一种网络安全体制的研究与设计*)

杨小平[1] 朱清新[2]

(四川师范大学计算机科学学院 成都610068)[1] (电子科技大学计算机学院 成都610054)[2]

A Research and Design for Network Security Mechanism

YANG Xiao-Ping[1] ZHU Qing-Xin[2]

(Computer College, Sichuan Normal University, Chengdu 610068)[1]

(Computer College of UEST of China, Chengdu 610054)[2]

Abstract IPSec provides interoperable, high quality, cryptographically-based security services for IP and upper layer protocols for IPv4 or IPv6, and it provides a protocol mechanism algorithm-independent. This paper gives an IPSec implementation after analyzing the base protocol mechanism of IPSec.

Keywords IPSec, TCP/IP, Protocol, Network security mechanism

1 前言

随着计算机网络在各个领域应用的广泛和深入，各种新兴业务如电子商务、电子金融、电子政务等得以迅速发展；而另一方面，愈演愈烈的网络黑客事件又给社会造成了巨大的损失，甚至威胁到一个国家和社会的安全。如今，网络信息安全已经成为关系到计算机网络发展前途的至关重要的问题。

Internet 是全球使用最广泛的计算机网络，TCP/IP 协议则是 Internet 采用的核心网络通信协议，而正是由于 TCP/IP 协议本身缺乏可靠的安全机制以及 Internet 的开放性，今天的计算机网络在安全性上就显得更加脆弱。当前有多种方案用于解决网络信息的安全问题，分别实现在 TCP/IP 协议栈的不同层上：在物理层上使用机械或电气方法防止信息被非法窃取，如电磁泄漏防护；在数据链路层上使用硬件加密设备直接加/解密链路两端的数据；在网络层上通过安全协议对需要保护的分组进行处理，如 SP3、NLSP、IPSec 等；在传输层上使用安全协议提供端对端的安全通信，如 SSL、TLS 等；在应用层上则可以实现对某些特殊服务进行单独保护，如 S-HTTP、SET 等等。各种解决方案中，在网络层提供安全保护具有如下优点：

1) 透明性。网络层屏蔽了上层服务的多样性以及下层链路的异构性，即安全服务的提供不需要应用程序、其他通信层次和网络部件做任何改动。

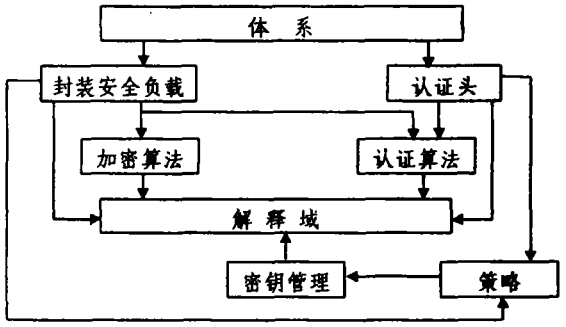
2) 灵活性。网络层上的安全保护可以提供端到端、主机到主机或者网络到网络等多种形式的安全通信保护，根据具体的需要灵活配置。

2 网络层安全协议——IPSec

IPSec 是由 IETF(Internet Engineering Task Force)的 IPSec 工作组所定义的网络安全标准。它不仅适用目前的 IPv4，也可以应用于下一代的 IPv6，它为 IP 及其上层协议(ICMP、TCP、UDP 等)提供安全保证，它提供的安全服务包括：访问控制、无连接数据包完整性验证、数据包始发方验证、防重放攻击功能、数据保密和有限的流量保密(防流量分析)等等[2]，是一个有着广泛应用前景的网络安全标准，目前已经得到了众多组织及厂家的支持，并已经开始大量地应用。

2.1 协议结构[1]

IPSec 协议包括如下组件：AH(Authentication Header，认证头)、ESP(Encapsulating Security Payload，封装安全负载)、IKE (Internet Key Exchange，Internet 密钥交换)、ISAKMP/Oakley (Internet Security Association and Key Management Protocol，Internet 安全关联和密钥管理协议)以及转码方式(加密算法组和认证算法组等)。各组件之间的关系如图1所示。



注：解释域(Domain of Interpretation)是一个单独的文档，存放 IKE 协商的参数。

图1 IPSec 各组件之间的交互关系

正如上图所描述的一样，IPSec 是一种协议套件，通过各个协议组件之间的相互作用实现 IPSec 体系描述的各种能力。总的来讲，IPSec 体系定义了主机和网关应该提供的各种安全能力，如要求主机使用 ESP 保证安全通信，使用 AH/ESP 和抗重播保护来保障数据完整性等等。

