信息安全新技术

杨义先　钮心忻　任金强 编著

北京邮电大学出版社
·北京·

内 容 提 要

本书对国内外网络信息安全方面有代表性的最新技术作了系统而详细的总结。全书共分八章，分别对信息隐藏技术、数字水印技术、多媒体信息伪装技术、入侵检测技术、电子支付技术、网络安全协议、智能卡安全技术和公钥基础设施(PKI)技术进行了充分的论述。

本书内容翔实，叙述通俗易懂，可作为通信与电子系统、信号与信息处理、密码学、信息安全、计算机应用等专业的研究生、本科生和大专生相关课程的教学参考书，也可作为从事国家网络信息安全工作人员在高新技术条件下做好本职工作、提高业务水平必备的实用工具书，还可作为国内网络安全、计算机安全和信息安全领域相关人员的技术培训教材。本书还可以为国内众多网络安全公司的技术人员和管理人员了解国内外最新技术动态提供有力的帮助。

图书在版编目(CIP)数据

信息安全新技术/杨义先，钮心忻，任金强编著. —北京：北京邮电大学出版社，2001.12

ISBN 7-5635-0560-1

Ⅰ.信… Ⅱ.①杨… ②钮… ③任… 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(2001)第 082737 号

信息安全新技术

北京邮电大学出版社出版发行

北京市海淀区西土城路 10 号

邮编：100876 发行部电话：62282185

E-mail：publish@bupt.edu.cn

各地新华书店经售

北京源海印刷厂印刷

*

850 mm×1 168 mm 1/32 印张 8.375 字数 218 千字

2002 年 3 月第 1 版 2002 年 3 月第 1 次印刷

印数：1—5 000 册

ISBN 7-5635-0560-1/TN·251 定价：16.00 元

前　言

安全是相对的，不安全是绝对的！在人类进入理想的共产主义社会之前，信息安全问题永远无法回避。

“发展”和“变化”是信息安全的最主要特征，只有紧紧抓住这个特征才能正确地处理和对待信息安全问题。“攻”与“守”双方当前争斗的暂时动态平衡体现了信息安全领域的现状。“攻”与“守”双方的“后劲”决定了信息安全今后的走向。“攻”与“守”双方既相互矛盾又相互统一。其实，在多数情况下，“攻”与“守”的角色都是由同一批人员担任。“攻”与“守”始终都是相互促进，循环往复，永无止境。

1. 信息安全越变越重要，安全系统成了无价之宝

前任美国总统克林顿曾经声言：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。的确，在信息时代，知识即意味着财富和实力。信息时代的到来，从多方面影响着国家利益的构成和内涵。信息本身成为国家利益的一个组成部分，信息量成为衡量国家间利益均衡的一个重要参数，对信息的开发、控制和利用成为国家间利益争夺的重要内容。伴随着信息技术与信息产业的发展，网络与信息安全问题及其对经济发展、国家安全和社会稳定的重大影响，正日益突出地显现出来，受到越来越多国家的关注。实际上，在信息化进程中，国家的安全与经济的安全越来越不可分割，经济安全越来越依赖于信息化基础设施的安全程度。高度发达的电子信息系统将成为国家经济发展的重要支柱和动力，

成为提高社会生活质量的基础设施，在国家经济安全中有着举足轻重的地位和作用。如果不能保障信息安全，就不可能获得信息化的效率和效益，在国际“信息战”威胁和国内外高技术犯罪的干扰破坏下，社会的经济生活就难以健康、有序地进行，国家的安全更无法确保。网络信息安全已经上升为一个事关国家政治稳定、社会安定、经济有序运行和社会主义精神文明建设的全局性问题。从这一意义上讲，网络信息安全系统的保障能力是21世纪综合国力、经济竞争实力和民族生存能力的重要组成部分。因此，必须努力构筑一个技术先进、管理高效、安全可靠、建立在自主研究开发基础之上的国家信息安全体系，以有效地保障国家安全、社会稳定和经济发展。构筑国家信息安全体系是一项跨世纪的战略任务，也是一项艰巨复杂的系统工程。信息安全需要一切相关高科技的最新成果的支持。在信息安全系统工程中，密码是核心，协议是桥梁，体系结构是基础，安全集成芯片是关键，安全监控管理是保障，检测攻击与评估是考验。

