第32卷 第22期 计 算 机 工 程 2006年11月
Vol.32 No.22 Computer Engineering November 2006
·网络与通信· 文章编号：1000—3428(2006)22—0107—04 文献标识码：A 中图分类号：TP393.08

IPSec协议实现及其现状分析

马士超[1,2]，王贞松[1]
（1. 中国科学院计算技术研究所，北京 100080；2. 中国科学院研究生院，北京 100039）

摘 要：IPSec协议是IETF开发的一组用来保障TCP/IP网络上数据安全传输的协议套件，目前存在多种不同的软件实现与硬件实现方案。该文对这些实现方案进行了综合分析，从安全性、实现复杂度、平台无关性等方面进行比较，并且对IPSec实现的未来作了展望。
关键词：IPSec；BITS；BITW；OS集成；

Implementation and Analysis of IPSec Protocol

MA Shichao[1,2], WANG Zhensong[1]
(1. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080;
2. Graduate School, Chinese Academy of Sciences, Beijing 100039)

【Abstract】 IPSec is a set of protocols developed by IETF to protect data transport on TCP/IP networks. At present, there exist many kinds of software implementations and hardware implementations. This paper analyses these implementation schemes, compares them in security, complexity, platform independence. The future of implementation of IPSec is forecasted at the end.
【Key words】 IPSec; BITS; BITW; OS Integration

Internet缺乏安全性是不争的事实，人们试图通过设计各种基于TCP/IP网络层次结构的安全协议来增强IP网络的安全性。例如基于应用层的PGP，PEM，S/MIME；基于传输层的SSL/TLS；IPSec[2]是基于网络层的安全协议。IPSec相对于其它协议的优点在于它是在TCP/IP协议的关键点实现安全机制，从而有效保障了高层各协议的安全性，减少了在TCP/IP网络上部署安全的复杂性。

目前对于IPSec协议有多种实现。例如Windows2000以上的Windows系列操作系统都提供对IPSec的支持；Linux的2.4版本本身虽不具备IPSec功能，但是Freeswan等开源项目使得Linux的2.4版本可以支持IPSec，Linux的2.6版本目前已经内嵌了IPSec的功能[3]；KAME等开源项目提供针对各种BSD版本的IPSec实现方案。

Motorola，Cavium以及Hifn，AMCC都提供IPSec的ASIC/FPGA实现。

1 IPSec协议概述

IPSec是IETF提出的IP安全标准[2]，它在IP层上对数据包进行安全处理，提供数据源验证、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。各种应用程序完全可以享用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，因此减少了密钥协商的开销，也降低了产生安全漏洞的可能性。IPSec可连续或递归应用，在路由器、防火墙、主机和通信链路上配置，实现端到端安全、虚拟专用网络(VPN)、Road Warrior 和安全隧道 技术[1]。

IPSec协议由核心协议和支撑模块组成。核心协议包括AH(验证头)与ESP(封装安全载荷)；支撑部分包括加密算法，HASH算法，安全策略，安全关联，IKE密钥交换机制[4~7]。结构如图1所示。

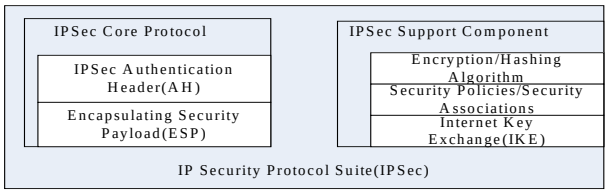

图1 IPSec协议总体结构

2 IPSec实现策略

无论IPSec应用于VPN还是端到端的安全，其实现机制均可以分为3种：OS集成，BITS(Bump in the Stack)与BITW(Bump in the Wire)。

OS集成方案在主机实施与路由器实施情况下都可以应用。在这种方式下IPSec与操作系统集成在一起。由于IPSec是一个网络层协议，因此可以当作网络层的一部分来实现。IPSec层需要IP层的服务来构建IP头。

IPSec与操作系统集成的优点主要有：(1)由于IPSec与网络层紧密集成在一起，因此它更有利于诸如分段、PMTU和用户场景之类的网络服务；(2)在每个数据流的级别提供安全服务更为容易，因为密钥管理、基本IPSec协议和网络层可以无缝集成在一起；(3)支持所有的IPSec模式。

