华大精制 高校教材

21世纪电子信息工程专业系列教材

网络安全技术

2009湖北省级精品课程教材

张月红　李京昆　主编

華中師範大学出版社

21世纪电子信息工程专业系列教材

网络安全技术

主　编：张月红　李京昆

副主编：刘　华　任思佳　胡汉襄

参　编：何　平　范义山　王　永

吴秉书　崔俊峰　邱　净

王　跃　沈　强　司　军

张书田　赵志强　陈　陆

郭瑞杰

主　审：张焕国　何炎祥

华中师范大学出版社

内容简介

作为职业技能培训系列教材，本书结合实际教学过程中的实验，具有很强的实用性和指导性。本书将为读者展现作为一名合格的信息安全专业人员所应具备的知识域的全貌。

本书共分七章，每章之间既有一定的关联，又可以是独立的专题。第一章是信息安全的概述部分；第二章介绍了主机系统面临的威胁及系统安全的基本要素；第三章为加密技术；第四章介绍了防火墙产品的原理、功能、部署方法及入侵检测的原理、功能、安装部署方法；第五章介绍了扫描评估的概念、风险评估的内容、评估方法、灾难恢复与备份技术的相关知识；第六章是主流攻击分析与对抗；第七章是标准与管理。

本书既可以作为计算机及相关专业的教材使用，也可以作为已经学习和掌握了 IT 技术的相关工程技术人员、网络系统管理人员的参考用书。对于希望快速系统地掌握信息安全技术与产品基础知识的入门者，本书也是一本不可多得的参考书。本书课程资源网址：http://jpk.hbxftc.com/wlaqfhjs

新出图证(鄂)字 10 号

图书在版编目(CIP)数据

网络安全技术/张月红主编. —武汉：华中师范大学出版社，2009.6
(21 世纪电子信息工程专业系列教材)
ISBN 978-7-5622-3977-2
Ⅰ. 网… Ⅱ. ①张… ②李… Ⅲ. 计算机网络—安全技术 Ⅳ. TP 393.08
中国版本图书馆 CIP 数据核字(2009)第 104869 号

网络安全技术

© 张月红 李京昆 主编

选题策划：第二编辑室　　**电话**：027－67867362　　**策划编辑**：陈　勇
责任编辑：廖　烨　田培军　　**责任校对**：王　炜　　**封面设计**：甘　英
出版发行：华中师范大学出版社
社址：湖北省武汉市珞喻路 152 号　　**邮编**：430079
销售电话：027-67863426　67863040　67867076　67861549
邮购电话：027－67861321　　**传真**：027-67863291
网址：http://www.ccnupress.com　　**电子信箱**：hscbs@public.wh.hb.cn
印刷：武汉理工大印刷厂
督印：章光琼
开本：787mm×1092mm　1/16　　**印张**：19.5　　**字数**：460 千字
版次：2009 年 6 月第 1 版　　**印次**：2009 年 6 月第 1 次印刷
印数：1－3100　　**定价**：33.80 元

欢迎上网查询、购书

前　言

21 世纪，人类社会已进入了信息时代，计算机的普及与互联网技术的飞速发展，使信息与信息系统成为一种重要的战略资源。随着信息网络地位的不断提高，电子商务的广泛开展，信息安全已成为 IT 领域的重中之重，更成为世人关注的社会问题和计算机科学的热点研究课题。因此，了解和掌握信息安全的相关知识是非常必要和有意义的。发展信息安全技术与产业、保障信息系统安全的关键是人才，因此，培养信息安全领域的专业人才，已经成为当务之急。

鉴于此，越来越多的人希望了解并掌握信息安全领域的相关知识，在这种强大需求的推动下，各大中专院校纷纷开设了信息安全专业课程，同时加大了对信息安全领域的科研投入，以期培养出：熟悉信息安全攻防原理，掌握攻防对抗的实践经验，精通各种安全防护技术及相关产品的应用维护，能够独立完成各种系统的安全评估与加固，参与和管理复杂的信息资产保障课题，以及熟悉信息安全工程和标准的信息安全专业人员。