2. 安全标准在不断变化，安全目标需无限追求

如何在设计制作信息系统时就具备保护信息安全的体系结构是人们长期追求的理想，科学合理的安全标准是人们达到此理想目标的“指挥棒”。美国国防部早在20世纪80年代就针对国防部门的计算机安全保密问题开展了一系列有影响的工作，后来成立了国家计算机安全中心(NCSC)。1983年NCSC公布了可信计算机系统评价准则(TCSEC)，以后，NCSC又出版了一系列有关可信计算机数据库、可信计算机网络指南等。在这些准则中，从用户登录、授权管理、访问控制、审计跟踪、隐通道分析、可信通道建立、安全检测、生命周期保障、文本写作、用户指南方面均提出了规范性要求，并根据所采用的安全策略、系统所具备的安全功能等方面将系统分为4类7个安全级别。这些准则对研究导向、规范生产、指导用户选型、提供检查机关评价依据，都起了良好的推动作用。

TCSEC 运用的主要安全策略是访问控制机制。

TCSEC 带动了国际计算机安全的评估研究，20 世纪 90 年代初西欧 4 国(英、法、荷、德)联合提出了信息技术安全评价标准(ITSEC)，它除了吸收 TCSEC 的成功经验外，首次提出了信息安全的保密性、完整性、可用性的概念，把可信计算机的概念提高到可信信息技术的高度上来认识。ITSEC 定义了 7 个安全级别，即 E6：形式化验证；E5：形式化分析；E4：半形式化分析；E3：数字化测试分析；E2：数字化测试；E1：功能测试；E0：不能充分满足保证。ITSEC 还对系统定义了 10 个安全功能。

1999 年 6 月，国际标准化组织(ISO)和国际电联(ITU)共同批准了由美国、加拿大、英国、荷兰、法国等 7 国联合研制的信息技术安全评估公共准则(CC)，称为 ISO/IEC 15408。该准则比以往其他信息安全评估准则更加规范，采用了类别、认证族、认证部件和认证元件的方式来定义。ISO/IEC 15408 准则规定了 3 种评估类别、8 个认证类别、7 个评估认证级别类别。

如今，有关安全的评测标准方面的研究还在继续，而且还将继续进行下去。信息安全体系是人们希望构建，并用于保障安全的理想追求。但是，由于包括人在内的信息系统是一个动态、时变、智能化、非线性的复杂大系统，它涉及因素多，关系复杂。所以，虽然人们为此作出了多年的努力，然而，至今为止，人们所拥有的解决方案仍然是局部的，有限能力的。

3. 安全概念在不断扩展，安全手段需随时更新

人类对信息安全的追求过程是一个漫长的深化过程。人为因素和非人为因素都有可能引起不安全的后果。为了对付非人为因素引起的不安全问题，人们已经研制出了各种各样的纠错编码，并取得了良好的效果。而在对付人为因素引起的安全问题方面，情况就更加复杂了。

为了防止敌对的第三方读懂收发信双方的机密通信内容，过

去几千年来，人们一直沿用加密和解密技术。直到20世纪60年代末，以加密和解密技术为基础的通信保密一直是信息安全的重点。

电信通信系统的发展，使人们意识到电磁泄露也可能造成信息的失密。从而，防电磁辐射的屏蔽技术也成了信息安全的一种重要手段。

计算机普及之后，以计算机病毒、非法存取等为代表的计算机安全问题成为了信息安全的新热点。为此，人们研制出了各种反病毒的工具，并采用了多种有效的身份识别和访问控制机制。

20世纪80年代以来，网络化的发展将计算机系统和通信系统融为一体，形成了以因特网为代表的计算机网络系统。随之而来的安全问题就更加复杂多样了。至此，人们才认识到，信息安全的概念远远不限于加密、解密、防泄露、反病毒和身份认证与访问控制。信息安全的含义，至少应该包括以下几个方面：

