IPSec：VPN 的安全实施

[美] Carlton R .Davis 著
周永彬 冯登国 徐震 李德全 等 译

清 华 大 学 出 版 社
麦格劳-希尔教育出版集团

(京)新登字 158 号

IPSec: VPN 的安全实施
Carlton R .Davis: **IPSec: Securing VPNs**
EISBN: 0-07-212757-0

书 名: IPSec: VPN 的安全实施
作 者: 美] Carlton R .Davis 著
周永彬 冯登国 徐震 李德全 等 译
出 版 者: 清华大学出版社(北京清华大学学研大厦,邮编 100084)
http:// www .tup .tsinghua .edu .cn
责任编辑: 赵彤伟
印 刷 者: 清华大学印刷厂
发 行 者: 新华书店总店北京发行所
开 本: 787×960 1/ 16 印张:24 .25 字数:461 千字
版 次: 2002 年 1 月第 1 版 2002 年 1 月第 1 次印刷
书 号: ISBN 7-302-04942-4/ TP・2780
印 数: 0001～6000
定 价: 52.00 元

译者序

因特网与大多数包交换网络都是建立在 Internet 协议(IP)之上;因而,要解决这些网络的安全问题,首先必须解决 IP 的安全问题。而 IPSec 协议正是解决 IP 通信安全的一个可行方案,它使用强的密码认证协议和加密算法来保护 IP 通信的完整性和保密性。但是,由于该协议很复杂,因此要真正理解它并不是一件容易的事情。它涉及多方面的知识,如密码学、TCP/ IP 协议以及它自身的体系结构。我们认为 Carlton R . Davis 所著的《IPSec: VPN 的安全实施》有利于从本质上理解和掌握 IPSec 协议,而且对理解和掌握密码学基础知识、PKI、LDAP 和 VPN 等也有很大的帮助。

本书实际上是一本高级科普读物,介绍的内容很广泛,要想了解细节的读者还得进一步阅读相关的资料。不过,我们相信,本书的翻译出版必将有助于国内 IT 专业人员、学生和相关人员对 IPSec 协议、密码学基础知识和 VPN 的更好的理解。

参加本书各章的翻译人员如下:前言和第 2 章由张兴兰博士翻译,第 1 章和第 4 章由李德全博士翻译,第 3 章由张振峰博士翻译,第 5 章到第 7 章由周永彬博士翻译,第 8 章到第 13 章由徐震博士翻译,附录 A 到附录 C 由周永彬博士翻译。全书最后由冯登国研究员和周永彬博士统稿和审校。

本书的出版得到国家 973 项目(编号:G1999035802)和国家杰出青年科学基金(编号:60025205)的支持,在此表示感谢。

感谢清华出版社第六编辑室的汤斌浩主任,感谢他的大力支持与帮助。感谢清华出版社第六编辑室的赵彤伟女士,感谢她为本书的出版提出的宝贵意见。最后,感谢所有帮助和支持我们的人。

译　　者

2001 年 8 月于北京

前言

因特网与大多数包交换网络一样都是建立在 Internet 协议(IP)基础上的。然而,IP 本身是不安全的。截获传输中的 IP 包比较容易,修改和重放 IP 包而又不被目的主机发现也比较容易。IP 使用一个 16 比特的头校验和来验证 IP 数据报的完整性。

这是非常初级的安全机制,因为在修改数据包之后可以重新计算校验和,并把新的校验和重新插入到校验和头域。因此,无法保证 IP 数据包来自它所声称的出处;也无法保证它在从起始地到目的地的传输过程中没有被修改。

IP 安全(IPSec)协议为保护 IP 通信的安全提供了一个可行的解决方案。IPSec 使用强的密码认证和加密算法来保护 IP 通信的完整性和保密性。但是,该协议详尽并且复杂,因此,有时被认为是一个难题。

本书的目的是以浅显易懂的形式介绍这个重要协议的各个组成部分;同时说明为了保护 IP 通信的安全如何以虚拟专用网络(Virtual Private Network,VPN)的形式来使用它们。本书覆盖范围很广,对于经验丰富的 IT 专业人员(网络/ 安全工程师、管理员、开发人员和程序员)有深刻的借鉴意义,同时也是一份很好的参考资料。对网络安全相关知识知之甚少的人也可以从本书中受益。