但对提供VPN和内联网解决方案的公司而言，OS集成方案有一个不容忽视的缺陷：限制提供高级方案的能力。

BITS将IPSec插入网络层和数据链路层之间。其示意如图2所示。

基金项目：国家“973”计划基金资助项目(2004CB318202)；中科院计算所知识创新科研基金资助项目(20056210) ;国家自然科学基金资助项目(60303017)
作者简介：马士超(1978－)，男，博士生，主研方向：安全芯片设计，SOC以及嵌入式系统；王贞松，教授、博导
收稿日期：2006-01-21 **E-mail：**scma@ict.ac.cn

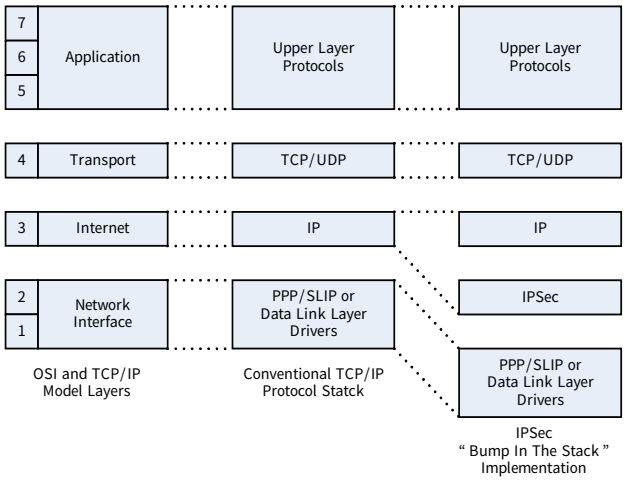

图 2 IPSec 的 BITS 实现示意图

这种实施方案最大的问题就是功能的重复。它要求实现大部分网络层特性，比如分段和路由表。其优点是只需一次实施，就可提供完整的方案。

BITW 在逻辑上等同于 BITS 实施方案。在这种实现中，IPSec 的实现在一个设备中进行，该设备直接接入路由设备的接口。该设备一般不运行任何路由算法，而仅是用来保障数据包的安全。其结构如图 3 所示。

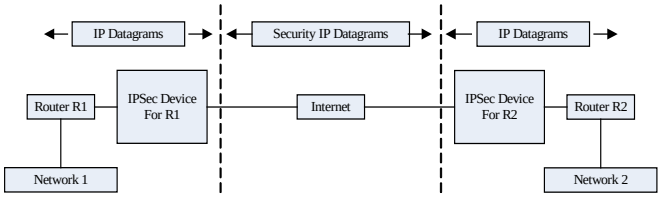

图 3 IPSec 的 BITW 实现示意图

3 软件实现分析

IPSec 的软件实现无论其是否与操作系统进行集成，都是与操作系统相关的。下面分别就 Windows、Linux 与 *BSD(Berkeley Software Distribution)等 3 类操作系统的 IPSec 实现进行分析。

3.1 基于 Windows 的 IPSec 软件实现

3.1.1 OS 集成方案

集成在 Windows 中的 IPSec 实现以服务的形式提供数据安全与认证。Windows 系统中的 IPSec 包含 3 个组件：策略代理，IKE 模块和 IPSec 驱动。这 3 个模块通过与 Windows 中的 TCP/IP 驱动和 cryptoAPI 进行交互来提供 IPSec 的所有功能。其中策略代理负责 IPSec 策略的获取与分发，IKE 模块在策略代理的驱动下进行安全关联的协商。Windows 系统中采用的认证策略包括：Kerberos(一种网络认证协议)，证书与预共享密钥。

3.1.2 NDIS 实现

Windows 操作系统提供了多种截获数据包的机制。内核模式的包过滤机制主要有 TDI 过滤、NDIS Intermediate 驱动、Filter-Hook 驱动、Firewall-Hook 驱动以及 NDIS Hooking 过滤驱动等几种机制。NDIS Intermediate 驱动介于网络设备的驱动程序(Miniport Driver)与协议驱动(Protocol Driver)之间，对于 Miniport 驱动表现为 Protocol 驱动，对于 Protocol 驱动表现为 Miniport 驱动，可以对网络层的数据进行处理，因此非常适合用来进行 IPSec 处理。基于 NDIS 的 IPSec 的实现一般采用如图 4 所示的结构。

