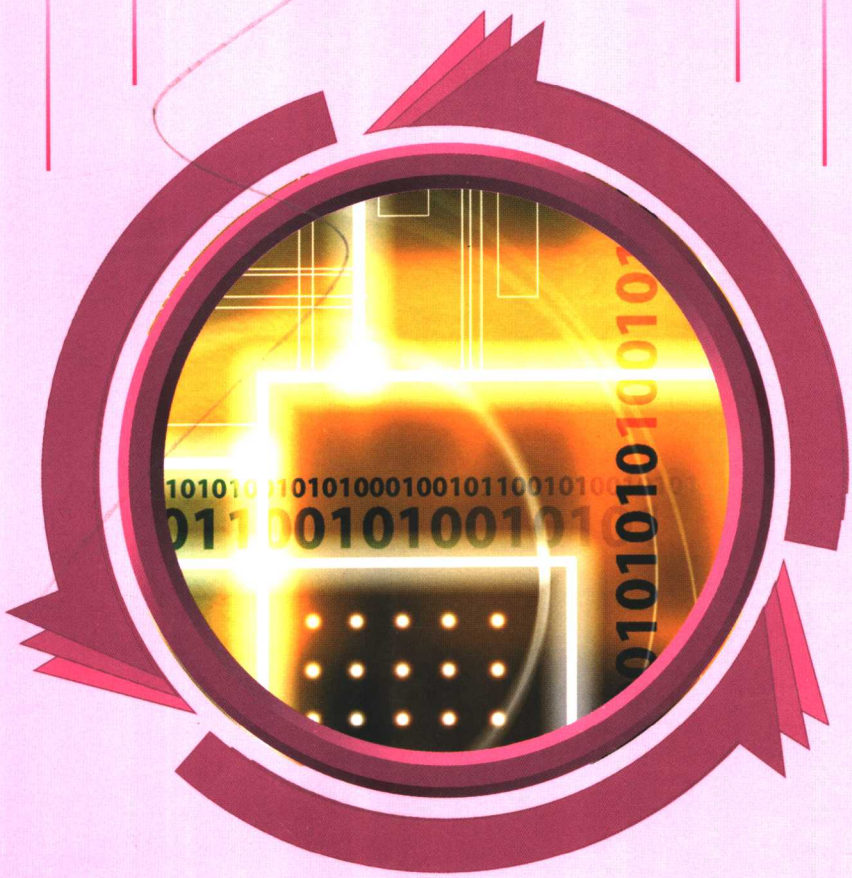
现代通信高技术丛书

IPSec解析

周贤伟 主编
薛 楠 编著



国防工业出版社
National Defense Industry Press

现代通信高技术丛书

IPSec解析

IPSec Jiexi

周贤伟 主编
薛 楠 编著

国防工业出版社
http://www.ndip.cn

内 容 简 介

本书从实用和科研的角度出发，比较全面、系统地介绍了 IPSec 及相关安全技术的最新发展。

全书共分 14 章，系统、全面地介绍了 IPSec 技术，详细分析了密码技术、TCP/IP 技术、IPSec 体系结构和组件、身份认证和保密性机制、认证头和封装安全载荷的用法以及密钥交换、IP 压缩、IPSec 实施等技术。

本书内容翔实，深入浅出，覆盖面广，具有先进性、科学性和很高的实用价值，适合于高等院校计算机、通信、信息安全等专业师生以及对 IPSec 感兴趣的科研人员和工程技术人员选做参考用书。

图书在版编目(CIP)数据

IPSec 解析 / 周贤伟主编；薛楠编著. —北京：国防工业出版社，2006.5

(现代通信高技术丛书 / 周贤伟，邓忠礼，郑雪峰主编)

ISBN 7-118-04413-X

Ⅰ. I... Ⅱ. ①周...②薛... Ⅲ. 因特网-传输控制协议 Ⅳ. TP393.4

中国版本图书馆 CIP 数据核字(2006)第 016367 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100044)

腾飞胶印厂印刷

新华书店经售

*

开本 787×1092 1/16 印张 13 字数 283 千字

2006 年 5 月第 1 版第 1 次印刷 印数 1—4000 册 定价 25.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)68428422 发行邮购：(010)68414474

发行传真：(010)68411535 发行业务：(010)68472764

《现代通信高技术丛书》编委会

序

当今世界已经进入了信息时代，信息成为一种重要的战略资源，信息科学成为最为活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业已经成为国民经济的主导产业，作为信息传输基础的通信技术则成为信息产业中发展最为迅速，进步最快的行业。目前，个人通信系统和超高速通信网络迅猛发展，推动了信息科学的进一步发展，并成为21世纪国际社会和全球经济的强大动力。

