21世纪高等职业教育计算机系列规划教材

信息安全基础

胡国胜　张迎春　主　编
孟庆华　孙修东　周巧婷　副主编

涉及技术前沿的无线局域网安全、云计算与云安全技术

将信息安全技术以案例、故事和实验为载体，让学习变得轻松

配备课件

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

21 世纪高等职业教育计算机系列规划教材

信息安全基础

胡国胜　张迎春　主　编

孟庆华　孙修东　周巧婷　副主编

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书为计算机网络技术专业的入门教材。作者根据高职学生的特点及人才培养目标，通过案例和故事引出信息安全概念，诠释信息安全内涵，通过操作让学生初步掌握必备的安全技术和技能。全书共分 14 章，内容包括信息与信息安全认识、物理安全与信息安全风险评估、经典信息加密方法、信息加密应用、信息隐藏与数字水印操作、黑客与系统嗅探、黑客攻击技术、攻击防范技术、病毒防治、操作系统安全管理、无线局域网安全与管理、数据备份与恢复、云计算与云安全、信息安全法律法规案例分析。

本书融知识与趣味于一体，以案例、故事和实验为载体，理论联系实际，帮助学生全面掌握信息安全基础知识，易学易用。本书可以作为高职高专计算机信息类专业的教材，也可以作为企事业单位网络信息系统管理人员的技术参考用书。

图书在版编目（CIP）数据

信息安全基础 / 胡国胜，张迎春主编. —北京：电子工业出版社，2011.3
（21 世纪高等职业教育计算机系列规划教材）
ISBN 978-7-121-12169-2

Ⅰ. ①信… Ⅱ. ①胡… ②张… Ⅲ. ①信息系统－安全技术－高等学校：技术学校－教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2010）第 213711 号

策划编辑：徐建军
责任编辑：徐建军　　特约编辑：关山美
印　　刷：涿州市京南印刷厂
装　　订：涿州市桃园装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：18.5　字数：473.6 千字
印　　次：2011 年 3 月第 1 次印刷
印　　数：4 000 册　　定价：31.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着计算机技术、网络技术和通信技术的发展，人们在享受信息资源的同时，也面临着信息安全方面的威胁。信息安全已经成世界性的现实问题，已影响到政治、经济、军事、文化和意识形态等领域，甚至威胁到国家安全。信息安全也是保护个人隐私和保证社会稳定的必要前提。高职信息安全技术专业是适应社会发展需要而开设的急需专业。

高职信息安全技术专业自2003年开设至今，还没有一本系统介绍该专业的入门教材，很多院校用网络安全技术教材作为该专业的入门教材，而事实上网络安全技术只是信息安全的一部分，很多同学在学完专业课后还没弄明白信息的概念和信息安全的内涵。

目前，市场上的网络安全技术教材重技术轻管理、重技能轻素质、重应用轻思维。在传授知识和技能的同时，要注重培养学生增强信息安全管理意识，提高职业道德和职业素养，加强法律法规教育和提高分析问题、解决问题的能力。这些对信息安全技术专业学生尤其重要，很多黑客受到利益的驱使，加之缺少法律意识，最终走上犯罪道路。因此，我们有义务培养学生学会利用相关法律法规条文解读现实案例，保护自己，提高法律意识。

目前大多网络安全技术的教材对加、解密算法采取回避方法。对信息安全技术专业学生来说，弄清有关密码的基本概念和密码体系是完全有必要的，如对称加密和非对称加密等。在讲述RSA算法时，几乎现有所有教材都采用本科教材的案例，不利于学生去验证RSA加密和解密算法，不利于掌握RSA精辟思想，对高职学生需要进行简化。当然，授课时，老师可以根据授课对象来选择教学的内容及讲述的深度。

大多现有教材没有涉及信息隐藏技术和云安全内容，其实信息隐藏技术在现实版权保护和潜信道方面应用广泛，操作起来比较简单；云安全在木马病毒查杀中已显出巨大的威力。这些不是概念，我们有必要将这些最前沿的知识介绍给学生。

鉴于上述几点，我们编写了本书。本书全面介绍了信息与信息安全知识、物理安全和安全评估、基本加密和解密的方法、网络的攻防技术和工具、信息隐藏和数字水印操作方法、操作系统安全管理、无线局域网安全与管理、云安全与信息安全法律法规等内容。

在本书编写的过程中，张迎春老师和周巧婷老师编写了第9章和第10章，孟庆华博士、孙修东老师编写了第8章，计大威老师编写了第8章和第11章部分的实训内容，张迎春老师和蔡军英老师参与了部分图表的制作，其余部分由胡国胜老师编写完成，最后校对和统稿由胡国胜和张迎春老师共同完成。邱洋、李曼、范晓燕也参加了部分内容的编写工作。我们的同事们在本书写作过程中提供了很多帮助，在此一并表示感谢。

在写作过程中，作者参考了书后参考文献中的专著、教材和网站内容，并部分引用，在此对其作者表示衷心感谢，由于疏忽，书中部分引用内容没有标明出处，在此对相关作者表示诚挚的歉意。

