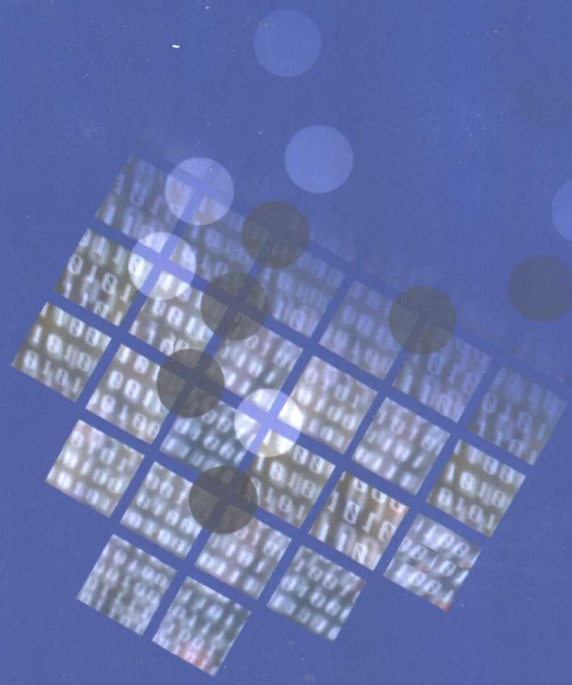

卿斯汉　蒋建春　编著

网络攻防技术原理与实战

科学出版社
www.sciencep.com

网络攻防技术原理与实战

卿斯汉　蒋建春　编著

国家重点基础研究发展规划资助项目(项目编号:G1999035810)
国家自然科学基金项目资助项目(项目编号:60083007)

科学出版社
北京

内 容 简 介

本书是一本系统论述网络攻防与信息对抗的专著。书中总结了目前网络攻击现状与发展趋势，详细地分析了计算机及网络系统面临的威胁与黑客攻击方法，详尽、具体地披露了攻击技术的真相，给出了防范策略和技术实现措施。

全书共分20章，主要内容包括：网络攻击的历史、现状和发展趋势，网络攻击的目标与分类方法，网络攻击模型，各种实际攻击技术，常用的网络攻击关键技术原理，网络重要服务的攻击理论与实践，网络攻击案例，网络攻击的规范策略与体系、防火墙技术原理与应用、弱点检测技术原理与应用、入侵检测技术原理与应用、网络诱骗系统原理与应用、计算机及网络攻击应急响应及取证等。

本书可以作为计算机、通信、信息安全专业本科高年级学生、硕士生和博士生的教材，也可供从事网络与网络安全工作（企业IT人员、网络管理和维护人员、网络应用开发者）和有关方面研究工作的广大工程技术人员参考。

图书在版编目（CIP）数据

网络攻防技术原理与实战/卿斯汉，蒋建春编著. —北京：科学出版社，2004

ISBN 7-03-012480-4

Ⅰ.网… Ⅱ.①卿… ②蒋… Ⅲ.计算机网络－安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2004）第100566号

策划编辑：鞠丽娜/责任编辑：丁 波

责任印制：吕春珉/封面设计：三函设计

科学出版社 出版

北京东黄城根北街16号

邮政编码 100717

http //www sciencep com

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

* * *

2004年1月第 一 版 开本 787×1092 1/16

2004年1月第一次印刷 印张：19 3/4

印数：1－4 000 字数：450 000

定价：29.00元

（如有印装质量问题，我社负责调换〈环伟〉）

序

因特网的迅速发展，促进了网络互联、信息共享与信息的全球化。信息全球化不但为我国带来发展机遇，也向我们提出了严峻的挑战。多年来，国外的主流操作系统 Windows 等主宰了 IT 市场，与此同时，基于 Windows 操作系统的应用也成为黑客攻击的主要目标。当前，随着网络互联范围的扩大，信息与网络安全已成为全球关注的问题，从一定意义上讲，没有信息系统的安全，就没有完整的国家安全。我们应该从战略的高度考虑信息系统的安全，不仅应当重视信息系统的防范，同时应当重视针对网络与主机系统的攻击技术与手段，更好地保护我国基础信息网络和重要信息系统的安全。以往，我们的科研工作与实际工作大多数以防范为主，近年来，虽然我国有关数据加密、防火墙、入侵检测、备份与恢复、PKI 公钥基础设施等的论文、著作、技术报告与工程项目日益增多，但是，专门涉及网络攻防、网络攻与防并重的专著，还不多见。实际上，网络攻击技术与网络防范技术是密不可分的，二者是相辅相成、相互促进、螺旋式发展的。因此本书的出版恰逢其时，将会对促进我国信息安全事业的发展起到积极作用。