- 信息的保密性：保证信息不被未授权者获取；
- 信息的完整性：保证真实的信息从真实的信源到达真实的信宿；
- 信息的可用性：授权者可以随时使用信息和信息系统的服务；
- 信息的可控性：信息系统的管理者可以控制管理系统和信息；
- 信息行为的不可否认性：每个通信者具有法律生效的证据证明其是否实施过信息交换和获取的行为。

90年代以来，层出不穷的黑客事件使人们进一步深刻地认识到，仅仅只有被动的保护还不能全面涵盖信息安全的各个方面。因此出现了信息安全的新提法，认为信息安全的概念应该包含信息的保护、检测、反应和恢复4个方面的内容。虽然保护信息的保密性、完整性、可用性、可控性和不可否认性是必不可少的安全需求，但是，构建一个安全系统时，应该有相应的检测评估，不要等到黑

客进入之后再去亡羊补牢。因此，有必要研究发展检测评估理论、技术和工具，并用它们来实施系统功能的静态分析评价和实时动态检测报警。一旦发现系统的防护能力不足以抵御黑客的入侵，检测系统就立即报警，同时还需要及时地对报警作出反应，以便减少损失，发现入侵者的来龙去脉，及时补救系统漏洞，为捕获入侵者提供线索。如果黑客攻击已经造成了损失，系统还必须拥有恢复的手段，使系统在尽可能短的时间内恢复正常，提供服务。

随着社会信息化步伐的加快，我们有理由相信，信息安全的概念和相应的解决信息安全问题的手段也将会不断地发展。信息安全至少需要“攻、防、测、控、管、评”等多方面的基础理论和实施技术。

4. 安全技术在迅速更新

信息安全是一个复杂的巨大系统，技术、政策实践与意识、培训与教育三个层面的问题都必须加以考虑。其中，信息安全技术可能是最具活力的一个方面。信息安全是现代信息系统发展应用带来的新问题，它的解决也需要现代高新技术的支撑，传统意义的方法是不能解决问题的，所以信息安全新技术总是在不断地涌现。本书的目的就是要对信息安全技术领域的若干新技术进行系统介绍。由于我们已经在《网络信息安全与保密》一书（北京邮电大学出版社，1999 年 11 月出版）中对信息安全领域的密码技术、防火墙技术、虚拟专用网络技术、病毒与反病毒技术、数据库安全技术、操作系统安全技术、物理安全与保密技术等信息安全技术作了适当介绍，所以本书就不再重复这些内容了。本书重点介绍以信息伪装、数字水印、电子现金、入侵检测、安全智能卡、PKI、网络安全协议等为代表的信息安全最新技术。

本书是北京邮电大学信息安全中心全体成员集体智慧的结晶。在本书写作过程中曾志峰博士、李鸿培博士、夏光升博士、徐国爱博士、陈明奇博士、吴秋新博士、钟鸣博士、李新博士、岳军巧博

士、毛琼硕士、丘天豪硕士、李琛硕士、庄严硕士、王慰硕士、戴杨波硕士等为本书提供了丰富的参考文献。特别感谢胡正名教授、李中献博士、冯运波博士、张振涛博士、古利泽硕士、温巧燕教授、罗守山教授、牛少彰教授、卓新建博士，他们以及北京邮电大学信息安全中心百余位研究人员在网络信息安全方面研究的丰富成果是本书的营养源泉。本书也是国家重点基础研究发展规划项目(编号：G1999035805)、国家杰出青年基金项目(批准号：69425001)、国家自然科学基金项目(批准号：69882002，60073049)资助和高校骨干教师资助计划项目的成果。

由于作者水平有限，书中难免出现各种失误和不当之处，欢迎大家批评指正。

作　者

2001 年 11 月

目　录

第1章　信息隐藏技术

过去几千年的历史已经证明：密码是保护信息机密性的一种最有效的手段。通过使用密码技术，人们将明文加密成敌人看不懂的密文，从而阻止了信息的泄露。[1~22]但是，在如今开放的因特网上，谁也看不懂的密文无疑成了“此地无银三百两”的标签。“黑客”完全可以通过跟踪密文来“稳、准、狠”地破坏合法通信。为了对付这类“黑客”，人们采用以柔克刚的思路重新启用了古老的信息隐藏技术，并对这种技术进行了现代化的改进，从而达到了迷惑“黑客”的目的。当然，无需讳言，信息隐藏技术在国内外重新受到青睐的另一个重要原因是相关用户希望通过此项技术来回避密码管制的政策风险。[23~35]