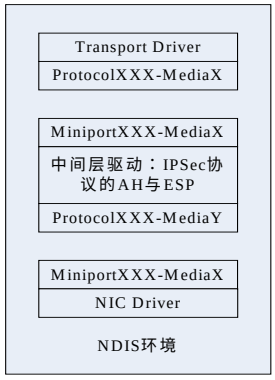

图 4 基于 NDIS 的 IPSec 实现

3.2 基于 Linux 的 IPSec 软件实现

Freeswan 与 USAGI 是两个针对 Linux 操作系统进行 IPSec 实现的开源组织。他们的 IPSec 实现都提供对 IPv4 和 IPv6 两种版本的支持，并且随着内核技术的发展，提供不同的方案。

3.2.1 Freeswan 实现

FreeSwan 的早期版本是基于虚网卡和注册协议的机制，其外出处理和进入处理结构如图 5 所示。

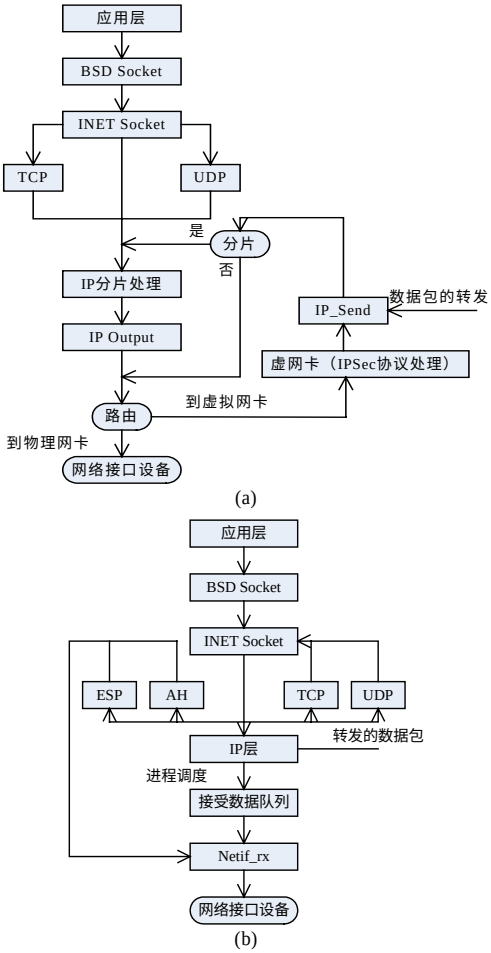

图 5 基于虚网卡和注册协议机制的 Freeswan 的外出处理和进入处理

从外出处理和进入处理的流程可以看出，该方案通过虚网卡和注册协议的机制避免了许多网络层功能的重复设计。例如外出的数据包在经过网络层的路由进入虚网卡进行 IPSec 处理后重新进入网络层，数据的分片处理等操作不需要重新实现；进入处理的数据包经过网络层到达传输层后经

过 IPSec 处理后，仍然再次进入接收队列，并再次进入网络层，而无需重新实现 IPSec 处理后的后续功能。

3.2.2 USAGI 实现

USAGI 的实现中并没有采用 Freeswan 的虚接口与注册协议的方式，而是采用在多种数据通路上增加 IPSec 功能的方法。以 IPv6 版本中为例，IPSec 功能被加在 TCP 的 ipv6_xmit(), UDP/ICMP 的 ipv6_build_xmit(), 邻居侦测包的 ndisc_send_ns() / ndisc_send_rs()。由于 Linux 内核 2.5 版本以后采用新的网络体系结构 XFRM，因此 USAGI 的后期版本基于 XFRM 结构。

Freeswan 实现与 USAGI 实现的一个重要不同是，Freeswan 致力于作为一个 Module 提供 IPSec 功能，而 USAGI 的实现则修改了原有内核的代码，并且由于 USAGI 的 IPSec 实现没有采用 Freeswan 的虚网卡和注册协议的机制，因此一些网络层的功能在 USAGI 的实现中不得不进行重新实现。