本书由我国著名信息安全学者卿斯汉研究员领衔编著。全书共分 20 章，由网络攻击的历史、现状和发展趋势；网络攻击的目标与分类方法；网络攻击模型；网络攻击身份隐藏实战技术；网络攻击目标系统信息收集实战技术；网络攻击弱点挖掘实战技术；网络攻击目标权限获取实战技术；网络攻击活动隐藏实战技术；网络攻击实施实战技术；网络攻击开辟后门实战技术；网络攻击痕迹清除实战技术；常用的网络攻击关键技术原理剖析；网络重要服务的攻击理论与实践；网络攻击案例；网络攻击的防范策略与体系；防火墙技术原理与应用；弱点检测技术原理与应用；入侵检测技术原理与应用；网络诱骗系统原理与应用；计算机及网络攻击应急呼应及取证等章节组成，涵盖了网络攻防领域的主要内容。本书对网络攻防进行了清晰和完整的描述，不仅深入阐述了网络攻防的技术原理，而且通过大量实例对攻防的技术原理进行佐证，反映出当代网络安全攻防研究发展的趋势。

卿斯汉研究员及其项目组成员，长期从事信息系统安全的基础理论与关键技术研究，在信息安全域有很深的造诣和丰富的实践经验。本书通过作者的工程实践，包括一些国内外文献中鲜有的技术细节，可以加深读者对网络攻防内涵的理解。本书内容丰富，取材合理，有理论，有实践，是一部特点鲜明、深入浅出的网络攻防专著。

我衷心祝贺本书的顺利出版，我相信，她的面世将有力地促进我国信息安全事业的发展，并产生广泛影响。

中国工程院院士

周仲义

2003 年 10 月

前　言

信息安全包括攻击与防范两大范畴。长期以来，有关信息安全的著作，大部分偏重于有关防范的内容，例如，密码理论、防火墙技术、PKI公钥基础设施、入侵检测、备份与恢复、数据库系统安全、操作系统安全等。但是，专门讨论网络攻击技术，同时研究网络攻击与防御技术的著作却不多见。实际上，网络的攻击与防御是网络安全的两个侧面，它们是相辅相成，密切相关的。不深入探讨网络的攻击理论与技术，做到知己知彼，就不可能很好地保护网络信息系统的安全。有鉴于此，作者根据多年来在此领域中的潜心研究与实践经验，写作出版了这本关于网络攻防技术原理与实战方面的著作。

本书是一本系统论述网络攻防与信息对抗的专著，书中总结讨论了目前网络攻击的现状与发展趋势，详细地分析了计算机及网络系统面临的威胁与黑客攻击方法，详尽、具体地披露了攻击技术的真相，揭开了“网络攻击”的神秘面纱。同时，针对网络攻击方法，给出了防范策略与技术实现措施。

全书共分20章，主要内容包括：网络攻击的历史、现状和发展趋势；网络攻击的目标与分类方法；网络攻击模型；各种实际攻击技术，包括：网络攻击身份隐藏、网络攻击目标系统信息收集、网络攻击弱点挖掘、网络攻击目标权限获取、网络攻击活动隐藏、网络攻击实施、网络攻击开辟后门、网络攻击痕迹清除等；常用的网络攻击关键技术原理；网络重要服务的攻击理论与实践；网络攻击案例；网络攻击的防范策略与体系、防火墙技术原理与应用、弱点检测技术原理与应用、入侵检测技术原理与应用、网络诱骗系统原理与应用、计算机及网络攻击应急响应及取证等。

本书涵盖了网络攻防领域的主要内容，不但深入探讨网络攻防的基本原理与关键技术，而且通过大量实例说明网络攻防的实战过程。本书同时囊括了作者自身科研的成果，分析了网络攻防的热点问题及发展趋势，使读者阅读本书之后，对网络攻防有一个全面和完整的认识，有助于读者建立更加科学和有效的网络信息系统防范体系。