为了方便教师教学，本书配有电子教学课件，请有需要的教师登录华信教育资源网（www.hxedu.com.cn）免费注册后进行下载，如有问题可在网站留言板留言或与电子工业出版社联系（E-mail：xujj@phei.com.cn），也可以与作者联系（E-mail：jamhu8@sohu.com）。

虽然编写本书花了较长时间，并经过多次改稿，但书中难免存在疏漏和不足，希望同行专家和读者能给予批评和指正。

编　者

目　录

第 1 章　信息与信息安全认识 …… （1）
1.1　现实中的安全问题 …… （2）
1.1.1　奥巴马的决定 …… （2）
1.1.2　两个事件 …… （3）
1.1.3　两个案例 …… （4）
1.1.4　三个故事 …… （5）
1.1.5　五个困惑 …… （7）
1.2　区分信息、消息、数据、信号与通信 …… （8）
1.2.1　信息、消息、数据与信号的区别 …… （8）
1.2.2　信号与通信关系 …… （9）
1.3　信息安全的内涵 …… （10）
1.3.1　从电影《谍中谍》认识信息安全 …… （10）
1.3.2　什么是信息安全 …… （12）
1.3.3　信息安全的发展过程 …… （13）
1.4　网络脆弱性分析 …… （17）
1.5　信息安全威胁分析 …… （18）
1.6　信息安全模型 …… （18）
第 2 章　物理安全与信息安全风险评估 …… （20）
2.1　安全管理的重要性 …… （21）
2.2　物理安全涉及的内容和标准 …… （23）
2.2.1　机房与设施安全 …… （23）
2.2.2　防火安全 …… （26）
2.2.3　电磁泄漏 …… （28）
2.3　开展风险管理 …… （30）
2.3.1　风险识别 …… （30）
2.3.2　风险评估 …… （32）
2.3.3　风险控制策略 …… （37）
第 3 章　经典信息加密方法 …… （40）
3.1　从恩尼格玛密码机认识密码 …… （41）
3.2　初识密码学 …… （43）
3.2.1　从密码的起源了解密码 …… （43）
3.2.2　从基本概念了解密码 …… （46）
3.2.3　古典密码体系的演化 …… （49）
3.2.4　对称密码算法的精粹 …… （53）
3.2.5　非对称加密算法的神奇 …… （61）
3.2.6　混合加密体系 …… （64）
3.2.7　统计分析法 …… （65）

第 4 章　信息加密应用 …… (67)
4.1　CA 认证 …… (67)
4.2　认识散列函数 …… (68)
4.2.1　散列函数 …… (68)
4.2.2　散列函数的应用——MD5 算法 …… (71)
4.3　PGP 加密与使用 …… (74)
4.3.1　PGP 工作原理 …… (74)
4.3.2　PGP 软件包的使用 …… (75)
4.3.3　创建并导出密钥对 …… (77)
4.3.4　文件的加密与解密 …… (78)
4.3.5　使用 PGP 销毁秘密文件 …… (80)
4.3.6　PGP 邮件加密与解密、签名与验证 …… (80)
4.4　电子签名 …… (82)
4.5　数字签名 …… (83)
4.6　认证机构 CA …… (84)
4.7　数字证书 …… (85)
4.7.1　数字证书的作用 …… (86)
4.7.2　Windows XP 中的证书 …… (86)
4.7.3　数字时间戳服务（DTS） …… (87)
4.8　认证技术 …… (88)
第 5 章　信息隐藏与数字水印操作 …… (90)
5.1　两个故事 …… (91)
5.2　信息隐写术 …… (93)
5.2.1　数字水印 …… (94)
5.2.2　潜信道 …… (96)
5.3　信息隐藏软件应用 …… (97)
5.3.1　图片水印制作 …… (97)
5.3.2　视频水印制作 …… (101)
5.3.3　音频隐形水印制作 …… (103)
第 6 章　黑客与系统嗅探 …… (105)
6.1　案例 …… (105)
6.2　OSI 模型 …… (106)
6.3　TCP/IP 模型与 OSI 模型的关系 …… (107)
6.4　网络扫描 …… (108)
6.4.1　黑客 …… (108)
6.4.2　黑客入侵攻击的一般步骤 …… (111)
6.5　实施攻击的前期准备 …… (112)
6.5.1　网络信息收集 …… (112)
6.5.2　进行网络扫描 …… (117)
6.5.3　进行网络监听 …… (123)