3.3 基于*BSD 的 IPSec 软件实现

FreeBSD, NetBSD, OpenBSD 下面的 IPSec 实现是由 KAME 项目组来完成的。其实现与 Freeswan 的理念不同，并不作为一个单独的 Module，而是修改原来的网络结构或处理模块，所以相对来说其结构要较 Freeswan 的设计简单，但实现复杂。IPSec 的流出处理和流入处理流程见图 6。

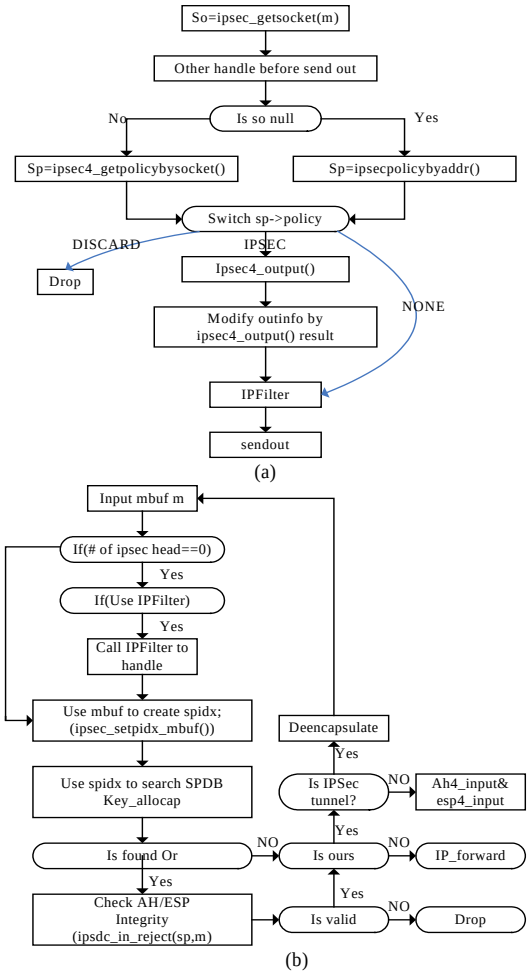

图 6 KAME 中的流出处理与流入处理流程

4 硬件实现分析

硬件实现的方案相对于软件实现方案除了在安全性上有所提高，速度性能上有所增加外，另一个显著的优点是平台无关性，即不必为不同的操作系统平台采取不同的解决方案。目前采用 ASIC/FPGA 方式实现 IPSec 协议的主要有 Cavium 的 Nitrox 系列，Motorola 的 MPC 系列以及 Hifn，AMCC 等公司的相关产品。由于 Cavium 与 Motorola 分别采用不同的设计，并很有代表性，因此本文以二者的设计为例进行分析。

4.1 Cavium 硬件实现方案

目前以 ASIC 的方式支持 IPSec 的设计主要有 Cavium 的 Nitrox-I 系列和 Nitrox-II 系列。以 Nitrox CN10xx 为例，它的内部结构如图 7 所示。

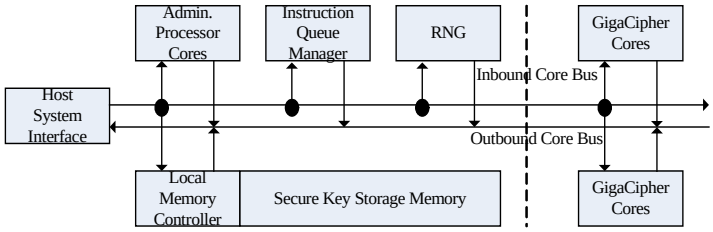

图 7 Nitrox CN10xx 系列 IPSec 实现的内部结构

GigaCipher 模块包括寄存器堆、ALU 单元、Hash 单元(MD5,SHA1)、加密单元(3DES、RC4 以及 AES)、模运算单元(模乘与模指)以及宏指令解析分发单元。从 GigaCipher 单元的组成可以看出该设计采用的宏指令结构有一定程度的灵活性。而从该设计的接口可以看出，该芯片并能不从芯片级和板级支持 BITW 结构，而只能从系统级实现，因为该芯片只能通过 PCI/PCIX 与系统进行数据交互，而不能真正做到完全解除系统对于安全处理的负担；并且该芯片并不能处理数据包的解析与重新包装等操作。