1.1　信息隐藏的历史沿革

随着多媒体技术和 Internet 的迅猛发展，互联网上的数字媒体应用正在呈爆炸式的增长，越来越多的知识产品以电子版的方式在网上传播。数字信号处理和网络传输技术可以对数字媒体（数字声音、文本、图像和视频）的原版进行无限制的任意编辑、修改、拷贝和散布，造成数字媒体的知识产权保护和信息安全的问题日益突出，并已成为数字世界的一个非常重要和紧迫的议题。因此，如何防止知识产品被非法复制及传播，也是目前急需解决的问题。传统的信息安全技术无法解决这些新问题。因此，国际上近几年来开始提出并尝试一种新的关于信息安全的概念，开发设计不同于传统密码学的技术，即将机密资料信息秘密地隐藏于一般的文件中，然后再通过网络传递。由于非法拦截者从网络上拦截下来的伪

装后的机密资料，并不像传统加密过的文件一样，看起来是一堆会激发非法拦截者破解机密资料动机的乱码，而是看起来和其他非机密性的一般资料无异，因而十分容易逃过非法拦截者的破解。其道理如同生物学上的保护色，巧妙地将自己伪装隐藏于环境中，免于被天敌发现而遭受攻击。这一点是传统加解密系统所欠缺的，也是信息隐藏的基本思想。

顾名思义，所谓信息隐藏的意思就是将秘密信息秘密地隐藏于另一非机密的文件内容之中。其形式可为任何一种数字媒体，如图像、声音、视频或一般的文档等等。信息隐藏的首要目标是隐藏的技术要好，也就是使加入隐藏信息后的媒体目标的降质尽可能小，使人无法看到和听到隐藏的数据，达到令人难以察觉的目的。信息隐藏还必须考虑隐藏的信息在经历各种环境、操作之后而免遭破坏的能力。比如，信息隐藏必须对非恶意操作、图像压缩和信号变换等，具有相当的免疫力。信息隐藏的数据量与隐藏的免疫力始终是一对矛盾，不存在一种完全满足这两种要求的隐藏方法。通常只能根据需求的不同有所侧重，采取某种妥协，使一方得以较好的满足，而使另一方做些让步。从这一点看，实现真正有效的信息隐藏的难度较大，十分具有挑战性。

信息隐藏技术和密码技术的区别在于：密码仅仅隐藏了信息的内容，而信息伪装不但隐藏了信息的内容而且隐藏了信息的存在。信息隐藏技术提供了一种有别于加密的安全模式，其安全性来自于对第三方感知上的麻痹性。在这一过程中载体信息的作用实际上包括两个方面：①提供传递信息的信道；②为隐藏信息的传递提供伪装。随着计算机网络和多媒体技术的发展，信息隐藏技术的应用在不断扩展，载体信息的作用也在发生着变化。例如：用于版权保护的数字水印技术，这时的载体信息是具有某种商业价值的信息，而秘密信息则是一些具有特殊意义的标识或控制信息。应该注意到，密码技术和信息隐藏技术并不是互相矛盾、互相竞争的技

术，而是互补的。它们的区别在于应用的场合不同、要求不同，但可能在实际应用中需要互相配合。例如：将秘密信息加密之后再隐藏，这是保证信息安全的更好的办法，也是更符合实际要求的方法。

数字化的信息隐藏技术的确是一门全新的技术，但是它的思想其实来自于古老的隐写术。大约在公元前 440 年，隐写术就已经被应用了。当时，一位剃头匠将一条机密消息写在一位奴隶的光头上，然后等到奴隶的头发长起来之后，将奴隶送到另一个部落，从而实现了这两个部落之间的秘密通信。类似的方法，在 20 世纪初期仍然被德国间谍所使用。实际上，隐写术自古以来就一直被人们广泛地使用。隐写术的经典手法实在太多，此处仅列举一些例子：