第 7 章　黑客攻击技术 …… （132）
7.1　从案例认识黑客逐利本性及危害性 …… （132）
7.2　黑客攻击的一般步骤 …… （133）
7.3　黑客如何实施攻击 …… （134）
7.3.1　口令破解攻击 …… （134）
7.3.2　缓冲区溢出攻击 …… （141）
7.3.3　欺骗攻击 …… （144）
7.3.4　DoS/DDoS 攻击 …… （147）
7.3.5　SQL 注入攻击 …… （149）
7.3.6　网络蠕虫攻击 …… （150）
7.3.7　木马攻击 …… （151）
第 8 章　攻击防范技术 …… （156）
8.1　两个案例 …… （156）
8.2　防火墙 …… （157）
8.2.1　认识防火墙 …… （157）
8.2.2　防火墙技术 …… （159）
8.2.3　防火墙的体系结构 …… （164）
8.2.4　个人防火墙应用演示 …… （167）
8.3　入侵检测技术 …… （169）
8.4　VPN 技术 …… （171）
8.4.1　认识 VPN …… （171）
8.4.2　VPN 组建实例 …… （174）
8.5　“蜜罐”技术 …… （182）
第 9 章　病毒防治 …… （184）
9.1　笑话与事实 …… （184）
9.2　认识计算机病毒 …… （186）
9.2.1　了解病毒的起源和发展 …… （186）
9.2.2　病毒和木马技术发展趋势 …… （189）
9.2.3　病毒的特征和分类 …… （190）
9.3　从病毒命名看特性 …… （191）
9.4　典型病毒分析与消除 …… （193）
9.5　认识恶意代码 …… （201）
第 10 章　操作系统安全管理 …… （204）
10.1　操作系统入门 …… （204）
10.1.1　混沌初开 …… （204）
10.1.2　Windows 的精彩世界 …… （205）
10.1.3　Linux 的自由天地 …… （206）
10.2　系统安全始于安装 …… （207）
10.3　Linux 系统安全 …… （207）
10.3.1　引导系统时——GRUB 加密 …… （207）
10.3.2　进入系统时——身份认证 …… （208）

10.3.3 使用系统时——权限设置 …… (210)
10.3.4 网络通信时——数据加密 …… (211)
10.3.5 提供服务时——访问控制 …… (211)
10.3.6 贯穿始终的安全分析 …… (212)
10.4 Windows 系统安全 …… (213)
10.4.1 保护 Windows 系统安全的基本措施 …… (213)
10.4.2 使用 MBSA 检查系统漏洞 …… (216)
10.4.3 综合案例 …… (217)
第 11 章 无线局域网安全与管理 …… (222)
11.1 无线局域网 …… (222)
11.2 无线局域网典型设备 …… (223)
11.3 无线局域网安全技术 …… (226)
11.4 无线攻击方法 …… (230)
11.4.1 方法与过程 …… (230)
11.4.2 空中传播的病毒 …… (231)
11.5 无线网络安全防御措施 …… (232)
11.6 无线安全管理实例 …… (236)
第 12 章 数据备份与恢复 …… (242)
12.1 初识数据备份与恢复 …… (242)
12.2 Windows 数据备份典型方法 …… (243)
12.2.1 备份系统文件 …… (243)
12.2.2 备份硬件配置文件 …… (244)
12.2.3 备份注册表文件 …… (245)
12.2.4 制作系统的启动盘 …… (245)
12.2.5 备份整个系统 …… (246)
12.2.6 创建系统还原点 …… (246)
12.2.7 恢复上一次正确配置 …… (247)
12.2.8 返回驱动程序 …… (247)
12.2.9 硬件配置 …… (247)
12.2.10 一键还原 …… (247)
12.3 巧用数据恢复软件 …… (248)
第 13 章 云计算与云安全 …… (252)
13.1 Animoto 的创业故事 …… (252)
13.2 云计算 …… (253)
13.3 云计算就在我们身边 …… (254)
13.4 云计算的演变 …… (256)
13.5 云计算的特点 …… (257)
13.6 云计算的定义 …… (258)
13.7 判断云计算 …… (259)
13.8 云安全 …… (259)
13.9 云安全的特点 …… (262)

13.10 瑞星“云安全”计划 …… (263)
13.11 趋势科技云安全解决方案 …… (265)
13.11.1 基于特征码的传统解决方案已经过时 …… (265)
13.11.2 全新的“云安全”网络防护解决方案 …… (265)
13.11.3 趋势科技“云安全”技术架构 …… (266)
13.11.4 Secure Cloud 云安全特点 …… (268)
第 14 章 信息安全法律法规案例分析 …… (269)
14.1 信息安全中的法律问题 …… (269)
14.1.1 何为犯罪 …… (269)
14.1.2 计算机病毒问题 …… (271)
14.1.3 民事问题 …… (273)
14.1.4 隐私问题 …… (274)
14.2 案件分析 …… (275)
附录 A 常用端口大全 …… (279)
附录 B 重要标准文件 …… (280)
参考文献 …… (281)

第 1 章　信息与信息安全认识

无恃其不来，恃吾有以待也；无恃其不攻，恃吾有所不可攻也。

——《孙子兵法》

一人之事，不泄于二人；明日所行，不泄于今日。

——《兵经百言》

信息安全在古代就已经受到了智者、军事家和政治家的重视。随着社会信息化程度的提高，信息安全与人们生活已息息相关，同时，信息安全面临诸多挑战。无论是个人计算机、手机、卫星、精确制导武器、网络安全，还是企业、事业、政府都回避不了信息安全。信息安全甚至关系到国家的安全。