在本书的写作与出版过程中，作者受到中国科学院信息安全技术工程研究中心广大工作人员与研究生的支持和帮助。特向中心副主任倪惜珍和贺也平两位研究员，以及文伟平博士生、刘雪飞博士生、马恒太博士、张旺硕士、杨凡硕士、周武硕士、卢大航硕士、李小满硕士生、孙淑华硕士生、张楠等表示感谢。同时感谢网上安全论坛中的网友所提供的资料以及其他各界朋友的支持。

作者在长期的科研实践中，还得到了许多领导和专家的支持和鼓励，包括：张效祥、何德全、沈昌祥、蔡吉人、周仲义、魏正耀、胡启恒、倪光南等院士，中国科学院高技术研究与发展局局长桂文庄研究员，特别是著名信息安全专家周仲义院士在百忙之中为本书作序，使我们深受鼓舞。

本书的出版得到国家自然科学基金资助项目（60083007）和国家重点基础研究发展规划资助项目（G1999035810）的支持，作者在此深表谢意。同时，作者感谢科学出版社的编辑鞠丽娜女士，她为本书的顺利出版付出了大量心血。

本书是作者在网络攻防领域工作中的一次总结，也是一次新的尝试。由于水平有限，书中如果有不当之处，希望广大读者不吝赐教。

作　者

于中国科学院信息安全技术工程研究中心

2003 年 10 月

目　录

第 1 章　网络攻击的历史、现状与发展趋势

1.1　网络安全历史回顾

Internet 的飞速发展和普及，促进了网络信息系统的应用和发展。许多关系到国际民生的重要应用，如交通控制和国防信息系统等，越来越依赖于计算机网络。社会信息化和信息网络化，突破了应用信息在时间和空间上的障碍，使信息的价值不断提高。各种基于网络的信息系统已成为国民经济关键领域中的重要组成部分，例如，电力信息系统、气油运输和存储系统、金融服务信息系统、交通指挥通信系统、社区服务信息系统、医疗卫生信息服务系统、电子商务信息系统等。然而，对网络的依赖性越大，所产生的风险也越来越大。网络系统面临入侵、事故、失效等的威胁，这不但影响网络系统本身，还将形成一种链式反应，产生重大后果，如图 1.1 所示。

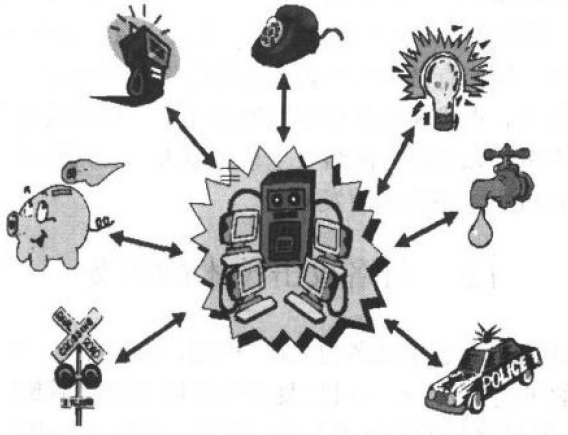

图 1.1　与网络相关的重要信息系统

受社会因素的影响，网络信息会受到破坏、窃取、篡改等各种威胁，造成信息无法使用。信息安全拓宽了国家安全概念，信息是国家的重要战略资源，也是公司、社会部门、个人的资产。网络信息化改变了传统意义上的有形空间安全概念，无形的“数字信息空间”的安全问题越来越突出。“数字信息空间”逐步深入到社会的方方面面，但由于它“看不见，摸不着”的独特性，大多数人未曾意识到它的安全问题。计算机网络作为信息的重要载体倍受大家关注，1988 年著名的“Internet 蠕虫事件”和计算机系统 Y2k 问题足以让人们高度重视信息系统的安全。2000 年春季，黑客通过分布式拒绝服务攻击，导致网络服务瘫痪，令人震惊。2001 年 8 月，“红色代码”蠕虫利用微软 Web 服务器 IIS 4.0 或 IIS 5.0 中 index 服务的安全缺陷，攻破目的机器系统，并通过自动扫描感染方式传播蠕虫，在 Internet 上大规模泛滥。由于信息系统安全的独特性，人们已将其用于军事对抗领域，计算机病毒和网络黑客攻击技术将会用作军事武器。网络攻击的发展将会改变以往的竞争形式，包括战争。Shane D.Deichmen 在他的论文《信息战》中写道：“信

