浅议 IP SEC 的核心技术——安全关联
Security Association in IP SEC System

荣京东　　荣 霓*
Rong Jingdong　　Rong Ni

（桂林陆军学院计算机中心　桂林　541001）
(Computer Centre, Guilin Military College, Guilin, 541001)

摘要　介绍新一代互联网安全协议 IP SEC 以及其核心技术——安全关联。并对 IP SEC 的发展及其应用进行了展望。

关键词　IP SEC　网络安全　安全关联
中图法分类号　TP393.08

Abstract　The Internet protocal standard-IP SEC and its key technique——Security Association are described. The application and expectation of IP SEC are also discussed.

Key words　IP SEC, network security, security association

随着计算机硬件制造技术的进步和网络协议的改进，计算机网络安全的重要性日益突出。以网络上广泛使用的 TCP/IP 协议为例，由于本身协议组存在的安全问题，它无法适应日益增长的对安全的需求，成为众多网络攻击者实施网络攻击的主要途径。在这种情况下，旧有的 TCP/IP 协议已经无法满足人们的要求，安全协议的研究与开发势在必行。在这种情况下，新一代的安全 IP 协议 IP SEC 应运而生，并力图成为业界基于 IP 的安全标准。为了将 IP SEC 更好地运用于网络实践，我们需要加强对 IP SEC 协议技术的研究。

1　关于 IP SEC

1.1　IP SEC 简介

IP SEC 的实现即是在主机或者安全网关上，提供对 IP 流的保护。这种保护是基于由用户或者系统管理员建立和掌握的安全策略数据库 Security Policy Database (SPD) 定义的要求，或者是以上两种人员建立的限制内操作的应用所定义。数据包被基于 IP 的 3 种模式中的一种选择，并按照与数据库相匹配来传送层的头信息。每个包将或者接受 IP SEC 的安全服务，或者被丢弃，或者被允许旁路 IP SEC，这都基于选择器指出的适用数据库政策。

2001-06-06 收稿。

* 国防科技大学计算机学院　长沙，410001.

1.2 IP SEC 目标

提供给 IP V4 和 IP V6 可以互操作的、高效的、基于加密的安全机制。安全服务集合提供包括访问控制、无连接的完整性、数据源认证、包转发的防止（protection of relay），机密性（加密算法）、以及有限的交通流机密性。这些都是基于 IP 层提供给本层或者上层的保护。因此高层的 TCP，UDP，ICMP，BGP 等协议都可以使用它。

1.3 IP SEC 作用

它基于 IP 层提供的安全服务是通过允许系统选择所需的安全协议，决定应用于服务的算法，并为所需的服务提供加密的密钥。它可以被用来保护一对主机、一对安全网关、以及一个主机和一个安全网关之间一条或多条通路。它的 DOI 还支持 IP 压缩的协商，当加密在 IP SEC 内使用时，它被激发。它可以防止较低协议层的有效压缩。

1.4 IP SEC 工作方式

使用 2 个安全协议：认证报文头 Authentication Header（AH）和压缩安全有效载荷 Encapsulating Security Payload（ESP）。

AH 提供无连接的集成、数据源认证，以及可选择的防止转发的服务。

ESP 提供机密性（加密），有限的流加密，以及无连接的集成、数据源认证，以及可防止转发的服务。当 ESP 被调用时，安全服务中的某一集合就会被使用。

AH 和 ESP 都是访问控制的载体，都基于加密密钥的分发和与安全协议相关的报文流管理。在 IP V4 和 IP V6 中这些协议既可以单独使用，也可以合起来使用，以提供理想的安全访问集合。每个协议都支持两种使用模式：传输模式和隧道模式。在传输模式中，协议主要向高层协议提供保护，在隧道模式中，协议被用来隧道 IP 报文。

IP SEC 允许用户或者系统管理员控制所提供的安全服务的粒度。IP SEC 的管理必须将工具合成一体以便指明：使用何种安全服务，以何种结合方式；给定的安全防护应使用何种粒度；使用何种安全有效的加密算法。

1.5 IP SEC 的实现方式

可以在主机、路由器连接点、防火墙等地方实现方式有：（1）将 IP SEC 集成进本地的 IP 实现。该方法要求访问 IP 源代码，适用于主机和安全网关；（2）打入协议栈“Bump-in-the-stack”（BITS）。IP SEC 在一个已经存在的 IP 协议栈之下实现，位于本地 IP 和网络驱动程序之间。该方法不需要访问源代码，便于实现。一般主要适用于主机；（3）板外加密芯片的使用。是一种常用的网络安全系统设计，被军方和一些商业公司采用。也叫打入线缆“Bump-in-the-wire”（BITW）实现。既可以用于主机，也可以用于网关。一般而言，BITW 设备是可以被 IP 寻址的。

2 IP SEC 关键技术 Security Association

安全关联 Security Association（下简称 SA）是 IP SEC 的基本概念。AH 和 ESP 都使用了 SA，而 IKE 的主要功能就是建立和维护 SA。

2.1 SA

SA 是一个能对其传输的流提供安全服务的简单的“连接”，它可以通过 AH 或者 ESP 的使用来提供，但是不是这两者的同时使用。一旦 AH 和 ESP 都作用于一个流上，2 个（或更多）的 SA 被建立。如两个主机、两个安全网关之间的双向通讯需要 2 个 SA（每个方向一

个）。

SA 由安全参数索引 Security Parameter Index（SPI）、IP 目的地址、安全协议标识（AH or ESP）3 个部分惟一指定。原则上，目的地址可能是单播地址、广播地址或者组播地址。但是目前的 IP SEC SA 管理只对单播地址有定义。