信息安全涉及的领域很广，主要包括数学、物理、微电子、通信、计算机等，有着系统的技术体系和丰富的科学内涵，初学者要准确、全面把握信息安全的概念并非易事。

本章主要目的是帮助学生正确区别信息、消息、信号等基本概念；理解通信基本模型；正确认识信息安全的内涵及发展过程；了解网络面临的安全威胁及信息安全模型。

20 世纪 90 年代以来，我国信息产业持续高速发展，已经成为国民经济第一支柱产业。未来三年，电子信息产业销售收入保持稳定增长，产业发展对国民生产总值（GDP）增长的贡献不低于 0.7%，三年新增就业岗位超过 150 万个。到 2008 年年底，全国固定电话用户和移动电话用户位居世界第一，中国网民达到 2.44 亿人。金融、外贸、海关、税务、科技、教育等近千个部门已经成功组建了中国计算机信息应用系统；网上购物、网上教育、远程医疗也改变着我们习惯已久的生活方式。在全球范围内电子商务发展日趋成熟的情况下，电子政务又成为新的发展热点，现已注册各级政府网站 18 000 多个。构筑安全、便捷、畅通的数字化政务空间，是我国电子政务建设的主要目标。我国启动了国家信息化建设，信息技术和网络技术在各个行业技术改造和结构调整发挥了非常重要的作用，以信息化带动工业化，实现社会生产率快速提高。

信息技术在带给人们前所未有的便利和巨大效益的同时，也使人们面临信息安全方面的巨大挑战，在网络世界内，每个个人、团体、国家都可以自由表述自己的观点，实施自己的行为。恐怖分子、犯罪集团也在利用网络组织和实施恐怖、犯罪活动。黑客组织直接以网络为目标进行恶性攻击，敌对势力对意识形态领域的渗透和对政府、军队秘密信息的窃取，给我国主权、国家安全和社会稳定带来极大的威胁。更令人担忧的是，我国信息化规模的高速发展建立在大规模引进国外新兴信息技术基础之上，我国信息化产品自主化水平还很低，在计算机和公用网络的软硬件技术方面，国内只在微机等低端产品上有数量优势，而中央处理器和操作系统几乎完全建立在美国公司产品的基础上。在大型设备和通信设备方面，运行在其上的系统软件、支撑软件也大多数是国外的产品，一旦我们所依赖的国外核心技术得不到保证，或存在严重的安全隐患，势必对我国的信息安全和国家安全造成严重的后果。

信息安全自古以来一直受到人们的重视。我国春秋时代的军事家孙武（公元前 535 年—？）在《孙子兵法》中写道：“能而示之不能，用而示之不用，近而示之远，远而示之近。”这体现了孙武对军事信息保密的重视。古罗马统治者 Caesar（凯撒，公元前 100 年—公元前 44 年）曾使用字符替换的方法传递情报。本节从美国总统奥巴马的决定、谷歌事件、电影故事和一

些困惑说起，引入信息安全概念、信息安全的定义、信息系统的安全威胁及信息安全发展的过程。

1.1　现实中的安全问题

信息安全已经深入社会生活的各个领域。为了让同学们更好地理解信息安全的重要性，我们从一些典型的事件、案例、故事和困惑入手。

1.1.1　奥巴马的决定

奥巴马（Barack Obama）关注网络安全，招募青年才俊组建“黑客”部队。据《纽约时报》2009 年 5 月 31 日报道（如图 1-1 所示），美国政府日益重视计算机网络安全，奥巴马认为来自网络空间的威胁已经成为美国面临的最严重的经济和军事威胁之一。由于美国当前仍未脱离金融危机困境，诺斯洛普·格鲁门公司（Northrop Grumman）、美国通用动力公司（General Dynamics）、洛克希德·马丁公司（Lockheed Martin）及雷神公司（Raytheon Company）等美国军方和情报机构、国防承包商，更容易招揽到过去向往硅谷高科技公司的年轻网络天才。五角大楼也已经招募数千名“黑客士兵”，网络战已经被纳入美国战争规划中。

图 1-1　《纽约时报》新闻（http://www.nytimes.com）

在大多数企业不断裁员瘦身之际，这些国防承包商却迅速行动起来，通过并购小型高科技公司、资助学院研究计划和刊登广告征求“网络忍者”等手段，招聘 20 岁出头的网络天才，以加强美国的信息战能力。这些年轻人在肯尼迪航天中心和五角大楼的机密实验室中，边听震耳欲聋的摇滚乐，边探测国家网络的安全漏洞，并研发计算机网络防护软件，阻止各种入侵攻击，或反击敌对国家的网络攻击，他们被称为“黑客战士”。