由于该设计用宏指令的方式来实现 IPSec 的核心部分，流水性能差，数据的吞吐率相对来说不是很高。

4.2 Motorola 硬件实现方案

与 Cavium 的宏指令设计方式不同，Motorola 的 MPC 系列安全协处理器完全采用硬线逻辑资源处理各种加密算法(私钥加密算法与公钥加密算法)，认证算法以及随机密钥生成器。其系统结构框图见图 8。

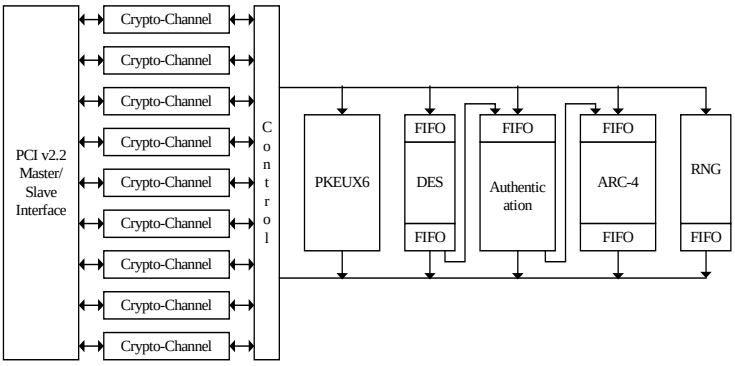

图 8 Motorola MPC190 功能框图

从上面的框图可以看出，该处理器支持多达 9 个通道，因此至少有 9 个网络通信可以得到同时处理，每个网络通信使用单独的通道；各处理功能模块之间采用流水处理，增大了系统的并行性。

同 Cavium 的设计类似，该方案仍然具有如下两个缺点：

(1)不具备对于网络数据包的解析以及重新组装功能，因此不能彻底解决系统其它功能模块的解包与封包处理负担；

(2)外部接口采用 PCI 接口，因此不能从芯片级或者板级支持 BITW 结构。

5 各种实现方案的比较

下面通过列表的方式对各种软件和硬件实现的方案进行介绍(见表 1)。

表 1 IPSec 各种实现性能比较

	Windows	NDIS	Freeswan	USAGI	KAME	Motorola	Cavium
软件/硬件	软件	软件	软件	软件	软件	硬件	硬件
实现方式	OS 集成	BITS	BITS	OS 集成	OS 集成	BITW(不彻底)	BITW(不彻底)
流水/并行性	不能流水，并行性差	不能流水，并行性差	不能流水，并行性差	不能流水，并行性差	不能流水，并行性差	可以流水，有一定并行性	不能流水，并行性差
网络层功能重复	无重复	重复	无重复	重复	无重复	无重复	无重复
平台无关性	Windows	Windows	Linux	Linux	*BSD	平台无关	平台无关
速度性能	一般	差	不错	一般	一般	很好	好
兼容性	差	差	部分兼容	部分兼容	部分兼容	兼容	兼容
灵活性	一般	好	好	一般	一般	差	差

其中“网络层功能重复”是指该实现是否重复了网络层的部分功能；“平台无关性”表示该实现是否只能在特定的平台上工作，“兼容性”是指该实现是否能与其它实现通过 IPSec 进行网络通信；“灵活性”主要指该实现方案能否适应协议新的变化。

从表 1 中可以看出，硬件实现相对于软件实现具有更高的性能，并且能适应多个不同的平台；但是相对于软件实现来说，灵活性差，例如软件实现基本上已经完成了从 IKEv1 到 IKEv2 的过渡，但是硬件实现对于 IKEv2 的支持仍然需要通过软件的修正进行。

6 总结与展望

本文分析了 IPSec 协议的结构以及实现的策略，并对基于 Windows, Linux, *BSD 等操作系统的软件实现进行了介绍和分析，指出了 Freeswan、USAGI 以及 KAME 等实现策略的异同；针对 IPSec 协议的硬件实现，分析了 Hifn，Cavium 以及 Motorola 等公司的设计。从中可以看出各种实现都有其相应的优缺点。

