操作系统的网络实现细节，显然可以大幅度降低成本并提高 IP Sec 实现的灵活性。截止定稿时间，作者与其开发组已完成基于 Windows 嵌入式 IP Sec 的详细设计。

## 参 考 文 献

[1] N. Doraswamy, D. Harkins, IPSec: the new security standard for the internet, intranets, and virtual private networks, 1999.

[2] M. B. Steven, Security problem in the TCP/IP protocol suite, Computer Communication Review, 1989, 19(2), 32-4.

[3] S. Kent, R. Atkinson, RFC2406 IP Encapsulating Security Payload (ESP), November 1998, http://www. ietf. org/html. charters/ipsec-charter. html

[4] S. Kent, R. Atkinson, RFC2402 IP Authentication Header(AH), November 1998, http://www. ietf. org/html. charters/ipsec-charter. html

[5] Douglas E Comer, David L. Stevens 著，赵刚等译，用 TCP/IP 进行网际互连，北京，机械工业出版社，2000.

## A MODEL EMBEDDED WITH VPN

Xu Guoai Yang Yixian Hu Zhengming

(*Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

**Abstract** In this paper, the system framework of IP Sec and TCP/IP software is researched, and a security model embedded with VPN is given. The model can realize the IP Sec without detail of OS TCP/IP, and decrease the cost of VPN.

**Key words** Network security, Virtual private network, IP Sec, Maxium transport unit

徐国爱： 男，1972 年生，博士生，研究方向为密码学与网络安全.
杨义先： 男，1961 年生，博士生导师，研究方向为编码密码学与信息安全.
胡正名： 男，1931 年生，博士生导师，研究方向为编码密码学.