对象

本书适合三类主要对象:IT 专业人员、学生和任何渴望对 IPSec、相关的加密和认证密码算法以及 VPN 有更好了解的人员。本书以模块化的形式撰写,对每一个新的主题,其内容都是以这样的一种方式介绍的,即不需要预备知识就可以理解。然而,随着主题的展开,也给出了更多的细节。

本书选材范围很广。例如,有关于对称密钥和公开密钥密码算法、数字签名方案、Diffie-Hellman 密钥交换和杂凑函数的全部细节,这使得本书对学习密码学课程的大学生或开发安全应用软件的专业人员有很大价值;对那些渴望得到关于密码学的简单认识的人

也很有价值。

我们介绍的主题很广泛,因此本书对那些需要定期参考关于IPSec、TCP/ IP、密码学、LDAP、PKI或VPN的相关信息的IT专家或学生来说无疑是一本很好的参考书。

组织

本书给出了5个主要主题领域内的信息和对其的深刻理解。这些主题以其在本书中出现的先后顺序列举如下:

TCP/ IP

第1章有关于TCP/ IP协议簇的详细概述,其中包括对IPv4、IPv6、TCP、UDP、ICMP和IGMP的讨论。

密码学

第2章到第4章包含了与IPSec有关的密码方案(加密算法、数字签名方案、密钥交换、杂凑函数和消息认证码)的深刻描述和分析。

PKI

第5章给出了X.509、PGP数字证书及其各个组成部分的简介,并说明如何用它们来构造公开密钥基础设施(PKI)解决方案。

LDAP

第6章可被视为关于无处不在的轻量级目录访问协议(LDAP)的初级读本。

IPSec

本书的其余部分,即从第7章到第13章,包含了IPSec协议及其技术组成的详细描述,并深入分析了如何通过VPN使用这些协议以保护IP通信的安全。

致谢

在完成这项工作之际,我要感谢我的家人和朋友,感谢他们给我的鼓励和支持。同时我也想对 Luc Boulianne 和我以前所在的 McGill 大学说声谢谢,是他们激起我对网络安全和 IPSec 的兴趣。

还有许许多多多的人,他们的帮助使这本书得以出版。在此,我要花一点时间提及一些人的名字,向他们深表谢意,感谢他们为本书的出版所作出的贡献。首先,我必须对 Steven M . Elliot、Alexander Corona (McGraw-Hill 出版社的执行编辑和采编)和 Mark Luna(来自 RSA 出版社)说声谢谢,感谢他们的耐心和鼓励。感谢 Joanna V . Pomeranz、Joseph Cavanagh、Peter Karsten 以及 V&M 制图组的其他人员所做的出色的复制编辑工作。感谢 Bronislav Kavsan (来自 RSA)提供了技术简介;还要感谢 William Chan 设计了本书的封面;感谢 Maria Tahim 撰写了封面的内容;感谢本书的编辑——Mcgraw-Hill 出版社的 David Nash。

作者简介

Carlton R . Davis 在加拿大蒙特利尔 McGill 大学获得了计算机科学学士和硕士学位。多年来他一直在许多与 IT 安全相关的职位上任职,这为他提供了在 VPN 应用和其他网络安全工具方面的第一手经验。这些职位包括 PGP 安全公司(美国网络联盟(Santa Clara, CA))的高级系统工程师、加拿大 Bell 实验室(Montreal, Canada)的 Unix 系统管理者、McGill 大学(Montreal, Canada)计算机科学学院的系统管理员。

审阅者简介

McGraw-Hill 出版社作为技术书籍出版商的领头羊已有 100 多年了,它以带给读者权威的、最新的信息而自豪。为了保证该书达到尽可能高的准确性,我们邀请许多一流的行家和技术专家对该书内容的准确性进行了评价。

我们很荣幸地向 Bronislav Kavsan 表示感谢,感谢他的远见卓识。Kavsan 先生是 RSA 信息安全公司的副总裁,他领导一个工程组织开发了高级 PKI 产品系列。

Kavsan 先生于 1999 年加入 RSA 信息安全公司,他的兴趣涉及数据通信协议、网络安全和公开密钥基础设施。他有 25 年以上的信息系统数据通信经验,包括 VPN/ IPSec 系统的体系结构和实现以及在数据通信协议领域(Bell 实验室, AT&T/ 朗讯技术公司)的研究与开发。

目录

第 1章

TCP/IP概述

第1章 概 要

本章将讨论以下主题:

- TCP/IP的历史
- TCP/IP协议体系结构
  - —数据链路层
  - —网络层
    - * Internet协议(IP)
    - * Internet控制报文协议(ICMP)
    - * Internet组管理协议(IGMP)
  - —传输层
    - * 传输控制协议(TCP)
    - * 用户数据报协议(UDP)
  - —应用层