硬件实现是个趋势，尤其随着千兆甚至万兆网络的发展，软件实现已经越来越不能满足系统的性能需求。目前的硬件实现由于采用了 PCI 接口作为与系统的接口，不能实现真正意义上的芯片级 BITW 方式。同时另一个需要解决的问题是如何将灵活性与平台无关性等一些优点在硬件实现上进行统一。另外，如何实现硬件实现各功能模块的高速互连也是一个很有意义的课题，例如采用高性能的 SOC 总线。

参考文献

1 Scott C, Wolfe P, Erwin M. Virtual Private Networks(Second Edition)[M]. O'Reilly, 1999.

2 Doraswamy N, Harkins D. IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks[M]. Prentice Hall PTR, 2003.

3 Kanda M, Miyazswa K, Esaki H. USAGI IPv6 IPSec Development for Linux[C]. Proceedings of the 2004 International Symposium on Applications and the Internet Workshops, 2004.

4 Harkins D C D. The Internet Key Exchange[S]. RFC2409, 1998.

5 Kent S, Atkinson R. IP Authentication Head[S]. RFC2402, 1998.

6 Kent S, Atkinson R. IP Encapsulating Security Payload[S]. RFC2406, 1998.

7 Kent S, Atkinson R. Security Architecture for the Internet Protocol[S]. RFC2401, 1998.

(上接第 103 页)

用户仍需要等待一段时间。即便是达到了产品阶段，还需要经受市场的考验，不然重蹈蓝牙技术的覆辙，昙花未现便已凋零，不管谁赢得了标准之争也只能是一个失败的尝试，这需要整个产业链的共同努力。

5 Zigbee

Zigbee 是一种新兴的短距离、低速率、低成本、低功耗的无线网络技术。它采用直接序列扩频(DSSS)技术，工作频率为 868MHz、915MHz 或 2.4GHz，都是无需申请执照的频率。该技术的突出特点是应用简单，电池寿命长，有组网能力，可靠性高以及成本低。主要应用领域包括工业控制、消费性电子设备、汽车自动化、农业自动化和医用设备控制等。

Zigbee 联盟成立于 2001 年 8 月。ZigBee 协议由 5 家公司共同提出：霍尼韦尔，Invensys，三菱，摩托罗拉和飞利浦。IEEE 802.15.4 技术标准是 ZigBee 技术的基础。完整的 Zigbee 协议套件由高层应用规范、应用会聚层、网络层、数据链路层和物理层组成。网络层以上协议由 ZigBee 联盟制定，IEEE802.15.4 负责物理层和链路层标准。

Zigbee 具有功耗低、成本低、网络容量大、时延短、安全、工作频段灵活等诸多优点，无论未来几年 Zigbee 的市场占有率如何，它的发展空间仍具有相当大的潜力。

6 结束语

到目前为止各种无线个域网技术虽然已经取得了很大进展，但是要达到真正的商业成功，还要从技术和应用两方面改进。在技术方面要进一步提高系统的传输速率和吞吐量；保证 QoS 前提下提高频谱利用率和系统容量；改善功率控制功能，延长个人设备的电池使用时间；进一步增强系统的安全性能；采用智能的无线资源管理技术提供不同服务请求。在应用方面，要进一步降低用户设备的价格，使设备更加容易安装、使用和维护。总之，随着无线个域网技术的不断发展以及和其他类型无线网络的不断融合与互补，无线个域网将在全球范围内获得极为广泛的应用，取代线缆连接各种个人用户设备，给人们的生活带来方便和快捷。

参考文献

1 Karaoguz J. High Rate Wireless Personal Area Networks[J]. IEEE Comm. Magazine, 2001, 39(12): 96-102.

2 FCC. Docket ET 98-153-2002. Revision of Part 15 of the Commission's Rules Regarding Ultra-wideband Transmission Systems[S]. 2002.

3 IEEE. P802.15-04/0137r1-2004. DS-UWB Physical Layer Submission to 802.15 Task Group 3a[S]. 2004.

4 IEEE. P802.15-04/268r3-2004. Multi-band OFDM Physical Layer Submission to 802.15 Task Group 3a[S]. 2004.