黑客防线

口令破解与加密技术

胡志远　编著

机械工业出版社
CHINA MACHINE PRESS

黑客防线

口令破解与加密技术

胡志远　编著

机械工业出版社

本书全面介绍了口令和密码的相关知识，包括一些常用加密技术、口令管理、策略、安全和口令破解等。直接明了地告诉读者黑客入侵、获取口令的方式，让读者可以快速地操作、运用并采取相关的防御措施。书中大量的实例可使读者轻易地按照说明与操作来加强防范措施，了解黑客行径。另外，书中口令破解工具一章还讲解了常见操作系统存在的一些关于密码泄漏的描述和应用，这也是本书所独有的。本书内容通俗易懂，可使所有上网用户增强网络安全意识，同时对致力于网络安全加密技术的开发人员有很大的参考价值。

图书在版编目（CIP）数据

口令破解与加密技术/胡志远编著．—北京：机械工业出版社，2003.7
（黑客防线）
ISBN 7-111-12448-0

Ⅰ．口…　Ⅱ．胡…　Ⅲ．电子计算机—密码术　Ⅳ.TP309.7

中国版本图书馆 CIP 数据核字（2003）第 049394 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
策　　划：胡毓坚
责任编辑：韩　菲
责任印制：路　琳

北京蓝海印刷有限公司印刷·新华书店北京发行所发行

2003 年 8 月第 1 版·第 1 次印刷
787mm×1092mm　1/16 ·22.5 印张·557 千字
0001—5000 册
定价：33.00 元

出版说明

近年来，计算机网络在国内得到了迅速的发展。在网络的大量应用中，安全正面临着前所未有的挑战。信息安全已经成为一个综合的工程，甚至将成为一门新兴的研究学科，需要我们在网络安全领域进行长期的研究和攻关。

网络的基础在于资源的共享，这一直是网络的基本准则。随着 Internet 的飞速发展，网络上的资源共享越来越强化。随之而来的，网络安全问题也越来越突出了。网络在带给人们诸多便利的同时，也成了许多犯罪分子攻击的目标。他们以计算机为工具，同时又以计算机为目标，在网上对计算机数据信息进行恶意的修改、删除，从而造成计算机系统难以正常运行甚至瘫痪。如果我们从另一方面去看问题，黑客也使我们发现自己网络的缺陷并改进它，从某种意义上说，日益完善的安全系统和逐渐完美的防火墙，是和黑客技术密不可分的。黑客的存在是网络发展的必然结果，尤其在我国，互联网络还处于雏形阶段，存在着不可忽视的缺陷与漏洞。如何改良网络结构，完善网络安全体系，是我们的当务之急。政府部门也对网络信息安全非常重视，并鼓励大力发展信息安全事业，以使我国在全球信息网络化的发展中占据主动地位。

目前，社会上对精通网络与信息安全知识的人才需求越来越强烈，广大技术人员和网络用户也十分希望能迅速提高自己应对安全问题的能力。由此，机械工业出版社联合北京地海森波网络技术有限公司《黑客防线》编辑部共同策划出版了“黑客防线”丛书，旨在为读者提供有关网络安全方面的知识和技术，从不同侧面阐述网络安全的相关技术。在丛书撰写过程中，切实考虑读者对知识的需求，内容做到通俗易懂，其中涉及的很多技术都是工作在网络安全第一线作者的心血结晶。对从事网络安全事业的技术人员来说，本套丛书是一个很好的帮手，从中可学到很多实用技术和宝贵经验，从而得心应手地应对各种网络安全问题。对于那些想学习网络安全知识和技术的读者而言，本套丛书也不失为好的学习工具书，通过学习不仅能迅速掌握网络安全知识，提高自身防范能力，而且为走上网络安全事业的道路奠定了基础。

我们始终坚持以普及网络安全知识，加强全民安全意识，提高我国信息技术和网络安全水平为己任，希望这套丛书的出版能满足读者的需求，并请广大读者批评指正，提出宝贵意见。

机械工业出版社

前　言

如果说在过去十年里，个人计算机的流行和普及是计算机工业的主旋律，那么今后十年，信息高速公路的建设将会是新的主题。迅速发展的国际互联网正把世界联系成一个整体，极大地加速了信息流通的速度和吞吐量，加快了社会生活的步伐。广大的国际互联网用户无一不感叹计算机和网络技术给工作和社会生活带来如此巨大而积极的影响。