诺斯洛普·格鲁门、通用动力及雷神公司主要研究先发制人的主动出击型信息战，找出其他国家计算机网络系统的安全弱点，并研发软件工具以瘫痪敌方系统或窃取其中机密信息。雷

神还在设计一种名为“蜜罐（Honeypot）”的数码陷阱，以伪装成国防部网站等引诱黑客上钩，然后再解析黑客发动攻击的软件程序码，以阻挡黑客入侵。

据 20 多岁的军方情报机构人员哈丁（Hardin）估计，目前美国军方有 3000～5000 名信息安全专家，另有 50 000～70 000 名官兵参与一般的计算机相关任务。若再加上电子战等领域的专家，美军信息战部队总人数已超过 88 700 人。

《纽约时报》报道，奥巴马签署一份密令，成立军方网络司令部。这一举动表明，美国认为随着自己武库中计算机武器不断增加，美国必须制定战略，如何在未来各种可能的冲突中使用它们，不管是将它们作为威慑力量还是与常规武器一起使用。美国官员尚未说明是否会主动发起网络进攻，但他们认为网络战可以与常规战争相提并论。

1.1.2　两个事件

事件 1：谷歌事件

美国政府为谷歌（Google）提无理要求撑腰，对中国监管互联网发难。美国总统奥巴马 2010 年 1 月 22 日表态支持希拉里（Hilary Duff Ceinton），而希拉里 1 月 21 日以颇受争议的讲话（在华盛顿演讲主题是美国如何对待互联网自由）力挺在中国惹出麻烦的谷歌公司，这一奇怪的美国“官商勾结”的链条惊动了全世界。

谷歌成为美国外交工具。谷歌威胁撤出中国之前曾与美国政府沟通。美国《赫芬顿邮报》网站刊文披露，1 月 7 日，希拉里在国务院举行晚宴，主题是如何利用高科技推动美国在世界范围的外交，嘉宾之一就是谷歌全球首席执行官（CEO）埃里克·施密特（Eric Schmidt）。希拉里称，如果美国的外交政策“要鼓励公民社会发展、反抗暴力与压迫，像 Twitter、Google、YouTube 那样都是十分重要的 21 世纪的工具”，这就是 21 世纪战略的一部分：利用技术工具的力量推动全球外交。文章说，“通过政府与企业领导人的合作，我们正团结一致谋划如何最有效率地利用数字技术工具在全世界推动外交”。美国外交政策网站说美国正在多个国家推动“公民社会 2.0”运动，就像之前推出的“美国之音”和“欧洲自由之声”，鼓励寻求自由和公民权利的草根运动。

全球最高端的互联网技术政策专家博客网 CIRCLEID 曾打比方说，美国的互联网特殊地位一直就是国际社会的一根刺。美国《新科学家》杂志写道：每当你上网、发邮件或下载音乐时，背后有一个看不见的力量在运作，确保你连上你想去的网站、邮箱和数据库。这个强大的力量叫什么？美国政府。在欧洲，几年前以法德为首的欧洲经济和科技界巨头就齐聚柏林启动了“Quaero”计划，谋略打造能与谷歌相抗衡的超级搜索引擎，一些欧洲媒体甚至满怀期待将其称为“谷歌杀手”。2008 年年底，欧洲数字图书馆在布鲁塞尔开馆，被称为针对美国文化侵袭的象征。

新加坡《联合早报》说，“美国政商再次联手，以维护信息自由流通为名义，以谷歌退出中国市场为要挟，试图在政治效应和商业利益上双双获利。这是美国政治和资本彼此呼应、相互支持的最新事例”。这篇题为“中美之间操控与反操控”的文章说，帝国本性的主要特征之一，就是企图操控他国政策，目的是要使自身利益最大化，继而不断扩张本国资本的全球影响力。在当前全球化时代，虽然帝国的暴力倾向在减弱，但操控他国政策的本性没有改变。美国近年来试图操控中国汇率政策就是其中之一。

事件 2：土耳其黑客借 SQL 注入侵入美国军方服务器

2009 年 5 月 31 日，据国外媒体报道，《信息周刊》日前发文称，美国政府调查人员正在检测两个存有敏感信息的军方服务器，怀疑它们遭到了土耳其黑客的入侵。

据该文章公布，根据调查记录显示，其中一个服务器于 1 月 26 日遭到入侵。这次入侵行为是由著名的“m0sted”土耳其黑客组织发起的，访问该服务器上网站的用户被重定向到一个气候网站上。

另据调查结果显示，2007 年 9 月还发生了一次入侵事件，相同的黑客组织入侵了美国工兵的服务器。访问者被重定向到 m0sted.com 网站，上面包含很多反美和反以色列的口号和图片。《信息周刊》表示，目前还不清楚黑客是否在这两次入侵事件中访问了敏感信息。

据悉，黑客利用了 SQL 注入攻击入侵了这些军方服务器，访问了服务器数据库。通过输入特定 SQL 命令，黑客可以获得未加过滤敏感字符的服务器的控制权限。

为了确认黑客的身份，美国国防部的调查人员曾先后研究了来自谷歌、雅虎和微软等搜索引擎的记录信息。

1.1.3　两个案例

案例 1：GSM 通信密钥被破解，全球 30 亿手机恐遭窃听[1]