2.2 保护模式[1~4]

根据要保护内容的具体要求，IPSec 可使用传输模式和通道模式两种保护模式，如图2所示，它们的主要区别如下所述。

*)本论文得到国防科技重点实验室基金项目的支持—新型信息安全体制与信息战新概念研究，编号：2000JS06.5.1.DZ0219。杨小平 讲师，硕士研究生，主要研究方向是计算机网络通信及安全。朱清新 博士后，教授，博士生导师，主要研究方向是计算机网络通信及安全。

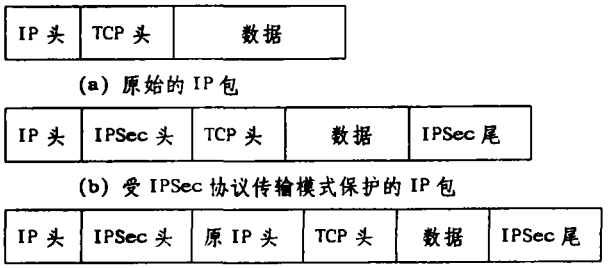


图2 分别使用 IPSec 传输模式和 AH 通道模式的 IP 包

1)传输模式 主要用于对上层协议的保护,即保护 IP 数据包的负载,如 TCP 数据段、UDP 数据段或 ICMP 数据包。在 IPv4中,负载指位于 IP 包头之后的数据。在 IPv6中,负载指 IP 包头和扩展包头(除目标地址选项)之后的数据,而目标地址选项也和负载一起受到保护。传输模式典型地用于两个主机之间的端到端通信。

2)通道模式 用于对整个 IP 数据包的保护,它将被保护的 IP 数据包用一个新的 IP 包包装,即把原数据包作为新数据包的负载,在原数据包前加一个新的 IP 包头(外部包头),因此原数据包在整个传送过程中是被完全封装的,传送路径上的路由器都无法看到原数据包的包头。并且,由于新数据包的源地址和目标地址都可以与原数据包不同,从而进一步增加了安全性。该模式典型用于安全网关之间或者主机与网关之间的保密通信。

2.3 安全协议与安全服务

IPSec 协议用于在 IPv4或 IPv6上提供互操作的、高质量的,基于密码学的安全服务,它提供了与密码学算法无关的协议框架,这种模块化的设计允许用户在不改变具体协议实现的情况下选择不同的算法或算法组,即可根据用户的不同需求来选择不同的算法。同时,为了实现不同 IPSec 协议实现之间的互操作性,IPSec 协议也规定了协议的强制算法。这种机制使 IPSec 协议的应用具有极大的灵活性和可扩展性[1,2]。

IPSec 协议包含两种传输安全协议:AH(认证头协议)和 ESP(封装安全负载协议),并辅之以应用层级的密钥管理程序或协议(如 IKE)[2]。AH 用于为 IP 数据包提供数据完整性、数据始发方认证以及防重放攻击服务,它不提供数据保密服务,所以它不需要加密算法,仅需要一个验证器。AH 协议定义了对数据包的保护方法、AH 头的位置、数据验证的覆盖范围以及输入输出的处理规则等,AH 协议不对所使用的数据验证算法进行定义,它是独立于具体的数据验证算法的[3]。

ESP 可以提供数据保密服务,数据始发方认证,数据完整性认证,防重放攻击,和有限的流量保密性服务。数据保密服务是 ESP 提供的主要功能;数据始发方认证和数据完整性认证作为一个整体,是 ESP 的可选用服务;防重放功能仅在有 ESP 认证时生效,并且具体处理取决于报文的接收方;流量保密需要使用 ESP 通道模式,一般在安全网关处实施,这样可隐藏报文的实际收发地址[4]。

AH 和 ESP 这两个子协议可以单独也可结合起来使用。每种协议又支持两种工作模式:传输模式和通道模式。在传输模式中,协议主要为上层协议提供安全服务;通道模式中,协议保护了整个内层的 IP 数据包。图3显示了 AH 协议和 ESP 协议所能提供的安全服务[3]。

安全服务 \ 协议	AH	ESP
访问控制	√	√
无连接数据包完整性验证	√	√
数据包始发方验证	√	√
防重放攻击功能	√	√
数据保密		√
有限的流量保密		√

图3 AH 协议和 ESP 协议所能提供的安全服务

2.4 安全关联[1,2]