作为职业技能培训系列教材，本书结合实际教学过程中的实验，具有很强的实用性和指导性。本书将为您展现作为一名合格的信息安全专业人员所应具备的知识域的全貌。

本书共分七章，每章之间既有一定的关联，又可以是独立的专题。

第一章是信息安全的概述部分，主要介绍五个方面的问题，包括信息安全的发展简史、信息安全的概念、信息系统的安全威胁、信息安全的管理目标、面临的机遇与挑战。

第二章介绍了主机系统面临的威胁及系统安全的基本要素，共分为十节。第一节综述；第二节口令的安全性、强口令的设置方法及通过组策略保护账户口令安全的技术；第三节用户的权利和权限及设置方法；第四节 Windows 系统的启动机制；第五节进程的定义、系统主要的进程及进程安全管理方法；第六节 Windows 系统服务的安全威胁、安全策略和管理方法；第七节端口安全管理策略和常见的管理方法；第八节日志的安全性、配置及保护方法；第九节共享资源的安全问题、管理方法及常见故障的分析与解决方法；第十节补丁管理方法。通过本章的学习，读者能够较为全面地掌握在没有任何防护产品的前提下，如何使用 Windows 自带的工具和方法进行主机防护，从而更好地理解信息安全。

第三章为加密技术，这是目前应用最为广泛的安全技术，是信息安全的核心。主要介绍了各类加密算法、数字签名、公钥基础结构、加密工具应用于机密文件的加密存放、邮件和文件的传输。通过本章的学习，读者能够规划 PKI，解决网络内部的信息访问及重要文件和邮件的加密传输。

第四章介绍了防火墙产品的原理、功能、部署方法及入侵检测的原理、功能、安装部署方法。通过本章的学习，读者能够系统地掌握信息安全产品的基础知识，深入了解防火墙技术与入侵检测技术在构筑信息系统边界安全中的相互补充与配合情况。

第五章介绍了扫描评估的概念、风险评估的内容及评估方法、灾难恢复与备份技术的相关知识。通过本章的学习学习，读者能对信息安全系统有一个整体的认识：首先是系统

的风险扫描与评估，以确定安全需求和制定安全规划。其次，灾难的恢复与数据备份是信息系统恢复的最后一道防线，正确使用备份设备和恢复技术，才能避免系统灾难。

第六章是主流攻击分析与对抗，共分为五节。第一节协议分析的基础知识；第二节协议分析的主要功能；第三节 TCP/IP 协议解码；第四节应用解码，包括三次握手分析、IP 碎片分析、FTP 解码和 HTTP 解码；第五节安排有八个攻防实战项目。通过本章的学习，读者能够较系统地掌握和理解协议，直观地了解每个数据包的结构。八个实战训练项目使读者能更深入地了解网络中的各类风险的产生与对抗方法。

第七章是标准与管理，主要包括三个方面内容：安全管理标准及标准的演化过程、安全管理体系、BS7799 和 CC 安全管理标准解析。

为本书提供大量实践项目支持的是襄樊亮剑信息安全技术有限公司和襄樊信息技术安全检测协会。我们的团队成员有：李京昆教授、张焕国教授、何炎祥教授、任思佳、刘华、胡汉襄、吴秉书、崔俊峰、邱净、王跃、沈强、司军、张书田、赵志强、陈陆、郭瑞杰，全书的校阅工作由张月红老师负责。由武汉大学计算机学院张焕国教授、何炎祥教授担任本书主审。编者对大家一年来的辛勤劳动表示诚挚的感谢！