传输控制协议和 Internet 协议(TCP/ IP)是应用最广泛的网络协议。可将 TCP/ IP 看作推动数据传输的引擎、数据传输的管道以及引导数据在因特网上传输的导航器。因特网几乎可以用来完成所能想像的任何交易。你可以在线购买杂货,一小时内货物就送到了你的家门口。随着时间的推移,在线交易会越来越深入我们的生活。因此,了解一些有关这——无处不在的、已逐渐成为我们生活中不可缺少的一部分的基础设施——因特网的知识会对我们大有益处。

由于因特网在我们的生活中是如此重要,以至于我们必须考虑其安全性。不幸的是,有很多公司的安全设施远不能令人满意,而他们却希望我们在网上和他们交易。即使不能完全通晓,但能了解一些网络安全的概念和术语无疑也是有益的。这不仅对专家适用,对我们每一个人也都适用。点击按钮通过因特网传送我们的信用卡号和银行账号信息之前,我们必须能够点击我们打算与之交易的公司网站上的‘安全’链接并有足够的信息用以判断这些安全机制是否足以保护网上交易。如果能够对此作出正确的判断,就能避免因信用卡号、银行账号或个人识别号(PIN)落入不适当的人手中而陷入困境。

为了更好地理解 IPSec 协议和其他安全协议,必须深入理解 TCP/ IP 协议。本章将用一些实例详细介绍 TCP/ IP 协议簇中那些与 IPSec 相关的部分。如果读者对此细节不感兴趣,请跳过本章,直接去阅读感兴趣的内容。我们首先简要介绍一下因特网和 TCP/ IP 的历史。

1.1 TCP/ IP 的历史

20 世纪 60 年代中期,冷战正酣,(美)国防部希望建立一个能在核战争条件下幸存的管理和控制网络。因此,国防部就委托其研究机构——高级研究计划署(ARPA),发明一种技术,使得即使网络的任何部分由于核打击而毫无先兆地突然消失,数据也能可靠地到达目的地。此前就早已存在,至今仍在使用的传输有线电话数据的电路交换技术存在着严重的缺陷。在电路交换中,必须在数据传输的两个节点间通过中继建立物理连接以形成通路。因此,如果电路的某一部分出了故障,就必须建立一条新的连接。如果损坏严重,建立

一条新的连接可能是非常困难且费时的。

为了解决这些问题,高级研究计划署采用了称为包交换的技术。包交换网络的概念是由 Paul Baran 在 60 年代初期提出来的[Baran64]。在包交换中,需要通过网络传送的数据被分成离散的部分,称为包。每个包在网络中独立地由一台计算机传送到另一台计算机,直至到达目的地。

第一个实验型网络称为 ARPANET,于 1969 年 12 月建成。该网络由子网和主机构成。其子网又由一些用传输线连接的微型计算机组成,这些微型计算机叫做接口信息处理器(IMP)。该网络有 4 个节点,分别位于加州大学洛杉矶分校、加州大学圣芭芭拉分校、斯坦福研究院和犹他大学。每个节点都是由通过电缆连接的、处于同一个房间的一个接口信息处理器和一台主机构成。为了讨论的方便,这里把主机和计算机等同。之所以选择这 4 个节点,是因为这些节点所在的部门都与高级研究计划署(ARPA)有大宗合同并且各自都有不同的、完全不兼容的计算机。这一试验网络发展极快:1970 年 7 月,发展到 8 个节点;到 1971 年 3 月增加 16 个节点;1972 年 4 月发展到 23 个节点;至 1972 年 9 月,已有 34 个节点。

在初期节点较少时,这个网络的运行非常顺利。但是,随着节点数的增加,这个试验网络崩溃了多次。此外,在 20 世纪 70 年代初期,当卫星网络和广播网络连上这个网络后,ARPANET 使用的网络控制协议(NCP[NKPC70])不能与这些网络很好地兼容。于是,高级研究计划署于 20 世纪 70 年代初期开始研究健壮的、能在不同网络上运行的协议。这一研究于 1974 年成功地开发出 TCP/ IP 协议簇。