但是许多用户没有注意到，在国际互联网积极影响的背后，也有许多阴暗面。以大家常用而熟悉的电子邮件为例。登录电子邮箱时所用的密码就很有可能被黑客盗用，而电子邮件的伪造现象也很普遍。

网络的安全问题又何止于电子邮件系统，诸如网络新闻、文件传输、万维网(WWW)等，同样存在此类问题。毫不夸张地说，在缺乏保护的情况下，用户在网络上存储和传输的任何信息，都存在着被泄露和篡改的可能性。风险总是和利益紧密相联系的，人们从网络上获得的利益越大，可能遇到的风险也越大。这就要求我们对密码和密码保护有一定的了解。

在计算机安全系统中，很大一部分就依赖于密码技术和加密技术。密码技术和计算机安全技术虽然在开始时是从不同的条件和目标下提出的，发展历史和背景不尽相同，但随着它们相依相存地发展，可以说从某种程度上已经密切地交融在一起了(当然并不是合而为一)。两者无论是加密算法的研究和设计，还是密码分析方法(即破译方法)的研究和分析，都在一个共同的目标下，为现代信息社会的有序化、合理化作出了重要贡献。所以作为一个网络安全爱好者，了解它们的工作原理和加密（这里也包括解密）工具是很必要的。

本书共分为 9 章，从基础知识、加密原理、解密工具到网络加密样样俱全。本书更多地配以大量的实例分析，结合当时的实战背景给读者分析加密的过程。当然，为了读者能更好地了解黑客的工作方式，本书还花费了大量的笔墨再现了黑客进行密码攻击的真实情况。下面介绍一下本书各章的内容：

第 1 章：概述。本章简单地介绍了数据加密和密码破解的一些知识，给读者以感性的认识。

第 2 章：加密技术。主要讲了加密算法、数据加密和数字签名等知识。本章还具体讲解了数据加密的实现。为读者学习以后各章内容打好基础。

第 3 章：口令加密。本章说明了用户识别的方法和用户口令的基本知识。

第 4 章：口令安全。本章说明了用户口令的破解方法、应用和实现。这里结合实例，说明了 Windows、UNIX 和常见数据库系统的口令原理、设置和相关注意事项。

第 5 章：社会工程学。这里结合一些具体实例，告诉读者真正的黑客不但要求掌握技术，而且还要掌握相关的社会关系学。这里的很多例子，就是讲黑客是怎么通过非法手段骗得口令的。

第 6 章：口令破解工具。本章对众多的需要口令的地方进行了分析，说明了相关漏洞和破解方法。大多数方法都涉及一些黑客和口令审计工具，不过有些工具会有破坏性，希望读者研究。

第 7 章：明文密码的拦截。明文密码在网上传播本身就是很危险的。这里介绍了网络监

听的特点、方法和防范。还有几个常用的网络监听工具的使用方法。

第 8 章：加密协议。在数据加密中最重要的就是对网络中协议的加密。本章介绍了网络中 OSI 各层次中的加密协议，例如 SSL、SSH、IPSec 等，并说明了各协议在 Windows、UNIX 操作系统中的实现方法。最后介绍了加密协议的一个应用——VPN。

第 9 章：加密工具。本章介绍了邮件、文件、应用程序数据加密工具，重点介绍了一个有史以来最著名的加密工具 PGP 的使用方法。

由于本书的特点，需要提到一些公司、产品和服务的名称。但是，需要特别指明的是，提到或者未提到某个特定的名称并不意味着任何批评或认可，也不意味着相应的公司、产品和服务是最受欢迎的。对于提到的公司的产品，只是对其产品的使用做一说明。

编　者

目　录

第1章 概 述

1.1 加密技术概述

如果说在过去十年里，个人计算机流行和普及是计算机工业的主旋律，那么今后十年，信息高速公路的建设将会是新的主题。迅速发展的国际互联网正把世界联系成一个整体，极大地加速了信息流通的速度和吞吐量，加快了社会生活的步伐。广大的国际互联网用户，无一不感叹计算机和网络技术给工作和社会生活带来如此巨大而积极的影响。

但是许多用户没有注意到，在国际互联网积极影响的背后，也有许多阴暗面。以大家常用而熟悉的电子邮件为例。登录电子邮箱时所用的密码就很有可能被黑客盗用，而电子邮件的伪造现象也很普遍。