如果您在阅读本书时发现了问题，或者对本书有什么意见和建议，欢迎随时与我们联系。编者邮箱是：honey _ bobo@sina. com。

编 者

2009. 2

目　录

第一章　信息安全概述

★ 心灵火花

在信息时代，世界的格局是：一个信息霸权国家，十几个信息主权国家，多数信息殖民地国家。

谁掌握了信息，谁控制了网络，谁就将拥有整个世界。

——美国未来学家托尔勒

凡是有可能出错的事情，肯定会出错。换句话说，不是事情是否出差错，而是什么时候出差错。

——墨菲法则

信息时代的出现，将从根本上改变战争的进行方式。

——美国前陆军参谋长沙利文上将

今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。

——美国前总统克林顿

★ 导　读

本章从信息安全的发展简史开始，介绍了网络安全现状和网络安全对信息系统的重要意义。接着从不同角度对信息安全的基本概念进行了初步介绍，如信息安全的定义、信息安全三要素等；通过分析信息系统的安全威胁，得出信息系统的安全风险与成因，并提示网络安全问题的严重性和破坏性。最后阐述了我国信息系统等级保护和信息安全领域存在的机遇与挑战等。本章内容只是对信息安全基础的简要介绍，在以后的章节中将具体分析安全技术与攻防实战。

信息安全起源于计算机安全。最初的计算机安全就是确保硬件和软件的物理位置远离外部威胁。在第二次世界大战期间开发了第一代大型机，从这些大型机投入使用的那一刻起，就有了计算机安全的需求。随着计算机通信需求的增加，美国国防部高级研究计划署（ARPA）开始考察设计一个冗余的、联网通信的可行系统，以保障军队交换信息。Internet 的奠基人 Larry Roberts 开发了这个项目。该项目命名为 ARPANET。自从 ARPANET 采用 TCP/IP 协议实现 Internet 的成功互联之后，一个需要三年时间才能进行全球性传播的计算机病毒，今天只需要几分钟就能够在全球范围内传播。随着维护国家安全的需求不断增长以及信息技术的不断进步，计算机安全管理最终得到了更大的扩展。

1.1　信息安全的发展简史

国际上信息安全的发展经历了三个重要时期。

1. 信息安全的启蒙期——通信保密时期

通信安全（COMSEC）的历程开始于20世纪40年代。在早期，信息系统的安全仅局限于保证电脑的物理安全以及通过密码（主要是序列密码）解决通信安全保密问题。把电脑安置在相对安全的地点，不容许陌生人接近，这可能是最早的信息安全防护策略了。由于信息需要异地交流，因此又采用了将数据拷贝在存储介质上，派专人秘密地送到目的地，然后拷贝进电脑再读取出数据的安全保密策略。在这个阶段主要强调信息的保密性，对安全理论和技术的研究也仅限于密码学，所以这一阶段的信息安全可以简单称为通信保密安全，它侧重于保证数据从本地传送到异地时的安全性。20世纪中叶，军方和政府的关注促进了通信保密的大力发展。此阶段计算机系统的主要威胁是搭线窃听、偷盗物理设备以及对系统产品实施间谍活动和破坏，需要防止非法人员截获信息及确保通信的真实性。当时涉及的安全属性主要是保密性，保证信息不泄露给未经授权的人或设备，确保信道、消息源、发信人的真实性及核对信息获取者的合法性。重点是通过密码技术解决通信保密问题。1949年Shannon发表的《保密通信的信息理论》将密码学的研究纳入了科学的轨道，移位寄存器的物理舞台给数学家基于代数编码的理论提供了运用智慧的空间。

2. 信息安全的导入期——数据保密时期

1967年春夏，美国国防部内共享资源的系统安全问题引起了研究人员的注意。那时，此类系统的产量增长较快，其安全性问题成为军队和设备承包人共同关注的焦点。1967年6月，ARPA组织了一个特遣部队来研究保护机密信息系统的过程。该特遣部队定期开会，陈述其建议，这些建议最终成为美国国防部的一篇文章——Rand Report R-609的主体。Rand Report R-609第一次确定计算机安全中的管理角色和方针问题。它指出，信息系统中的联网组件在军队中得到广泛使用，由此带来的复杂性已超出了保护这些系统的常规措施。这篇文章标志着计算机安全史上一个关键时刻的到来，即计算机安全的范围被大大扩展了，除了物理位置和硬件的安全之外，还包括：