安全关联(Security Association,SA)是构成 IPSec 的基础,是两个通信实体经协商建立起来的一种协定。SA 规定了安全通信要使用的 IPSec 协议、协议模式、加/解密算法以及数据完整性认证算法、密钥、密钥的有效期等等。SA 是单向作用的,所以两个实体之间的双向通信需要两个 SA,每个方向一个。一个 SA 使用 AH 协议或 ESP 协议,但二者不同时使用在一个 SA 上,如果需要由 AH 协议和 ESP 协议同时为一条通信流提供安全服务,则需要在通信双方都针对每一种协议来创建一个独立的 SA,即 SA 的组合使用。一个 SA 由3个参数惟一地标识:安全参数索引、目标 IP 地址、安全协议标识符。

在 IPSec 中,有两个数据库与 SA 紧密相关:SPD(Security Policy Database,安全策略库)和 SAD(Security Association Database,安全关联库)。SAD 是 SA 的集合,在 SAD 中存放了系统所有的 SA 和它们所使用的参数。系统通过查找 SAD 来确定每一个 SA 对相应通信所规定的具体保护形式,SAD 一般是由系统自动维护的。SPD 描述了系统的整体安全策略,它是创建和维护 SA 的根据。SPD 中的安全策略定义了对一个 IP 数据包提供何种安全服务(应用 IPSec 服务、绕过 IPSec 服务、丢弃数据包),以何种形式体现(指明具体应用的 IPSec 服务)等,它决定了受保护网络的安全性和可用性。SPD 是由系统管理人员人工进行维护的,它体现了整个系统的安全特性。

2.5 密钥管理[1,2]

IPSec 的密钥管理包括密钥的确定和密钥的分布,它贯穿于整个 SA 的协商、创建以及删除过程,分为手工密钥管理和自动密钥管理:手工方式指系统管理员以手工方式为每一个系统(主机和安全网关)配置该系统的密钥,该方式只能在相对稳定的小系统环境中使用,难以在可变的、相对较大的环境下使用,另外,它还常在系统测试阶段使用;自动方式是指系统能够自动地根据 SPD 为 SA 产生密钥,对系统的 SAD 进行自动维护,该方式适用于大规模、动态系统环境下的密钥管理,是 IPSec 密钥管理的主要使用方式。当前 IPSec 默认的自动密钥管理协议为 IKE/ISAKMP。

IKE(Internet Key Exchange)协议是 IPSec 协议中定义的用于进行自动密钥管理的标准协议,它用于动态地验证 IPSec 参与各方的身份、协商安全服务类型以及生成共享密钥等等。IKE 协议是 Oakley 和 SKEME 协议的一种混合型协议,并工作在 ISAKMP(Internet Security Association and Key Management Protocol)所规定的框架下。为了正确实施 IKE,保证协议的互操作性,必须遵守以下三个文档:

1)基本 ISAKMP 规范(RFC2408)

2)IPSec 解释域(RFC2407)

3)IKE 规范(RFC2409)

3 系统实现

3.1 实现环境

近年来备受推崇的 Linux 操作系统是 UNIX 类的操作系统,它遵循 POSIX 规范,含有 Unix System V 和 BSD4.3的许多功能;另外,Linux 操作系统采用了"自由软件许可"(GNU Public License)这一版权方式,任何人都可以免费获取操作系统源码,并能自由修改和发布。因此,采用 Linux 操作系统来实现 IPSec 安全规范是一个现实的方案,并且我们还可以在其上增加一些特殊的服务,并可以拥有完全的知识产权。

3.2 实现方式

目前,IPSec 的实现方式主要有以下三种[1,2]:

1)全部实现在 IP 模块中。这是通过直接修改操作系统中的 IP 协议模块,实现 IPSec 协议和操作系统集成在一起的方案,这种实现方案可以使代码间结合更紧密,系统效率当然最高。

2)全部实现在网络接口层。即更改具体的网络设备驱动程序,或者在已有的驱动程序上加上一层操作代码。这种方案的优势是不需要设计操作系统的源代码,简化了设计;但它的缺点也非常明显:一是必须在 IPSec 中实现大部分网络层的功能,如分段与重组、包路由功能等,这就从另一个方面增加了实现复杂度;二是这种实现方案产生了网络层的功能重复,将会在一定程度上降低数据包的处理速度。

3)使用专用设备实施。IPSec 的另外一种实现方式称作 Bump-in-the-wire(BITW),它是采用一个单独的设备来实现 IPSec 协议,然后将该设备挂接在主机或者路由器上。这种方案一般是由网络设备提供商采用的,对用户来讲体现的就是方便,但它不具有可扩展性。

从系统效率和可扩展性的角度出发,第一种实现方案最具有优势。当然,把 IPSec 实现在 IP 模块中需要修改大量的操作系统源代码,有一定的难度;但我们认为,从系统获得的效率以及该方案应用场合的可扩展性(既可用于主机也可用于安全网关)上来看这个代价是值得的。该方案的网络分层结构如图4所示。