网络的安全问题又何止于电子邮件系统，诸如网络新闻、文件传输、万维网（WWW）等，同样存在此类问题。毫不夸张地说，在缺乏保护的情况下，用户在网络上存储和传输的任何信息，都存在着被泄露和篡改的可能性。风险总是和利益紧密相联系的，人们从网络上获得的利益越大，可能遇到的风险也越大。这就要求我们对密码和密码保护有一定的了解。

在计算机安全系统中，很大一部分就依赖于密码技术和加密技术。密码技术和计算机安全技术虽然在开始时是从不同的条件和目标下提出的，发展历史和背景不尽相同，但随着它们相依相存地发展，可以说从某种程度上已经密切地交融在一起了（当然并不是合而为一）。两者无论从加密算法的研究和设计、密码分析方法（即破译方法）的研究和分析，都在一个共同的目标下，为现代信息社会的有序化、合理化作出了重要贡献。所以作为一个网络安全爱好者，了解它们的工作原理和加密（这里也包括解密）工具是很必要的。

1.1.1 为什么要进行加密

自从有了人类社会，作为社会的构成单位的人就会对他（或她）的隐私自然而然地提出保密的要求。激烈的市场竞争使得没有一个商家不把自己的很多资料作为机密信息，同时，企业间商业往来的数据资料也是不能向任何第三者透露的。一条信息的失密完全可能造成一笔生意的告吹，乃至给一个企业造成很大的经济损失。在军事计算机系统、国防计算机系统和外交计算机系统中，信息的机密性对一个国家的安全或外交政策是极端重要的。在信息化的当代社会，计算机和通信网络已日益结合并得到广泛应用，在给人们的生活和工作带来方便的同时，也带来了许多需要解决的问题，最突出的就是信息安全保密问题。但是，是否只有在计算机网络通信中才有安全保密问题呢？

随着信息技术的发展，计算机系统的概念变得越来越模糊，外延也越来越大。单个的个人计算机可以称之为一个计算机系统，一个局域网也可以称之为一个计算机系统，甚至因特网 Internet 这样的系统中，包含着许许多多的服务器、网络通信设备等硬件设施，也可以称之为一个计算机系统。从系统的角度来看，一个系统的安全强度取决于其中的每一个部件的

安全强度，任何一个部件的安全上的漏洞都会成为整个系统的安全脆弱点。可见，一个系统的安全强度不是由系统中最安全的部件的安全强度决定的，而恰恰相反，取决于系统中最不安全的部件的安全程度。

一个计算机系统，尤其是常见的计算机系统中，大多数是基于计算机网络的。计算机网络好比是日常生活中的公路或是铁路交通网络，各企业或机构的服务器好比实现生活中的货物仓库，这些货物仓库不仅要有专门人看守，而且在货物的运输过程中要确保货物通过公路或铁路安全地送达目的地。在计算机网络系统中，类似的情况是服务器上的数据只允许一部分应该看到的用户才能看到，而且数据在从一个机器到另一个机器的传输过程中必须保证他们不会被非法用户看见，更不允许他们被非法篡改。

可见，安全保密问题不仅存在于计算机网络通信中，而且存在于系统中的非网络通信部分，尤其是那些存有大量数据的计算机操作系统和数据库系统中。

操作系统安全和数据库安全的实现在一定程度上都使用了密码技术，因此计算机保密问题不仅仅存在于计算机网络的安全通信中，还同时存在于计算机操作系统和数据库系统中，而且几乎所有的计算机系统的信息安全保密问题都使用了密码学的研究成果。可见这里讨论密码与计算机系统安全是很必要的。

现在，国际互联网上的各种站点几乎都有各种各样的安全措施，例如防火墙（Firewall）、网络软件加密狗等。但是，这些都是系统或网站层次的安全设施，对于广大用户来说，更为直接、更为有效的方法、就是使用信息加密技术。

加密技术是一门实用的技术、有着悠久的历史。过去，加密技术仅被军事和间谍人员以及某些大型商业企业所采用，应用范围十分有限。加密学也是一门与数学有关的深奥科学，有能力研究加密学的人为数不多。恐怕这也是它鲜为人知的原因。随着国际互联网的商业化，这门古老的加密技术在社会上得到了从未有过的广泛关注。