◆ 数据的安全

◆ 限制对数据的随机访问和未授权访问

◆ 涉及机构内多个层次的人员

当时对计算机安全的研究主要集中于一个称为MULTICS（Multiplexed Information and Computing Service，多元信息和计算服务）的系统上。虽然这个操作系统现在被废弃了，但它仍值得关注，因为它是第一个，也是唯一一个以安全为主要目标创建的操作系统。1969年中期，在MULTICS项目重构不久，它的几个重要参与者创建了一个新型操作系统UNIX。当时MULTICS系统实现了多安全级别和密码，而UNIX系统没有。UNIX的基本意图是文字处理，并不需要与其原型具有一样的安全级别。实际上，直到20世纪70年代早期，甚至是最简单的安全组件——密码函数，也是作为操作系统的一个组件实现的。

20世纪70年代以后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，数据的传输已经可以通过电脑网络来完成了。当时对计算机安全的威胁主要是非法访问、脆弱的口令、恶意代码（病毒）等，需要解决的问题是确保信息系统中硬件、软件及应用中的保密性、完整性、可用

性。由于军方和政府对计算机安全的关注和推动，计算机安全开始了里程碑式的发展。典型标志是美国国防部制定的彩虹系列中的桔皮书（TCSEC）以及欧洲四国制定的ITSEC，TCSEC以信息安全的保密性为主，ITSEC则强调保障信息的保密性、完整性、可用性（即著名的信息安全三原则C·I·A）。这种环境下的信息安全可以归纳为对信息系统的保护，即信息安全（INFOSEC）。当时采用的防护手段主要包括加密技术、身份鉴别、访问控制、系统审计等安全机制，主要保证动态信息在传输过程中不被窃取，即使窃取了也不能读出正确的信息；此外还要保证数据在传输过程中不被篡改，让读取信息的人能够看到正确无误的信息。1983年美国国防部公布的可信计算机系统评价准则标志着计算机信息系统保密性问题的研究和应用迈上了新台阶。这一时期，国际上把相应的信息安全工作称为数据保护。

在20世纪70年代晚期，微处理器开创了计算机性能的新纪元。使用这种微处理器技术构建的个人计算机成为现代计算机的主流，从而使数据中心不再是数据的唯一来源。随着数据的分散，资源共享的需求在20世纪80年代开始增多，并促使个人计算机用户把他们的机器互联起来。这种联网能力既适用于大型机，也适用于微型机，所以用户能把所有计算资源整合在一起工作。信息安全矛盾逐渐由军方需求发展到商业和其他更广泛的应用领域。采用包过滤技术的第一代防火墙也在这一时期与路由器同时出现。1989年，贝尔实验室的Dave Presotto和Howar Trickey推出了第二代防火墙技术，即电路层防火墙，同时他们提出了第三代防火墙——应用层防火墙（代理防火墙）的初步结构。

3. 信息安全的发展期——信息安全保障时期

20世纪90年代以来，计算机网络迅速发展，信息无论是对内还是对外都得到了极大的开放，由此产生的信息安全问题跨越了时间和空间，此时的安全威胁已经演变成在网络环境中的黑客入侵、病毒破坏、计算机犯罪、情报窃取等。信息安全的焦点已经不仅仅是传统的保密性、完整性和可用性三个原则了，还衍生出了诸如可控性、抗抵赖性、真实性等其他的原则和目标。网络环境下的信息安全概念的产生，也使信息安全转化为从整体角度考虑其体系建设的信息保障阶段。人们需要保护信息在存储、处理、传输、利用过程中不被非法访问或修改，确保合法用户得到服务和拒绝非授权用户使用。互联网跨越了时间和空间的限制，也给信息安全带来了新的挑战，安全不再局限于对信息的静态保护，而需要对整个信息和信息系统进行保护和防御（深层防御），因此在新的形势下出现了信息保障（IA）。