实践证明,TCP/ IP 协议簇有很强的健壮性且能应用于各种不同的网络。此外,TCP/ IP 是开放的、免费的、独立于任何计算机硬件和操作系统的、简单且易于实现的等等,因此 TCP/ IP 变得非常流行。1983 年,加州大学伯克利分校的 UNIX(BSD UNIX)4 .2 版中集成了 TCP/ IP,BSD UNIX 在当时早已是非常优秀的操作系统。同年,(美)国防部把这一协议簇采纳为军用标准(MIL STD);同时,这一协议簇也成为因特网的前身——ARPANET 的标准。

今天,TCP/ IP 仍然是因特网的标准。这一协议的设计独立于任何特定的物理网络硬件的事实使得它可以集成到多种不同类型的网络中。目前,TCP/ IP 已集成到以太网、令牌环网、拨号网以及其

他各种类型的物理传输介质和几乎所有的现代操作系统中。

1.2 TCP/IP协议的体系结构

网络互连协议通常分层设计,每层负责通信的一个方面。有了分层的概念,就可以修改某一层而不影响其他层的功能。TCP/IP协议簇包含4层,每层都有各自独特的功能并由不同的协议组合而成,如图1-1所示。下面介绍各层的功能。

图1-1 TCP/IP协议簇各层协议

1.2.1 数据链路层

数据链路层又称为链路层或网络访问层。其在TCP/IP协议栈中处于最底层。以太网(IEEE802.3)、令牌环(IEEE802.5)、ATM(异步传输模式)等是数据链路层的一些例子。其中,以太网在局网(LAN)中应用最广泛。在本书写作时,以太网卡支持的传输速率有10兆比特或100兆比特每秒(Mb/s)和1吉比特每秒(Gb/s)。以太网本质上是一个基于总线硬件体系结构的广播网。

什么是广播网呢?在广播网中,网上传输的是短的消息,称为包(packet)。包中除了包含要传输的数据外,还包含了源地址和目的地址以及协议之类的信息。网上的每台机器都要检查包以确定自己的媒体访问控制(MAC)地址(亦称硬件地址)是否与某一包的目的地址域中的地址相匹配;如果匹配,就从网上取走该包;如果不匹配,就忽略它。

以太网采用称作载波侦听多路访问/冲突检测(CSMA/CD)的访问方法。通常,如果网上的某主机希望向另一台主机发送数据,就访问传输媒体并检查是否有数据信号;如果没有,它就传输数据。然

而,如果检测到信道中有数据,则退出并等待几毫秒,然后再次检测。如此反复,直到信道空闲,它才传输数据。如果在同一时间不只一台主机传输数据,则很可能发生数据冲突。CSMA/ CD 技术允许主机检测数据冲突的发生,如果发生了冲突,则重传授冲突影响的数据。要了解主机检测冲突的细节,请参阅[Tan96]。

前面提到,网络上的主机会检查自己所在子网上传输的数据包,并确定这些包中的目的地址是否与自己的 MAC 地址相匹配。下面讨论 MAC 地址。MAC 地址是分配给每一个以太网卡的、全球惟一的 48 比特地址。其通常以 16 进制数表示。在大多数 UNIX 系统中,MAC 地址以 6 组由冒号隔开的 16 进制数表示,如 08:00:20:3E:0C:11。在 Windows 系统中,6 组 16 进制数字以短横线分开,如:00-AA-00-15-20-0F。在 Windows NT 中,可用 ipconfig / all 命令显示 MAC 地址;在大多数 UNIX 系统中,等价的命令为 ifconfig -a。

MAC 地址的前 24 比特是组织的惟一标识符(OUI):这是电子电气工程师协会(IEEE)分配给每个以太网卡厂商的。如 Intel 生产的以太网卡的 MAC 地址都以 00AA00 开头,而 SUN 生产的则以 080020 开头。RFC1700[RP94]列出了分配给每个以太网卡厂商的号码。MAC 地址的其余 24 比特则由网卡厂商分配给网卡。每个厂商负责确保其生产的每个网卡的 MAC 地址的惟一性。

当数据链路层收到来自其上一层即网络层的包时,它先用适当的包头对其进行封装,如以太网数据链路层用以太网包头封装,然后将它发往指定的目的地。以太网包头中包含有诸如源硬件地址和目的地硬件地址之类的信息。如要了解以太网包头各域更详细的信息,请参阅 RFC1024 [RP88],那里有详细的说明。数据链路层上面的各层不关心硬件地址,它们只用 IP 地址来识别网络单元。而数据链路层则使用硬件地址来操作,它必须填充以太网包头中的目的地硬件地址域。