在安全方面要求并不高的小型企业或个人用户的系统中，对数据加密也是很必要的。现今常用的软件，从操作系统、数据库到常用的应用软件，或多或少地使用了加密技术。随着计算机硬件技术的迅猛发展，加密的强度和加密的方法也是逐渐提高和变得多样化。有了加密技术，计算机网络才会变得更加的成熟。

1.1.2 信息是怎么进行加密的

现在的电子商务就是建立在互联网平台上的，互联网中无线服务在安全与保密方面明显地令人忧虑，因为无线电信号易被窃听，即使有线网络也能被抽头。信息高速公路软件必须采用加密传送以防止窃听。

因为经济和军事原因，政府很早就懂得了保守信息秘密的重要性。保守个人、商业、军事或外交信息安全（或破译它们）的需要吸引了几代人的才智。解读一条编码的信息总是令人感到高兴。查尔斯·巴比奇使 19 世纪中叶的译码艺术取得了戏剧性的进展，他曾经写道："就我看来，译码是最令人着迷的艺术之一，并且我恐怕在它上面浪费了太多时间。在我还是个孩子时，我就发现它很迷人。那时和各地的孩子们一样，我们一群人用简单的密码做游戏。我们用字母表中的一个字代替另一个，这样就把信息编成了密码。一个朋友发给我一条以 'ULFW NZXX' 开头的密码电文，我就很容易猜出它表示 'DEAR BILL'，其中 U 代表 D，L 代表 E，以此类推。有了这七个字母，迅速解开其他密码就毫无困难了。"

过去的战争胜利了或失败了，取决于世界最强有力的政府有没有编制密码的能力，而这种能力今天任何一个有个人计算机并对此感兴趣的中学生都具备。不久以后，任何会使用计算机的孩子都会传输密码信息，而地球上的任何政府都会觉得它难以破译。这就是神奇的计算能力传播的深刻寓意之一。

如果你通过信息高速公路发出一条信息，你的计算机或其他的信息装置就可以用只有你才能使用的数字签字“签名”，信息将被加密，因此只有其特定的接收者方可破译。你可以发出一条信息，它可以是各种信息、声音、图像或数字货币。接收者基本上可以肯定这条信息确实是你发出的，在指定时间发出，没有经过丝毫篡改而且其他人无法将它破译。

使这种现象成为可能的机械装置根据的是数学原理，其中包括“单向功能”和“公共密钥加密”原理。这些都是高深的概念，所以在后面的描述中，准备对它们一带而过。但是不管从技术上说这个系统是多么复杂，使用起来都将极其简单。只要告诉信息装置做什么，一切就会毫不费力地发生。

“单向功能”是一种操作要比解开容易的功能。打碎一片玻璃是单向功能，但这对编码来说毫无用处。密码术所需的单向功能是：知道一条特殊信息，解码就会异常简单，而不知这条信息，解码就会十分困难。数学中有很多单向功能，其中之一与质数有关。孩子们在学校里就学过质数，质数只能被1和它本身整除。在前12个数字中，2、3、5、7、11是质数，4、6、8、10不是质数，因为它们都还可被2整除。9这个数不是质数，因为它还可被3整除。质数的个数是无限的，而且除了它们是质数外，没有其他特征。如果把两个质数相乘，所得的数字也能被这两个质数整除。举例来说，35能被7和5整除，寻找这样的质数叫做“分解因子”。

将两个质数11927和20903相乘，可以很容易地得出249310081。但是将它们的积249310081分解因子得出上述两个质数却要困难得多。这种单向功能，也就是分解因子的困难，预示了一种巧妙的密码：目前使用的一种最复杂的加密系统，即使最大型的计算机将一个大的乘积数分解还原为组成此数的两个质数也要很长时间。建立在分解因子上的密码系统有两个不同的译码钥，一个用来给信息加密，另一个不同，但却相关的是用来解密的。有了加密钥，把信息译成密码就相当简单，但只用它在可行时间内解密却不太可能。解密需要一个单独的密钥，只有信息的特定接收者或不如说接收者的计算机方可拥有。加密钥的基础是两个巨大的质数的乘积，而解密钥的基础则是质数本身。一台计算机可在瞬间内造出一对新的独特的密钥，因为对于计算机来说，选出两个大的质数并把它们相乘非常容易。加密钥造出后可公之于众而不会冒任何危险，因为即使另一台计算机将其分解因子后来取得解密钥也是非常困难的。