信息保障是信息安全发展的最新阶段，信息保障的概念最早源于美国。1996年美国国防部对信息保障作了如下定义：保护和防御信息及信息系统，确保其可用性、完整性、保密性、可认证性、不可否认性等特性。这包括在信息系统中融入保护、检测、反应功能，并提供信息系统的恢复功能。美国国家安全局（NSA）于1998年制定了《信息保障技术框架》（IATF），提出了“深度防御策略”，并于2002年9月颁布了《信息保障技术框架》3.1版本。目前信息保障已经成为美国等发达国家的国家战略。世界各国信息安全领域的研究，已经从早期的通信保密转为信息安全并发展到目前的信息保障阶段。防火墙技术、虚拟专用网、入侵检测等完整的安全解决方案在这个阶段也开始成为主角。

我国从20世纪70年代中期开始研究计算机与网络的安全保密系统，并于1985年发

布了第一个与信息安全相关的标准：信息技术设备和设施安全管理标准 GB4943。1994 年，国务院发布了《中华人民共和国计算机信息系统保护条例》。2006 年，在《中华人民共和国国民经济和社会发展第十一个五年规划纲要》第十五章第四节中阐述道：积极防御、综合防范，提高信息安全保障能力；强化安全监控、应急响应、密钥管理、网络信任等信息安全基础设施建设；加强基础信息网络和国家重要信息系统的安全防护；推进信息安全产品产业化；发展咨询、测评、灾难备份等专业化信息安全服务；健全安全等级保护、风险评估和安全准入制度。我国信息安全技术虽起步较晚，但起点高，发展迅速，无论从产业发展阶段、国家政策，还是从外部环境来看，与国际上先进国家的差距正在缩小，这预示着我国的信息安全产业将由此迈入一个快速发展的新阶段。

1.2 信息安全的概念

1.2.1 什么是信息安全

信息安全本身没有目标、边界和特征，只是由于信息和信息系统的所有者、管理者、使用者、监管者的存在，才具备可测量特征。信息及其系统是受安全的目标和需求驱动的。从工业时代进入信息时代后，信息、物质、能源成为了人类社会赖以生存和发展的三大基本要素。信息安全决定国家信息主权。信息时代，强国推行信息强权和信息垄断，依仗信息优势控制弱国的信息技术。知识经济时代，竞争首先表现为科技竞争，科技竞争的重点是对信息技术这一制高点的争夺。信息、资本、人才和商品的流向逐渐呈现出以信息为中心的竞争新格局。信息安全就成为影响国家政治命脉、经济发展、军事强弱的关键因素。

在信息时代，国家的安全观发生了显著变化，信息成为国家的重要战略资源。高效能的信息技术在推动人类社会发展的同时，信息安全已成为一个不可或缺的因素，甚至会演变为信息技术的一个最基本要素。那么它的本质到底是什么呢？

通常安全被定义为“免受危险的性质或者状态”，也就是防备敌人和其他损害。例如，国家安全是一个保护主权、资产、资源和人民安全的多层次系统。

◆ ISO 对“计算机安全”定义为：“为数据处理系统建立与采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。”这种定义可以理解为静态信息保护。另一种定义是：“计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行。”这种定义可以理解为动态信息保护。

◆《中华人民共和国计算机信息系统安全保护条例》中将信息安全界定为“保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行”。因此，所谓计算机信息系统的信息安全是指防止信息被故意的或偶然的非法授权泄漏、更改、破坏或使信息被非法系统辨识、控制，即确保信息的保密性、完整性、可用性、可控性。

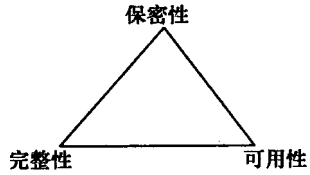
◆ 我国计算机信息系统安全专用产品分类原则给出的定义是：“涉及实体安全、运行

安全和信息安全三个方面。”