随着通信技术日新月异，学习通信专业知识不但需要扎实的专业基础，而且需要学习和了解更多的现代通信技术和理论，特别是数字通信、卫星通信以及传感器网络的现代通信技术方面的知识。从有线通信到无线通信，从固定设备间的通信到移动通信，从无线通信到无线因特网，到传感器网络技术。未来的通信将为人们提供全方位以及无缝的移动性接入，最终实现任何人在任何地方、任何时间进行任何方式的通信，使得通信技术适应社会的发展需要呈现经久不衰的势头。

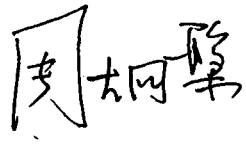
网络技术的飞速发展，通信技术在经济发展中的重要地位日趋重要，世界各国特别重视通信技术的理论研究和通信技术专业人才的培养，国外有关通信领域的文献资料和专著较多。就国内来讲，通信专业人才大量急需，为适应社会经济发展的需要，各高校和科研单位都在培养社会所需的通信专业人才。

为了增进通信及安全技术领域的学术交流，为了满足通信及信息安全专业领域的读者的需要，提供一套能系统、全面地介绍和讲解通信技术原理及新技术的系列丛书，北京科技大学等组织编写了这套《现代通信高技术丛书》。这套丛书内容涵盖了通信技术的主要专业领域，既可作为高等院校通信类、信息类、电子类、计算机类等专业高年级本科生或研究生的教材，又可作为有关通信技术和科研人员的技术参考书。

我觉得这套丛书的特点是内容全面、技术新颖、理论联系实际，针对目前

我国通信技术发展情况与目前已有的相关出版物之间已有一定距离这一情况，本丛书立足于现在，通过对基本的技术进行分析，由浅入深，努力反映通信技术领域的新成果、新技术和进展，是国内目前较为全面、技术领先、适用面广的一套丛书。在我国大量培养通信专业人才的今天，这套丛书的出版是非常及时和十分有益的。

我代表编委会对丛书的作者和广大读者表示感谢！欢迎广大读者提出宝贵意见，以使丛书进一步修改完善。



2005 年 3 月 20 日

前　言

随着 Internet 以惊人的速度发展以及人们生活节奏的加快，越来越多的人接入 Internet 网络，但由于 Internet 网络本身设计的缺陷及其开放性，使其极易受到黑客的入侵。计算机网络是一种有着广泛应用的信息传输系统，它是计算机与通信相结合的产物，它的安全性至关重要，特别是以 Internet 网络为代表的计算机网络正在成为未来全球信息系统最重要的基础设施，它的安全性将直接影响社会稳定和国家安全。IPSec 是一种协议套件，可以无缝地为 IP 引入安全。它可以为数据源提供身份认证、数据完整性检查和机密性机制、可以防止数据受到攻击。IPSec 除适用于 IPv4 也适用于 IPv6。IPSec 可为运行于 IP 顶部的任何一种协议提供保护，比如 TCP、UDP 和 ICMP 等。IPSec 是目前最易于扩展、最完整的网络安全方案。基于 IPSec 的这些特点，本书对 IPSec 进行全面阐述，详细介绍其具体应用，主要分析密码技术、TCP/IP 技术、IPSec 体系结构和组件、身份认证和保密性机制、认证头和封装安全载荷的用法以及密钥交换、IP 压缩、IPSec 实施等技术。

本书是作者在总结多年从事网络安全教学、科研工作的经验体会及研究成果的基础上，吸收国内外现有相关著作中许多精华编写而成的。它既有国内外专家观点和理论的精华浓缩，也包含作者从事信息安全研究和开发工作的总结，希望能给读者带来一些启迪和帮助。

全书分为 14 章。第 1 章概要介绍了密码学的基础知识。第 2 章分析了公钥基础设施。第 3 章介绍 TCP/IP 协议。第 4 章是 IP 安全综述。第 5 章研究 IPSec 体系结构。第 6 章分析认证头技术。第 7 章介绍封装安全载荷。第 8 章详细分析了 Internet 密钥交换技术。第 9 章讲述安全策略。第 10 章是 IPSec 的具体实施。第 11 章介绍实用 IP 安全技术。第 12 章研究了 IP 压缩 技术。第 13 章概述密钥恢复并提出了几种方案。本文最后在第 14 章介绍部署方案并给出了相应的例子。