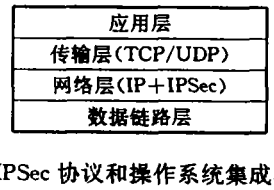


图4 IPSec 协议和操作系统集成在一起

3.3 系统总体结构

系统包含如下模块,各模块之间的关系如图5所示。

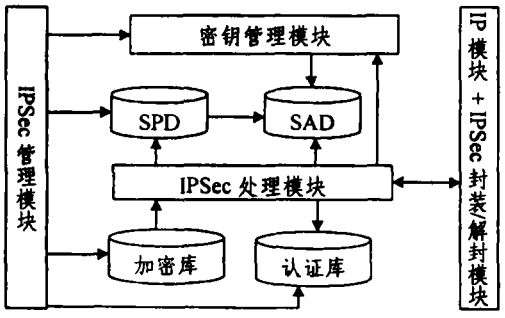


图5 系统主要模块及其相互关系

IPSec 管理模块 完成 IPSec 所需的配置和管理功能。如 SPD 的建立与维护;加密算法库、认证算法库的维护与管理等。

密钥管理模块 利用 IKE 实现通信双方的密钥交换,负责完成 SA 的创建、维护与删除,SAD 的建立与维护等功能。

IPSec 封装/解封模块 对于外出 IP 数据包,该模块将对其添加 IPSec 头并重新进行封装;对于进入 IP 数据包,该模块将完成 IPSec 头的解封装功能。该模块是通过直接在原 IP 模块上修改、添加代码来实现的,与原操作系统的 IP 模块紧密结合在一起。

IPSec 处理模块 该模块实现对外出 IP 数据包进行 IPSec 外出处理,对进入 IP 数据包进行 IPSec 进入处理,是整个系统的核心工作模块。

加密算法库 IPSec 是独立于具体的数据加密算法的,在加密算法库中提供了本系统所支持的全部加密算法。包括 DES-CBC、IDEA、Triple DES、RC5 等,其中 DES-CBC 是 IPSec 的强制加密算法,每个 IPSec 的实现都必须支持,这是为了保证不同 IPSec 实现之间的互通性。

认证算法库 同样,IPSec 也是独立于具体的数据验证算法的,在认证算法库中提供了本系统所支持的全部数据认证算法。IPSec 协议将 HMAC-MD5-96和 HMAC- SHA-96定义为默认的、强制实施的加密消息认证码算法,任何 IPSec 实现都必须支持它们。

SPD(安全策略库) SPD 中给出了系统对需要进行保护的通信所设置的保护类型,它描述了系统的整体安全策略,是 IPSec 处理模块工作的依据也是创建和维护 SA 的根据。

SAD(安全关联库) SAD 中记录了系统当前的所有 SA,它详细描述了每一个保护所需要的各种参数,如 IPSec 协议、协议模式、密码算法、会话密钥、密钥的有效期等。

结束语 今天的计算机网络已经渗透到了人们生活的诸多领域,它在给我们的生活方式带来巨大变化的同时也给我们带来了更多的安全隐患。如何更好地利用计算机网络,以产生更大的社会效益和经济效益,提高网络的安全性是我们必须首先解决的问题。当前的各种安全方法大多是基于 TCP/IP 分层模型的,这主要是因为 TCP/IP 协议是目前使用最广泛的网络通信协议。由 IETF(Internet Engineering Task Force)在1998年底所推荐的网络安全标准 IPSec 是工作在 IP 层上的网络安全协议,它对具体的用户有着很好的透明性,更具有一套强壮的、易于扩展的安全机制,至今已得到众多组织和厂商的支持,是一个很有发展前景的安全标准。

目前 IPSec 标准只定义了对双方通信的保护机制,还不能提供对多方通信(如广播)的自动保护,这是今后的一个研究方向;另外,由于 IPSec 的保护一般都要进行数据加密和数据完整性认证,整个过程必将增加对数据包的处理时间,增大网络时延,能否在 IP 层上通过对负载数据进行压缩后再进行保护来减小处理时间,这也是一个值得研究的方向。

参考文献

1 Doraswamy N, Harkins D. IPSec: The New Security Standard for the Internet, Intranet, and Virtual Private Networks, Prentice Hall PTR, 1999
2 RFC2401: Security Architecture for the Internet Protocol, Nov. 1998
3 RFC2402: IP Authentication Header, Nov. 1998
4 RFC2406: IP Encapsulating Security Payload (ESP), Nov. 1998