息战环境中的关键部分是参与者不需要拥有超级能力。任何势力只要拥有适当技术就可以破坏脆弱的 C2 级网络并拒绝关键信息服务。”相对 Mahanian 的“信息控制”战略（该战略试图控制信息领域的每个部分）而言，美国军方更现实的战略方法是“信息拒绝”（特别是对真实信息访问的拒绝）。RAND 的专家写道：“信息战没有前线，潜在的战场是一切联网系统可以访问的地方——油气管线、电力网、电话交换网等。总体来说，美国本土不再是能够提供逃避外部攻击的避难所。” Libicki 将信息战分成以下 7 种不同类型：命令控制的战争、基于智能的战争、电子战争、心理战争、黑客战争、经济信息战争、数字战争。

网络信息系统的安全问题不仅涉及保密性，而且涉及到完整性、可用性、可控性等多个方面。恶意事件、突发事件、恐怖主义和国家敌对行为等都将影响到信息系统的安全。2000 年发生的以网络瘫痪为目标的黑客攻击事件震惊了全美国，从受攻击的商业网站到各个网络公司，从联邦调查局到司法部，乃至白宫和国会，都受到了巨大的震撼。受社会政治环境气候影响，重大事件常常触发网络攻击的发生。黑客们攻击 Web 网站，修改主页，表明自己的观点，扩大影响。纵观计算网络发展，网络攻击事件时有发生。据有关资料统计表明，从事计算机业务的工作人员中，工程人员占 70%以上，内部人员占 65%左右。同时“白领犯罪”分子占绝大部分，大部分网络安全事件与内部人员相关。堡垒最容易从内部攻破，如何有效地防止内部人员作案是网络安全急需解决的问题。网络技术在造福人类的同时，也成为犯罪分子作案的工具。种种网络安全事件向人们敲响了警钟，网络安全绝不可掉以轻心。网络安全事关重大，必须努力寻求解决办法。网络安全在攻击和防御的对抗中，不断向前发展。

1.2 网络攻击技术的演变

尽管网络安全的研究得到越来越多的关注，然而，网络安全问题并没有因此而减少。相反，随着网络规模的飞速扩大、结构日趋复杂和应用领域的不断扩大，出于各种目的，盗用资源、窃取机密、破坏网络的肇事者也越来越多，网络安全事件呈迅速增长的趋势，造成的损失也越来越大。图 1.2 给出的 CERT/CC 安全事件统计数据报告表明了这一点。

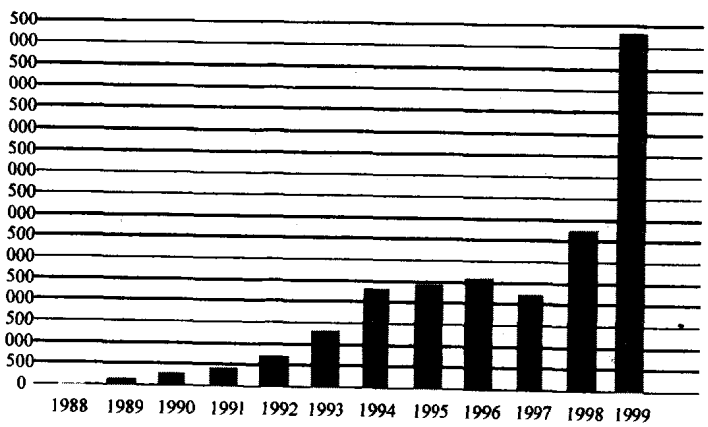

图 1.2 CERT/CC 安全事件处理示意图

John D. Howard 博士的论文认为，网络系统的攻击者共有黑客、间谍、恐怖主义者、公司职员、职业犯罪、破坏者 6 种类型，不同攻击者的攻击目的各不相同。图 1.3 所示的安全威胁金字塔说明攻击技术复杂性与攻击者人群数量变化之间的关系。