2.2 安全关联（SA）功能

SA 提供的安全服务依赖于所选的安全协议，SA 的模式，SA 的端点，以及协议内可选择协议的当选。

AH 同时还提供依赖于接收端判断力的反转发（部分顺序完整性）服务，以帮助抵御服务袭击。AH 是一个机密性未作要求（或者不被允许，例如，基于政府对加密算法的使用限制）时可以使用的合适的协议。它同时还提供对于 IP 头的选定部分的认证。例如，如果一个 IP V4 选项或者 IP V6 扩展头的完整性在发送方和接收方之间必须被保护。AH 可以提供该服务。

ESP 可根据用户要求提供机密的报文流。其机密程度部分地依赖于所使用的加密算法。

2.3 联合 SA

出于安全策略需要，有时对某一特定的数据流不能用一个单独的 SA 达成目的，只有使用多个 SA（SA 集束）才能实现所需的安全策略。处理的顺序是由策略定义的。例如，一个 SA 可能会介于一个移动的主机和安全网关之间，而另一个被嵌套的 SA 会延伸到安全网关之后。

安全关联可以以两种方式被合成一个集束，一是传输邻接，为一个 IP 数据报提供多于一个的安全协议，这种将 AH 和 ESP 结合在一起的方法只允许一个层次的结合。更多的嵌套将屈服于无附加利益（假设每个协议都采用了足够强的算法），因为最终的目的地操作将在一个 IP SEC 实例上进行。二是重复隧道，指的是影响 IP 隧道中多个层次的安全协议的实例。因路径上的每个隧道都起、止于不同的 IP SEC 地址，因此允许多层次嵌套，但对于中间安全网关的 ISAKMP 流必须指定正确的 SPD 条目。

2.4 安全关联数据库

以具体的 IP SEC 实现来处理 IP 流的细节很大程度上是一个局部问题而不是标准的问题。但是，处理的一些外部特征必须被标准化，以便协同工作和以最小的管理开销提供 IP SEC 的使用。

在模型中有两个名义上的数据库，安全策略数据库和安全关联数据库。前者指出用来决定一个主机、安全网关、或者 BITS/BITW 的 IP 实现的所有入站、出站 IP 流部署的策略。后者包括与每个（活跃的）安全连接相关的参数。而所谓的选择器是一组 IP 和上层的协议中被安全策略数据库用来映射到一个策略的域值。

每个 IP SEC 使用的界面需要名义上分离的入站和出站数据库 SAD 和 SPD，用来作为选择器的域的方向性。如果一个主机含有多个界面，或者一个安全网关含有多个外部的界面，那么每个界面拥有各自的 SAD 和 SPD 对则是必须的。

一个 SPD 必须在被提供了 IP SEC 保护和被允许旁路 IP SEC 的数据流中区别开来。这适用于由发送者提供的 IP SEC 和由接收者提供的 IP SEC。对于任何一个入站或出站的数据报来说，有 3 种处理选择：丢弃、旁路 IP SEC 或者申请 IP SEC。第一种选择指的是主机未允许离开的、横贯安全网关的，或者递交给一个应用的数据流。第二种选择是指被允许通过不需要附加 IP SEC 保护的数据流。第三种选择是指已经接受了 IP SEC 保护的数据流。对于这种数据流，SPD 必须指定要提供的安全服务、要运用的协议和要使用的算法。

3 结语

综上所述，IP SEC 作为新一代的计算机网络安全协议，在协议这个层次上对 TCP/IP 协议进行了较为完善的补充，并且还可以为下一代的 IP V6 所采用。由于协议的开放性，在具体开发时，用户可以方便地嵌入特定的加密算法，具有很强的灵活性。特别是作为协议核心的 SA，较好地解决了协议层安全结构的构成问题。

参考文献

1 William R, Cheswick, Steven M. Firewalls and Internet Security: Repelling the Wily Hacker, 1994.
2 Security Architecture for the Internet Protocol (RFC 2401).
3 Martin W, Murhammer et al.. A guide to Virtual Private Network, 1998.
4 Steven Brown. Implementing Virtual private Networks, 2000.
5 胡昌振，李贵涛等. 面向 21 世纪网络安全与防护. 北京：希望电子出版社，1999. 10.

（责任编辑：黎贞崇）

（上接第 236 页）

连网邮件扩展协议（S/MIME）、用于开发新一代的 VPN 的 IP 安全协议（IP SEC）等。

PKI 标准也在进一步完善，X.509 的数字认证结构一直处于不断的演变之中，其新版本不断增加新的功能。如 X.509 第 2 版添加了发布者和受检者标识功能；第 3 版增加了一个认证授权方式字段——类型/临界状态/值，可记录密钥、加密策略、用户和 CA 属性以及认证路径约束等信息。一些软件（如 Windows 2000）中已良好地集成了 PKI 组件，可实现证书的申请、颁发、管理等操作，构建 PKI 平台。

随着电子商务、企业虚拟专用网络（VPN）等的蓬勃发展，保障网络通信的安全迫在眉睫。PKI 对数据加密、数据签名、反否认、数据完整性及甄别所需的密钥和认证实施了统一的集中化管理，它必将得到广泛推广和采用，成为所有安全应用赖以存在的基础结构。

参考文献

1 颜逸品. Windows 2000 Server 企业网络建构实务. 北京：中国铁道出版社，2001.
2 ITU-T, Recommendation X.509. The Directory: Authentication Framework, 1997.
3 Merike Kaeo. 网络安全性设计. 潇湘工作室译. 北京：人民邮电出版社，2000.
4 张 琳等. 网络组建、管理与安全. 北京：人民邮电出版社，2000.

（责任编辑：黎贞崇）