本书参考或直接引用了国内外的一些论文和著作。编写过程中得到了国防工业出版社和北京科技大学的大力支持和帮助，在此一并深表谢意。

IPSec 是一门发展迅速的新兴技术，由于作者学识与水平有限，不妥之处在所难免，诚望读者批评指正。

编　者

2005 年 10 月于北京

目　录

第1章　密码学概述

密码技术历史悠久，其应用的时间大概可追溯到自人类社会出现战争的时候，据说凯撒大帝就曾用一种初级密码来弄乱它传达的命令。在今天的信息社会，计算机技术飞速发展，网络的开放性、共享性和互连程度不断扩大，网络上传输着大量敏感数据，其安全性已受到严重威胁。因此，对信息安全的保护越来越重要，密码技术是信息安全领域的核心技术，其越来越受到人们的关注。现代密码学的应用越来越广泛，已不再局限于军事、政治和外交领域，它的商用价值和社会价值也已引起了广泛的关注。世界各国都在加紧对密码技术进行研究和探索，试图发现更好的加密方法。这一问题的研究不仅在理论上而且在现实中都很有意义。

密码技术主要由密码编码技术和密码分析技术组成。密码编码技术是研究安全有效的密码算法，实现对重要信息的加密或认证。密码分析技术主要是破译密码或伪造认证码，达到窃取保密信息或进行破坏的作用。

1946年世界上第1台计算机诞生时，任何人都没有预测到50年后的今天，计算机在社会各个领域产生如此广泛和深远的应用和影响。计算机网络也已从最初的4个节点发展到横跨几大洲的几万个节点的Internet。网络的发展日新月异，各种网络技术和产品层出不穷，令人眼花缭乱。

随着网络规模和应用不断发展壮大，网络安全问题显得尤为突出。Internet已成为人们生活中不可缺少的一部分，但它同时也带来了许多社会问题。因此，对网络的管理和保护尤为重要。

1.1　网络安全

Internet设计的初衷是一个开放的网络并不提供保密服务，但是随着计算机网络的发展，各个国家都把政治、经济、军事、文化、科技等有关方面的信息送上Internet进行一定范围内的交流。如果一些敏感信息一旦让怀有敌意的人看到了，或者被别有用心的人修改，其结果可能危及到国家安全。

目前各国都将巨资投入Internet的商业化，网上购物、网上银行、网上办公等网络应用越来越广泛，正因为如此，不仅是外部而来自内部的对于系统安全的威胁也变得越来越大。不道德的雇员利用网络上的漏洞和管理上的疏忽通过盗取信用卡密码、用户账号、传播病毒等其他手段达到个人目的，给投资方、公司、国家带来了不可估量的损失。但由于Internet没有国家界限，因此处理这些案件非常困难，所以网络安全的重要性显得尤为突出。

计算机网络系统本身需要安全。一些人利用软件开发员在软件中留下的隐患，对网络系统进行攻击，对系统安全造成严重危害。现在，如果发生一次主计算机系统安全

崩溃事故，那么将有许多金融系统要遭到破坏。这种现象已经发生，只是我们还没有给予足够的重视而已。因此当前转账系统、密钥管理和数据仓库的安全性成为各界关心的焦点。

1.2 加密方法

1.2.1 加密基础

就加密方法而言，它有一部分建立在单向函数和陷门的基础上。所谓单向函数，是指一个函数很容易朝一个方向计算，但很难(甚至不可能)逆向回溯。所谓陷门，是指一种可供回溯的“小道”。换言之，利用它预留的安全隧道可欺骗系统逆行回到初始状态，也就暴露出秘密。

为使这样的单向函数能有效地应用于加密系统，它必须有能力对任何输入都进行这样的单向计算。比如在一个有限的范围内，很容易计算出数字的乘积，但却很难分解出生成那个乘积的各个乘数。另一个例子是离散对数问题：一个大质数 p 以及一个底数 g。已知一个特定的值 y，求指数 x，可表示为

$$g^x = y \bmod p$$

式中：mod 是求余的意思。模指数很容易便可计算出来，但假若想通过一次离散对数运算恢复原来的指数，却是异常艰难的。对于奇数、回文数字、可用 47 除尽的这些数字，如何用离散对数解决仍然非常困难。

单向函数没有正式的数学表达公式，但某些函数似乎拥有单向函数的一些属性，所以通常将它们称做单向函数。当然可能存在一些途径，可像求积那样快速地找出乘法因子，但迄今为止尚无人发现。正是考虑到这方面的原因，我们才可以很好地利用这种因子计算困难的特性。

所谓陷门函数(Trapdoor Functions)，解释起来稍微有些困难。现代加密算法广泛地运用了这种技术，但却很难一下子指着某个函数，肯定地说：“那便是陷门函数！”有一个例子可以很好地解释陷门函数。试想一棵树，上面有许多分枝。从一片树叶到树干是一条直路，不要求做任何选择。但要想从树干返回一片特定的树叶，却要求选择一个分枝，然后选择一个子分枝，接着是更深一层的分枝，依此类推，最后，选择具体的树叶。陷门函数负责的便是对这种分枝选择方法进行描述。