对这种加密方法的实际应用将成为信息高速公路安全系统的核心。世界将会依赖使用这一网络，因此有效地处理安全性非常关键。你可以把信息高速公路想象成一个邮政网络，在那里人人都有一个邮箱，它不可篡改并且有一把牢固的锁。每一邮箱都有一个狭缝，因此每个人都可放入信息，但只有邮箱的主人才可用钥匙取出信息。一些政府会坚决主张邮箱有第二道门，门钥匙由政府保管，但在此处这里将忽略政府方面的因素而集中讨论软件可提供的安全性。

每一用户的计算机或其他的信息装置会使用质数来创造一个公开的加密钥和一个相应的只有用户本人知道的解密钥。在应用中它是这样工作的：我有信息要发给你。我的信息装置或计算机系统查找你的加密钥并在发出之前将信息加密。虽然你的密钥是公开的，但没有人

能读懂加密的信息，因为公开密钥中不包含解密所需的信息。你收到信息后，你的计算机会用与你的公开密钥相对应的私人密钥将信息解密。

你想答复，于是你的计算机就查找我的公开密钥，然后用它给你的答复加密。无人可读这条信息，尽管它是用公开密钥加密的。只有我能读懂它，因为只有我才有私人的解密钥。这种方式非常实用，因为没有人事先买卖密钥。

质数和它们的乘积要多大才能保证有效的单向功能呢?

公开密钥加密概念是威特菲尔德·迪菲和马丁·海尔曼于 1977 年首次提出的。另一组计算机科学家隆·里维斯特、阿迪·沙米尔和雷奥纳德·阿德尔曼，不久就提出了使用质数分解因子的想法，这也是以他们名字的首字母命名的 RSA 密码系统的一部分。他们提出，分解一个 130 位的两个质数的乘积数需要几百万年的时间，不管使用的计算能力多大。为了证明这一点，他们找到下面这个 129 位数，并向世界挑战要他们找出它的两个因子。这个数就是圈内人熟悉的 RSA 129：

114 318 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541。

他们坚信用这个数做的公开密钥加密的信息将会永远安全。但是他们既没有预料到莫尔定律的全面效应，也没有预料到个人计算机的成功。前者大大提高了计算机的能力，而后者则使全世界的计算机和用户数目得到了显著提高。1993 年，世界各地 600 多个研究人员和爱好者通过使用 Internet 协调各自计算机的工作向这个 129 位数发动了进攻。不到一年，他们就分解出了这个数的两个质数，其中一个长 64 位，另一个长 65 位，这两个质数分别为：3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577 和 32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533。

从这次挑战中得出的一个教训是：如果加密的信息确实重要并且高度机密的话，公开密钥的长度为 129 位仍不够长。另一个教训是：任何人对加密的安全性都不应过份肯定。

将密钥只增加几位数字分解起来就会困难得多。今天的数学家相信用可预测的未来计算能力分解两个 250 位长的质数的乘积要用数百万年。可是谁知道呢?这种不确定性，也就是有人会用简单方法将大数字分解因子的可能性，表明信息高速公路的软件平台将会设计成这样一种形式，那就是它的加密系统将会随时更换。

有一件事大可不必担心，即质数会用尽或两台计算机偶然会用同样的数字作为密钥。适当长度的质数数量比宇宙中原子的数量还要大得多，因此两个密钥偶然相同的机会微乎其微。

密钥加密的方法不仅仅可以保密，还可以保证文件的真实性。因为用私人密钥编码的信息只能用公开密钥才能译码。它的工作方式如下：如果一个人有信息在发出之前需要签字，那么他的计算机会用私人密钥将其加密。现在这条信息只有用他的公开密钥，也就是你和所有其他人都知道的密钥方可解密。这条信息确实系我发出，因为没有其他人有用这种方式加密的私人密钥。

计算机接收这条加密信息，再用公开密钥将此信息重新加密，然后通过信息高速公路把这条双重加密的信息传送给你。

你的计算机收到信息后用你的私人密钥对其解密，这解除了第二层编码，但用那个人的私人密钥编的第一层密码仍然存在。然后你的计算机用公开密钥再次对其解密。因为它确实是由那个人发出的，如果这则信息解密正确，你也就知道它是真实的了。即使信息有些微小