◆ 美国国家安全局信息保障主任给出的定义是：“因为术语‘信息安全’一直仅表示信息的保密性，在国防部我们用‘信息保障’来描述信息安全，也叫‘IA’。它包含五种安全服务，包括保密性、完整性、可用性、真实性和不可抵赖性。”

1.2.2　信息安全的三要素

信息系统安全的三个基本原则：保密性、完整性和可用性（C・I・A）（图 1-1）。



1-1　信息安全的基本原则

图 1-1 体现了信息安全的基本原则。所有的信息安全控制、安全措施以及所有的威胁、脆弱性和安全过程都满足 C・I・A 的标准。BS7799 标准中指出：信息安全主要指信息的保密性、完整性和可用性的保持。即指通过采用计算机软硬件技术、网络技术、密钥技术等安全技术和各种组织管理措施，来保护信息在其生命周期内的产生、传输、交换、处理和存储的各个环节中，信息的保密性、完整性和可用性不被破坏。

◆ 保密性：是指确保只有那些被授予特定权限的人才能够访问到信息。信息的保密性依据信息被允许访问对象的多少而不同，所有人员都可以访问的信息为公开信息，需要限制访问的信息为敏感信息或秘密信息。根据信息的重要程度和保密要求将信息分为不同密级，例如《中华人民共和国保守国家秘密法》根据秘密泄露对国家经济、安全利益产生的影响不同，将国家秘密分为秘密、机密和绝密三个等级。组织可根据其信息安全的实际情况，在符合《中华人民共和国保守国家秘密法》的前提下将其信息划分为不同的密级，另外，信息的保密性有时效性，如秘密到期解密等。

◆ 完整性：一方面是指在使用、传输、存储信息的过程中保持信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性；另一方面是指信息处理方法的正确性。

◆ 可用性：是指保证被授权人在需要时能使用相关的信息资产，保证信息系统对信息的发送、存储和处理是正常和不间断的，并按要求能正常使用或在非正常情况下能恢复使用的特性，即在系统运行时能正确存储所需信息，当系统遭受攻击或破坏时，能迅速恢复并能投入使用。

除此之外，还要保证信息的真实性和不可否认性。真实性是信息保持真实或最初状态的质量和状态，而不是信息的复制或伪造。不可否认性指通信双方在信息交互过程中，确信参与者本身及参与者所提供的信息的真实同一性，即所有参与者都不能否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

1.3 信息系统的安全威胁

1.3.1 黑客

1. 黑客定义

黑客是英文“Hacker”的音译。动词原形为“Hack”，意为“劈”、“砍”。英文词典这样解释黑客行为：未经授权进入一个计算机的存储系统，如数据库。中文译成“黑客”，贬义似乎略重，有“未经允许”等不合法的含义。在早期麻省理工学院（MIT）的校园俚语中，“黑客”则有“恶作剧”之意，尤其指那种手法巧妙、技术高明的恶作剧，并且带有反既有体制的色彩。全球著名的微软公司在其1996年出版的百科全书（光盘版）里曾对黑客定义：从20世纪80年代开始，黑客这个词作为对一些人的称谓出现在计算机软件和计算机技术里。黑客有轻蔑的含义，通常是指喜欢通过个人计算机和拨号上网秘密地侵入另外一些计算机或计算机网络，然后查看或破坏存储在其中的数据和程序的人。更精确地说，黑客就是指那些通过不合法的途径进入别人的网络寻找意外满足的人。如今在公众眼中，黑客又更多地与电脑破坏分子联系在一起。