至于发现一片特定树叶的困难程度，显然取决于树的深度。图 1-1 展示的那棵树总

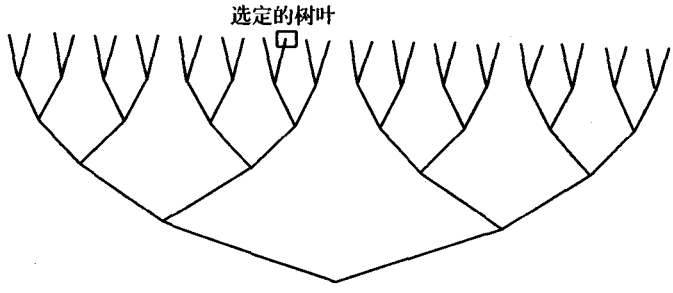


图 1-1 一棵陷门函数树

共有 5 层深度，所以有 2^5 片(32 片)树叶。从树干到图中选定的目标树叶所经过的“陷门”就是“左 - 右 - 右 - 左 - 右”这个密钥。应该注意的是，陷门函数完全不适合用做任何种类的加密用途，但为了演示一个陷门的概念，它还是能够胜任的。

在现代加密技术中，我们将单向散列函数应用于身份认证及完整性校验。“单向散列(Hash)函数”并不同于刚才讲述的“单向函数”的概念。散列函数采用一条长度可变的消息作为自己的输入，对其进行压缩，再产生一个长度固定的摘要。一致的输入会产生一致的输出。由于对任何长度的输入来说，输出都是固定的，所以显而易见地，对一种散列算法 H 来说，可能存在 2 个不同的输入：X 和 Y，比如 $H(X) = H(Y)$。这样便产生了冲突。单向散列函数的设计宗旨便是将这种冲突的发现(即找到 2 个会产生一致散列摘要的随机输入)变得非常困难。当今流行的单向散列函数是消息摘要 5(MD5，Message Digest 5)、安全散列算法(SHA，Secure Hash Algorithm)和 RIPEMD。尽管它们生成的摘要具有不同的长度，而且拥有不同的速度及抗冲突特性，但都是目前所广泛采用的。

和单向散列函数相比，单向陷门函数(建立在一个“陷门”的基础上)使用时要涉及到更多的计算。和用单向散列函数保障消息的完整性比较起来，假如用单向陷门函数(比如数字签名方案)来保障消息的完整性，那么后者需要的时间要多得多。在以后的章节内，我们将向大家展示 IPSec 和 IKE 及如何同时运用这 2 种技术。

另外一种经常用到的技术是简单的“异或(XOR)”函数。它既不是单向函数，也不是陷门函数，但同样是构建加密系统的一种有用工具。有基本数学知识的人都知道，2 个 0 进行 XOR 运算的结果是 0，2 个 1 进行 XOR 运算还是得 0，而 1 个 0 和 1 个 1(或者 1 个 1 和 1 个 0)的 XOR 运算结果是 1。XOR 运算一个非常重要的特点就是它的交替性。取得任何数据后，用长度固定(1bit、1B 或多比特、多字节)的一个密钥对其执行 XOR 运算，得到结果后，再用同样的密钥对那个结果执行 XOR 运算，便能恢复原来的数据。这其实就是一种非常简化的“加密”算法。但要注意的是，只要知道了输入或输出数据，都有可能推断出另一边的输入。这个特征通常并不是一种真正实用的加密算法所具有的，它暴露出用 XOR 算法进行加密的弱点[1]。

密码体制分为 3 种：一种是对称密钥密码体制，该体制的加密密钥和解密密钥相同或彼此间容易确定，其典型代表是美国的数据加密标准 DES；另一种是公钥密码体制，该体制的加密密钥和解密密钥不同，且从一个很难推出另一个，加密密钥公开而解密密钥保密，其典型代表是 RSA 体制；第 3 种是基于量子力学的量子密码。量子密码是以海森伯格(Heisenberg)测不准原理(光子的偏振现象)和 EPR 效应为物理基础，利用光纤异地产生物理噪声。它可以真正地实现“一次一密”密码，构成理论上不可破译的密码体制。光子不能被克隆的性质使量子密码编码操作过程不能被完全窃听，一旦存在窃听也可以察觉，并可以设法消除。

1.2.2　公钥密码体制

公钥密码学是现代密码学的一个主要分支。1976 年，Diffie 和 Hellman 首次提出了公钥密码的思想[2]，他们开创性的工作引发了密码学的一场变革，标志着公钥密码学的诞生。构建公钥密码系统需要单向陷门函数，1977 年，由 Rivest、Shamir 和 Adleman 3 位 MIT 计算机科学实验室的研究人员首先寻找到一单向函数，设计出著名的 RSA 公钥密码系