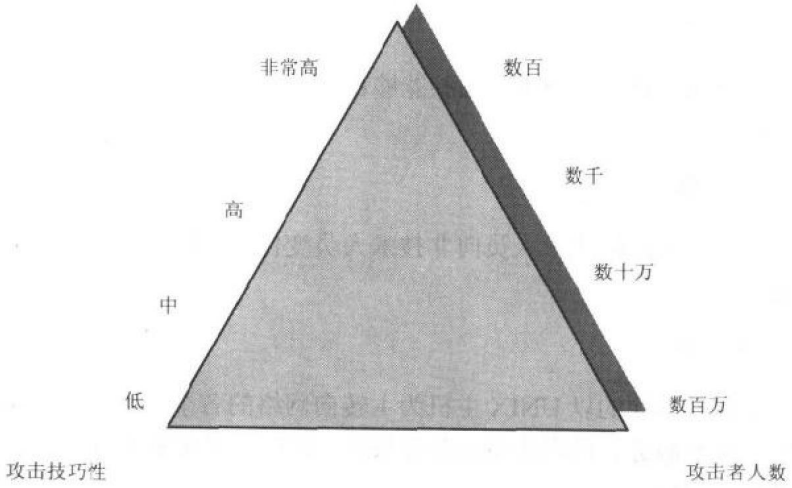

图 1.3　安全威胁金字塔

目前，已知的黑客攻击手段达数百种之多，而且随着攻击工具的完善，攻击者不需要专业知识就能够完成复杂的攻击过程，攻击的复杂度和入侵的技术知识如图 1.4 所示。

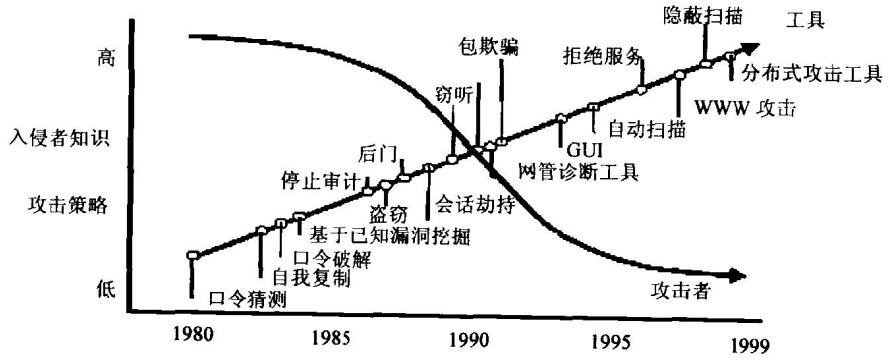

图 1.4　攻击的复杂度和入侵的技术知识示意图

黑客攻击早在主机终端时代就已经出现，1988 年著名的“Internet 蠕虫事件”开辟网络攻击的先例。小莫里斯从程序漏洞、协议弱点、口令猜测 3 个方面对网络信息系统安全进行了试探，结果令人震惊——6000 台网络主机因蠕虫程序而瘫痪。尽管这一事件已过去十余年，但是网络安全技术进展缓慢，网络安全问题仍然没有得到根本解决。随着 Internet 的发展，现代攻击则从以系统为主的攻击转变到以网络为主的攻击。攻击者为了实现其目的，使用各种各样的工具，甚至由软件程序自动完成目标攻击。现代攻击方法多种多样，如通过网络侦听获取网上用户的账号和密码、利用操作系统漏洞攻击、

使用某些网络服务泄漏敏感信息攻击、暴力破解口令、认证协议攻击、创建网络隐蔽信道、安装特洛伊木马程序、拒绝服务攻击、分布式攻击、协同攻击等，我们从以下7个方面来归纳网络攻击技术的变化特征：

1. 网络攻击自动化

网络攻击者利用已有攻击技术，编制能够自动进行攻击的工具软件，例如“中国小男孩”等工具软件。

2. 网络攻击人群

网络攻击人群从以前的技术人员向非技术人员变化，从单独个体攻击行为向有组织的攻击行为变化。

3. 网络攻击目标

网络攻击目标从以往的以UNIX主机为主转向网络的各个层面上。网络通信协议、密码协议、网络域名服务、网络的路由服务系统、网络应用服务系统，甚至网络安全保障系统均成为攻击对象。

4. 网络攻击协同

攻击者利用Internet上巨大的资源，开发特殊的程序，将不同地域的计算机协同起来，向特定的目标发起攻击。2000年2月，黑客以DDoS方法攻击雅虎（Yahoo!）等大型网站，导致服务瘫痪。爱尔兰数学家Robert Harley和他的3位同事动用Internet网络中9500台计算机强行破解了应用椭圆曲线算法加密的信息，其中密钥长度为109位。http://www.distributed.net提供一个协同攻击密码算法的典型实例。