2. 黑客的分类

黑客行为界定的模糊不清使黑客分类情况变得错综复杂。黑客通常分成三个阵营(图1-2)。

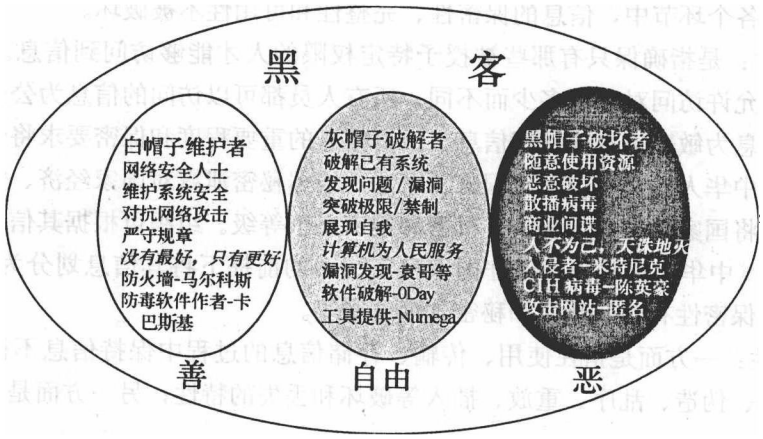


图1-2 黑客的分类

白帽子：网络安全人士。试图破解某个系统或网络以提醒该系统所有者的系统安全漏洞。这群人往往被称作“白帽黑客”或“思匿客”（Sneaker）。许多这样的人是电脑安全公司的雇员，并在完全合法的情况下攻击某系统。

灰帽子：最早来源于L0pht（一个非常出名的黑客团体），宣称建立一个“阁楼”——以示其既和组织安全测试员有区别，又不愿意和臭名昭著的黑帽子们搅在一起。这个词定义的大多数人和很多组织安全研究员一样是安全专家和顾问，但其更加独立。“我们用‘灰帽子’来代表那些独立的研究员，他们不是只对某一个特定的公司或产品感

兴趣”。@Stake（一家安全公司，由 L0pht 黑客中的核心成员组建）的研究和发展总监 Chris Wysopal 表示，“灰帽子”通常是指一般意义上的黑客。

黑帽子：就是骇客，主要是以网络攻击为主，带有主观恶意（一般是非法）的试图破解或破坏某个程序、系统及网络安全的人。这个定义常常对那些符合条件的黑客造成严重困扰，媒体将这群人称为“骇客”（Cracker）。有时这群人也被叫做“黑帽黑客”（“脚本小孩”则指那些完全没有或仅有一点点骇客技巧，而只是按照指示或运行某种骇客程序来达到破解目的的人）。

3. 信息安全界有代表性的人物

（1）防火墙的发明人——马尔科斯

马尔科斯是世界知名的安全专家，被公认为是代理防火墙的发明人，是第一个商业防火墙和早期的入侵检测系统的实现者，获得互联网安全大会（TISC）的 CLUE 大奖和 ISSA 终身成绩奖等多项奖项。马尔科斯从事安全工作已有十多年之久，比商业互联网的出现还早六七年，网民多称他为“防火墙之父”。他认为，现在人们把安全弄得很难、很复杂、很神秘、很时髦，也很前卫。人们对待网络安全就像对待火箭科学，甚至像是对待犯罪现场取证的学问一样，但事实是，计算机和网络安全真的是一件相当简单的事情。马尔科斯基于这套理论，对网络安全开出了安全药方。其基本的内容是：

◆ 所有缺省的安全策略是拒绝所有（Deny All），然后只准许那些必需的服务。

◆ 尽可能少地提供服务，记录这些服务的使用日志，对应用的错误进行检测，当然也可以进行入侵检测。

◆ 了解网络上在运行什么，如果管理员不知道网络的运行状况，怎么确保安全？内部尽可能隔离，隔离往往是最好的办法。不安全格式的内容尽可能不要流入内部，除非它是从可靠渠道来的。