GSM 是全球应用最广泛的一种移动通信标准。按这种标准的推广者、代表将近 800 家移动运营商利益的 GSM 协会说法，全球超过 212 个国家及地区的 30 多亿用户使用应用这一标准的移动电话，占到全球移动电话市场份额的 80%。为确保用户语音通信秘密性，GSM 使用分别由 64 位和 128 位二进制码组成的 A5/1 和 A5/2 串流密码进行加密。不幸的是，德国计算机高手卡斯滕·诺尔（Übersetzung für，见图 1-2）在 2009 年 12 月 30 日闭幕的“电脑捣乱者俱乐部”年会期间宣布，他与一些密码破译行家联手破解了全球移动通信系统（Global System for Mobile Communications，GSM）的加密算法，破解代码已经上传至文件共享网站供下载。破解 GSM 算法的计划由 24 人独立进行，这些人成功还原了 GSM 加密算法的密码本，数据量相当于 2TB 之巨（1TB=1024GB）。

诺尔现年 28 岁，美国弗吉尼亚大学计算机工程博士。据新华社电卡斯滕·诺尔 2009 年 12 月 29 日接受美联社记者采访时说，利用破解代码，一台高端个人计算机、一部无线电接收装置或一些计算机软件即可截获移动电话用户的语音通话信息。《金融时报》报道说，他原本打算于 2009 年 12 月 30 日在年会上演示破解代码的具体用法，但因这一做法的合法性存疑而被迫推迟。英国《金融时报》说，这一破解举动可能对全球 80%移动电话通信构成安全隐患，令全球 30 多亿移动电话用户置身语音通话遭窃听的风险中（见图 1-3）。（注，图 1-2、图 1-3 选自《广州日报》）

图 1-2　GSM 密码破译者卡斯滕·诺尔

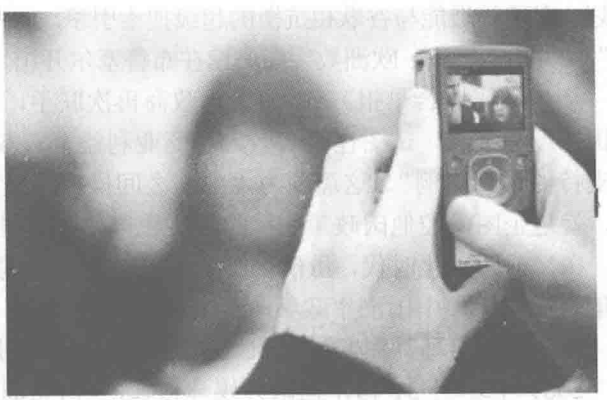

图 1-3　手机语音、图片可能被截获

案例 2：“妹妹五月天”里的黄毒与病毒（Virus）[3]

2009 年 4 月，四川省成都市警方破获了一个淫秽色情网站——“妹妹五月天”（见图 1-4）。警方调查发现这个网站不仅提供淫秽色情的内容，其中还隐藏着令人难以察觉的陷阱。登录浏览过这个网站的人，会在不知不觉中成为不法分子的猎物。

图 1-4　“妹妹五月天”网站

当时，四川成都警方在日常的网络巡查当中发现了异常：这个名叫“妹妹五月天”的网站的点击率突然增加。警方发现该网站存在大量淫秽色情内容，而且访问流量已经达到每天 10 万余人次。成都警方对这个网站实施 24 小时不间断监控，最终在成都北门一个小区内，抓获了两名犯罪嫌疑人刘某和邱某。

据审讯，两人为谋取不法利益于 2008 年建立了“妹妹五月天”网站。警方发现，这个网站与以往淫秽色情网站获利方式不同，一般说来，淫秽色情网站是通过会员注册的形式来获利的，缴费之后才能浏览网站的内容。而“妹妹五月天”是免费的，两名犯罪嫌疑人和一些制作销售 Trojan 木马病毒的不法分子合伙，利用“妹妹五月天”传播 Trojan 木马病毒，根据植入计算机的数量，由木马提供者付给他们相应的费用。据刘某和邱某交代，从建网站到案发，短短 5 个多月获利 10 万元。

1.1.4　三个故事

故事 1：“救命…”

有一个流传很广、家喻户晓的故事，故事的寓意是教育小孩要诚实。一个小孩和一群小伙伴在河边游泳。小孩为了戏弄同伴，装出溺水的样子，“救命呀，救命呀……”，小伙伴们做出迅速反应，却发现只是一个玩笑。一次、两次、三次……小伙伴们对他的救命请求信号麻木、迟钝了。有一次，小孩真的遭遇危险，发出“救命”的呼叫声时，谁也不当一回事，最终悲剧发生。故事的道理与应用广泛的拒绝服务攻击（DoS）几乎一样。

故事 2：“蜜罐（Honeypot）”计划

时年 27 岁的俄罗斯车里雅宾斯克人瓦西里·戈尔什科夫，最近被美国 FBI 逮捕并指控他利用计算机网络欺诈达 20 次。戈尔什科夫被判刑 3 年，还得赔偿西雅图 Speakeasy Network 公