IP 地址是如何转换为以太网地址或其他硬件地址的呢?数据链路层的地址解析协议(ARP)会完成此项工作。ARP 将 IP 地址映射为 MAC 地址的过程为:当一个数据报(这里可以理解为一个包)由第二层到达数据链路层时,ARP 模块从这个数据报中取出目的 IP 地址,然后检查自己的 ARP 表,看是否含有该 IP 地址的条目。这个 ARP 表是动态更新的,用于存放 IP 地址到硬件地址的映射。如果在 ARP 表中有该 IP 地址的条目,则把相应信息填入包的以太网头

中的目的硬件地址域,并传输该包。如果在 ARP 表中没有相匹配的 IP 地址,ARP 模块就向其所在子网的主机和路由器发一个 ARP 请求的广播包。ARP 请求消息申明拥有该 IP 地址和硬件地址的主机希望知道 ARP 请求消息中的指定 IP 地址对应的硬件地址。如果某主机的 IP 地址与该指定 IP 地址相同,则其 ARP 模块就发送一个 ARP 应答消息给出其 IP 地址和硬件地址。如果在该子网上没有网络单元的 IP 地址与需查询硬件地址的 IP 地址相同,则该包就被传送到下一个子网。查询过程继续,直到 ARP 请求包到达某个主机,其硬件地址正是待查询的硬件地址;或 ARP 请求包的生存期(将在后面介绍)到期为止。当发送 ARP 请求包的主机收到 ARP 应答时,它用应答包中的信息填充以太网头中的目的地硬件地址域,将此以太网头附加到它从第二层获取的数据报中,然后再向目的地传送。完成这些工作以后,该主机以 ARP 应答中的 IP 地址到硬件地址的映射信息更新 ARP 表。如果超过某个预定时间还没收到 ARP 应答,ARP 模块就向第二层发送一个目的不可达消息。关于 ARP 的更详细的信息,请参阅 RFC826[PLU82],那里有原始规范。

逆向地址解析协议(RARP)的功能刚好与 ARP 的功能相反:其将硬件地址映射为 IP 地址。RARP 主要用于无盘机器在启动时获取自己的 IP 地址。RFC903[FTMT84]包含 RARP 的原始规范。

在上面关于 ARP 的讨论中,我们谈到当数据链路层收到来自其上层(即网络层)的数据报时,先给数据报加上数据链路头,然后通过物理网络将数据报传输到目的地。当数据包从物理网络层到达数

图 1-2
数据在协议栈中向下传送时的封装和向上传送时的解封

据链路层时,数据包要经过相反的处理:去掉数据链路头,然后传给网络层进行处理,如图 1-2 所示。

1.2.2　网络层

网络层亦称 Internet 层。本层负责把数据包从源路由导向到目的地。在这一层中,我们感兴趣的协议有 IP、Internet 控制报文协议(ICMP)、Internet 组管理协议(IGMP)。下面讨论这些协议。

1. Internet 协议(IP)

IP 维系着整个 TCP/ IP 协议的体系结构。除数据链路层外,TCP/ IP 协议栈的所有协议的数据都是以 IP 数据报的形式传输的。IP 允许主机直接向数据链路层发送数据包,这些数据包最终会进入物理网络,然后可能通过不同的网络传送到目的地。IP 提供无连接的服务。在无连接的服务中,每个数据报都包含完整的目的地址并且路由相互独立;这样,使用无连接的服务时,数据报到达目的地的顺序可能与发方发送的顺序不同。这在面向连接的服务中是不可能的,就像电话一样,发方主机和目的主机之间会建立一条通道或连接,数据通过此连接传送,传送完成后再释放连接。

TCP/ IP 协议簇有两种 IP 版本:版本 4(IPv4)和版本6(IPv6)*。下面讨论这两个协议版本的数据报格式和编址模式。

IPv4 数据报格式

一个 IP 数据报包含一个报头部分和一个数据部分。报头部分由一个 20 字节定长的部分和一个变长的可选部分构成。数据部分的长度是可变的。图 1-3 图示了 IPv4 数据报格式。IP 数据报是按大端机(big endian)字节顺序即从左到右的字节顺序传送的,也就是低位的字节先传送。这是 TCP/ IP 包头中的任何二进制整数在网络中传输必须的字节顺序,也称为网络字节顺序。有些机器如 Pentium 机采用的是小端机(little endian)字节顺序即高位字节在前的顺序,则包头数据在传输前必须转换为网络字节顺序。现在研究 IP 包头的各个域。

* IPv5 是个实时的流协议。