◆ 了解防火墙上流出的流量是什么，如果了解了，也就不需要什么高级工具来判断木马、间谍软件、病毒、非授权访问等。

◆ 最好全部七层都进行控制，而不只是一层，深层防御不是只在一层。

◆ 不要浪费时间天天打补丁，如果你天天在打补丁，那么你已经被误导。

◆ 移动办公隔离到一个独立的区，移动办公很好，可是不安全。

◆ 防病毒软件很好，但不要指望天天升级。最好了解内部网络上使用的都是些什么软件。

◆ 不要指望用户理解你的安全策略是什么，简单地说明该怎么做。

◆ 安全外包是一个坏办法，除非你可以接受你的安全交给别人掌握。

（2）加密工具创始人——Philip Zimmermann

精明且具有商业头脑的 Zimmermann 想开发一种加密方面的产品，并提供一整套的解决方案，允许用户安全地存储文件和在 BBS 上发表信息，而这些电子文档不会遭到窃听与篡改。出于这一目的，他找到了公钥和对称密钥加密方法之间的均衡点——PGP（Pretty Good Privacy）。1991 年，他编写了 PGP 的第一个版本。PGP 是一个基于 RSA 公钥加密体系的邮件加密软件，其创造性在于把 RSA 公钥体系的方便和传统加密体系的高速结合起来，并且在数字签名和密钥认证管理机制上有巧妙的设计，成为目前几乎最流行的公钥加密软件工具。

(3) 尤金·卡巴斯基 Eugene Kaspersky

Eugene Kaspersky 现在是国际信息安全领域的顶尖级专家之一，计算机反病毒研究组织（CARO）的成员，对计算机病毒学所涵盖的问题在全球的很多专业会议上发表过大量文章和评论。

他出生于俄罗斯，1989 年在他的计算机上检测到 Cascade 病毒后，开始研究计算机病毒。1991 年至 1997 年在 KAMI 信息技术中心工作，在一组助手协助下开发出“AVP”反病毒方案（2000 年 11 月更名为卡巴斯基反病毒软件），1997 年卡巴斯基实验室股份有限公司成立。

1.3.2 攻击技术的分类

1. 攻击技术的分类

一个合理的，并且满足实际应用需求的攻击分类方法应包含六个特征：互斥性（分类类别不应重叠）、完备性（覆盖所有可能的攻击）、非二义性（类别划分清晰）、可重复性（对一个样本多次分类结果一致）、可接受性（符合逻辑和直觉）和实用性（可用于深入研究和调查）。不少分类的研究工作致力于提出一个满足上述标准的攻击分类体系，但都存在一定的不足。目前已有的攻击技术分类方法可以分为以下几种：一是基于经验术语的分类；二是基于单一特征的分类；三是基于属性的分类。

(1) 基于经验术语的分类

业界最初经常采用经验术语的分类方法。这种方法试图用一组术语对攻击的发起者、实施方法、技术实现、产生的后果等多个属性进行描述。这是一种利用攻击中常见的技术术语、社会术语等对攻击进行描述的方法。例如可以将攻击技术分为：病毒、蠕虫、拒绝服务、特洛伊木马、钓鱼、搭线窃听、IP 欺骗、软件盗版、越权访问、扫描、逻辑炸弹、电磁泄露等二十余类。

根据经验的分类方法，在描述攻击方法时存在一定的不确定性。第一，术语很难表现出其在相同或相近的技术层面的关联关系，而且差距过大。例如，IP 欺骗属于技术术语，而软件盗版则属于社会活动的范畴。第二，这种分类方法的适用性较差，且交叉过多。例如扫描与越权访问，扫描行为中包含的许多攻击方法也涉及越权访问的内容。又如病毒与特洛伊木马的关系也是模糊的，因此很难进行类别的区分。

基于术语的分类方法往往是根据经验确定的，虽然易于理解，但在逻辑性和层次结构上则存在不清晰、目的性不强的缺点，而且所采用的术语往往很难在专业层次上得到认同。

(2) 基于单一特征的分类

基于单一特征的分类是指仅从攻击某个特定的属性而对攻击进行描述的方法。

从系统滥用的角度将攻击分为九类：外部滥用、主动滥用、被动滥用、恶意滥用、间接滥用、硬件滥用、伪造、有害代码、绕过认证或授权。并进一步将其细化为 26 种具体的滥用攻击。

从实施方法的角度将攻击分为五类：中断、拦截、窃听、篡改、伪造。Jayaram 也根据攻击的实施方法将攻击分为物理攻击、系统弱点攻击、恶意程序攻击、权限攻击和面向