司和加利福尼亚 PayPal of Palo Alto 公司 69 万美元，以补偿他借助互联网犯罪给这两家公司造成的损失。他在车里雅宾斯克用自己的计算机上网时，找到了业务系统有薄弱环节的美国公司，入网后盗取了重要的信息。根据 FBI 掌握的情况，有黑客还盗取了几十个信用卡号。美国情报机构证实，受损失的除了上述两家公司以外，还有 CTF 公司等商业机构。2000 年 11 月 10 日，在“会谈”结束后，戈尔什科夫立刻被逮捕。（2002 年 10 月 5 日俄罗斯《晨报》报道）

故事 3：“震荡波”诞生[4]

2004 年 4 月 29 日，位于德国北部罗滕堡镇、人口仅为 920 人、名叫沃芬森（Waffensen）的小村里，有一个名叫斯文·雅尚（Swinton Yesun）的孩子，住在一所平凡的房子里，如图 1-5 所示。

孩子的母亲叫维洛妮卡（Veronika），开了一个门面不算大的以计算机维护修理为主的计算机服务部。4 月 29 日这一天是他 18 岁的生日。几天前，为了庆祝他的生日，斯文·雅尚在网上下载了一些代码，修改后将它放到了互联网上面。

第二天，这些代码开始在互联网上以一种“神不知鬼不觉”的特殊方式传遍全球。“中招”后，计算机开始反复自动关机、重启，网络资源基本上被程序消耗，系统运行极其缓慢，如图 1-6 所示。

图 1-5　德国沃芬森村的一所房子

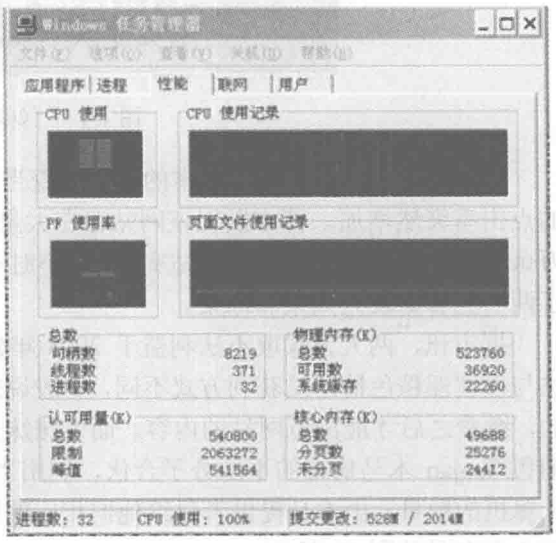

图 1-6　病毒占用大量系统资源

这就是全球臭名昭著的“震荡波（Worm.Sasser）蠕虫病毒。据不完全统计，“震荡波”自 2004 年 5 月 1 日开始传播以来，全球约有 1800 万台计算机感染了这一病毒。

2004 年 5 月 3 日，“震荡波”病毒出现了第一个发作高峰，当天先后出现了 B、C、D 三个变种，全中国已有数以十万计的计算机感染了这一病毒。微软公司悬赏 25 万美元查找元凶！

在我国，“五一”长假后的第一天，“震荡波”病毒的第二个高峰汹涌而来。仅 5 月 8 日上午 9～10 时的短短一个小时内，瑞星公司就接到用户的求助电话 2815 个，且 30%为企业局域网用户，其中不乏大型企业局域网、机场、政府部门、银行等重要单位。5 月 9 日，“震荡波”病毒疫情依然没有得到缓解。

开始有报道说是一个俄罗斯人编写了这种病毒，因为病毒始作俑者在编写这个病毒的过程中，加了一段俄语。

5 月 7 日，斯文·雅尚的同学将其告发，斯文·雅尚被警察逮捕。

其实，这个孩子在最开始并不是为了编写出一种病毒来危害别人，而是为了消除和对付“我的末日（MyDoom）”和“贝果（Bagle）”等计算机病毒。谁知，在编写杀毒程序的过程中，他设计出一种名为“网络天空 A（Net-sky）”的病毒变体。在朋友的鼓动下，他对“网络天空 A”进行了改动，最后形成了现在的“震荡波”病毒程序。

最后，由于斯文·雅尚在传播病毒的时候不到 18 岁，所以没有受到过重的惩罚。据说后来他成了一名反病毒专家。

1.1.5　五个困惑

在使用计算机时，经常会遇到各种各样的安全困惑，比如：

1）现在市面上的杀毒软件这么多，国外的有诺顿、卡巴斯基、McAfee 等，国内的有江民、金山、瑞星等，究竟哪一款杀毒软件查杀病毒的效果会更好一些呢？

2）为什么 U 盘里经常会出现 Autorun.inf、RECYCLER、RavMonE.exe 等病毒文件呢？如何防止这些病毒的传染与发作呢？图 1-7 所示为 U 盘病毒。