5. 网络攻击智能化

网络攻击与病毒程序相结合，病毒的复制传播特点使攻击程序如虎添翼。2001年出现的“红色代码”是一个典型的实例。

6. 拒绝服务网络攻击

最简单的拒绝服务攻击是“电子邮件炸弹”，它使用户在很短时间内收到大量电子邮件，使用户系统不能处理正常业务，严重时会使系统崩溃、网络瘫痪。

7. 网络攻击的主动性

网络攻击者掌握主动权，而防御者被动应付。攻击者处于暗处，而攻击目标则处于明处，下面以弱点的传播及利用为例予以说明。攻击者往往先发现系统中存在的弱点，然后开发出弱点攻击工具。弱点攻击工具的档次越来越高，并广泛传播，最后才出现弱点的检测与消除建议，如图1.5所示。

图1.6是1997至2000年攻击技术演变的趋势图。总之，人们面临来自计算机网络系统的安全威胁日益严重。安全问题已经成为影响网络发展、特别是商业应用的主要问题，并直接威胁国家和社会的安全。

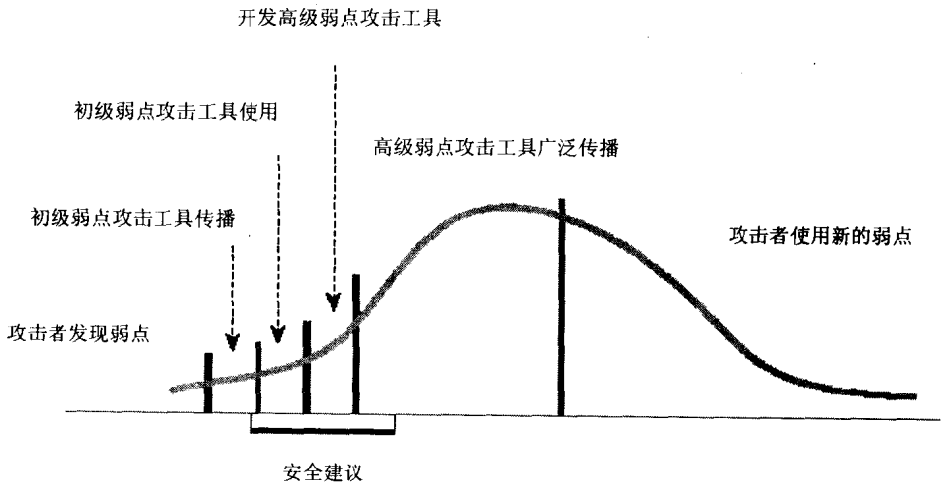

图 1.5　弱点传播及利用变化图

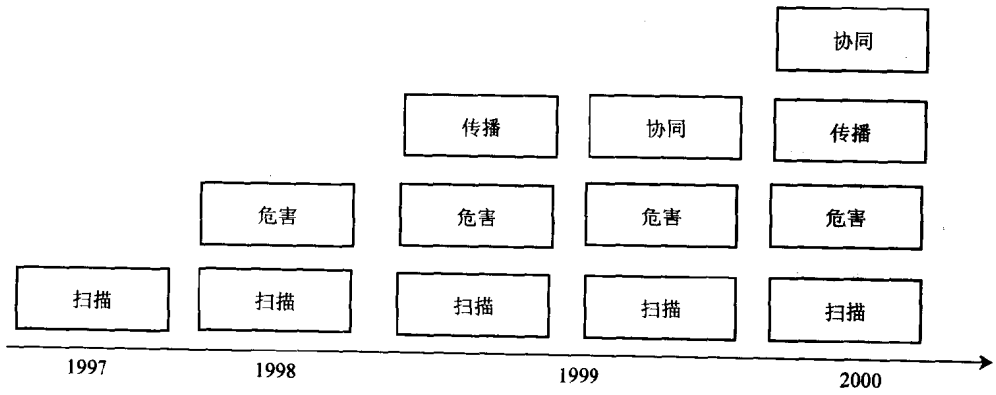

图 1.6　1997 至 2000 年攻击技术演变趋势图