3）为什么计算机硬盘里经常会出现一个名为“runauto..”的病毒文件夹，并且无法删除。

4）为什么桌面上会自动出现如图 1-8 所示的淘宝网特卖图标。当删除时，弹出如图 1-9 和图 1-10 所示的消息框。

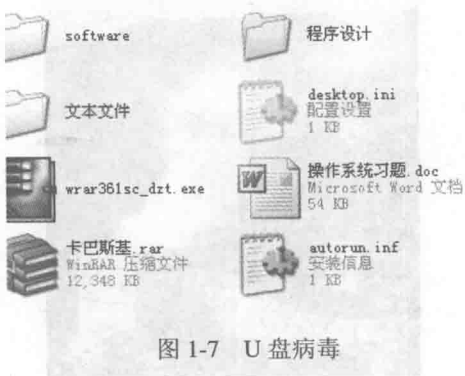

图 1-7　U 盘病毒

图 1-8　淘宝网特卖图标

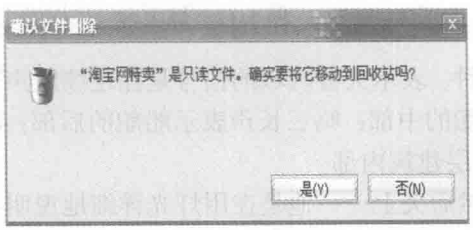

图 1-9　显示“只读”属性消息框

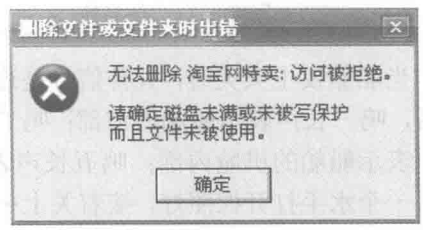

图 1-10　显示“无法删除”消息框

5）是否存在一劳永逸的信息安全解决和实施方案？

诸如此类的一系列安全问题，经常困扰着使用计算机的人们。

1.2　区分信息、消息、数据、信号与通信

1.2.1　信息、消息、数据与信号的区别

例 1：经济数据

2010 年 2 月 11 日，国家统计局和央行公布了 1 月份主要经济和金融数据，其中有关 CPI 和 PPI 的消息：1 月份 CPI 同比增长 1.5%，PPI 同比大幅上涨 4.3%，从中我们得到的信息是：CPI 增速低于预期，通货膨胀压力减小，近期加息的预期降低；CPI 与 PPI 指数拉大，物价上下游剪刀差拉大，显示工业生产继续稳步回升。

例 2：信号旗语（Signal Flag）

船上使用信号旗通信至今已有 400 多年的历史。旗号通信的优点是十分简便，因此，即使当今现代通信技术相当发达，这种简易的通信方式仍被保留下来，成为近程通信的一种重要方式，如图 1-11 所示。悬挂单面旗表示最紧急、最重要或最常用的内容。例如，悬挂 A 字母旗，传递的信息是“我船下面有潜水员，请慢速远离我船”；悬挂 O 字母旗，表示“有人落水”；悬挂 W 字母旗，表示“我船需要医疗援助”，等等。

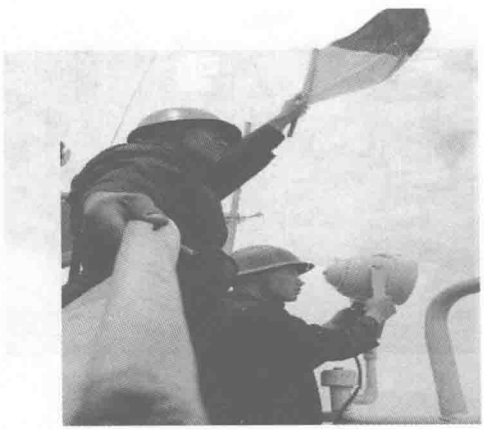

图 1-11　信号旗

图 1-12　烽火台

当船舶发生火灾时，火警信号是连续短声一分钟。表示火警区域的信号是在连续短声一分钟后，鸣一长声表示船舶的前部；鸣二长声表示船舶的中部；鸣三长声表示船舶的后部；鸣四长声表示船舶的机舱内部；鸣五长声表示船舶的上层建筑内部。

一个水手打开探照灯，接着关上……再打开，然后关上……他是在用灯光详细地说明某种信息。3 次短的闪光表示字母 S，3 次长的闪光表示字母 O，接着另外一个 3 次短的闪光表示字母 S。SOS 是求救信号。

例 3：古代烽火

人们观察到狼烟四起（光信号），它所蕴含的信息则是“外敌入侵”（见图 1-12）。

“烽火”，古代边防报警的两种信号（白天放烟叫“烽（fēng）”，夜间举火叫“燧（suì）”）。烽火台又称烽燧，俗称烽堠（hòu）、烟墩，古时用于点燃烟火传递重要消息的高台，系古代重要军事防御设施，最古老但行之有效的“土电报”。烽火台是为防止敌人入侵而建的，遇有敌