- 使用不可见墨水给报纸上的某些字母作上标记来向一个间谍发送消息。
- 在一个录音带的某些位置上加一些不易察觉的回声等。
- 将消息写在木板上然后用石灰水把它刷白。
- 将信函隐藏在信使的鞋底里或妇女的耳饰中。
- 由信鸽携带便条传送消息。
- 通过改变字母笔画的高度或在掩蔽文体的字母上面或下面挖出非常小的小孔（或用无形的墨水印制作非常小的斑点）来隐藏正文。
- 在纸上打印各种小像素点组成的块来对诸如日期、打印机标识符、用户标识符等信息进行编码。
- 将秘密消息隐藏“在大小不超过一个句号或小墨水点的空间里”（1857 年）。
- 将消息隐藏在微缩胶片中（1870 年）。
- 把在显微镜下可见的图像隐藏在耳朵、鼻孔以及手指甲里（1905 年俄日战争期间）；或者先将间谍之间要传送的消息

经过若干照相缩影步骤后缩小到微粒状，然后粘在无关紧要的杂志等文字材料中的句号或逗号上(第一次世界大战期间)。

- 在印刷旅行支票时使用特殊紫外线荧光墨水。
- 制作特殊的雕塑或绘画作品，使得从不同角度看会显出不同的印像。
- 用藏头诗，或者歧义性的对联、文章等文学作品。
- 在乐谱中隐藏信息(简单地将字母表中的字母映射到音符)。
- 古代，我国还有一种很有趣的信息隐藏方法，即消息的发送者和接收者各有一张完全相同的带有许多小孔的掩蔽纸张，而这些小孔的位置是被随机选择并戳穿的。发送者将掩蔽纸张放在一张纸上，将秘密消息写在小孔位置上，移去掩蔽纸张，然后根据纸张上留下的字和空格编写一段掩饰性的文章。接收者只要把掩蔽纸张覆盖在该纸张上就可立即读出秘密消息。直到16世纪早期，意大利数学家Cardan又重新发展了这种方法，该方法现在被称作卡登格子隐藏法。
- 利用掩蔽材料的预定位置上某些误差和风格特性来隐藏消息。比如，利用字的标准体和斜体来进行编码，从而实现信息隐藏；将版权信息和序列号隐藏在行间距和文档的其他格式特性之中；通过对文档的各行提升或降低三百分之一英寸来表示0或1等等。

……

信息隐藏研究虽然可以追溯到古老的隐写术，但在国际上正式提出数字化信息隐藏研究则是在1992年。国际上的第一届信息隐藏研究会于1996年在剑桥大学举行，这次会议推动了信息隐藏的理论和技术研究。中国台湾国立大学通信和多媒体实验室也做了大量的工作。1998年在美国俄勒冈州召开了第二届信息隐藏研

究会，1999 年 9 月 29 日～10 月 1 日在德国 Dresden 召开了第三届信息隐藏研讨会。最近 IEEE ICIP，EUSIPCO 的会议中也都研讨了信息隐藏。中国在 1999 年 12 月 11 日，由北京电子技术应用研究所组织，召开了第一届信息隐藏学术研讨会，2000 年 6 月 17～18 日召开了第二届信息隐藏学术研讨会。2000 年 1 月 15～16 日，国家“863”计划智能计算机专家组、中国科学院自动化研究所和北京邮电大学信息安全中心成功地举办了数字水印技术研讨会。2001 年 9 月，全国第三届信息隐藏学术研讨会又在西安召开。如今，信息隐藏已经成为当前国际上的研究热点。

信息隐藏技术作为一种新兴的信息安全技术已经被许多应用领域所采用。越来越多的数字视频、音频信号及图像被“贴”上了不可见的标签，这些标签往往携带隐藏了的版权标识或序列号来防止非法拷贝。军事系统广泛地采用信息安全技术，不只用加密隐藏消息内容，还用信息隐藏技术来隐藏消息的发送者、接收者甚至消息本身。类似的技术还用在移动电话系统及其他的电子媒介系统中。

信息隐藏术也正日益受到研究机构和业界的关注，主要动力来自人们对版权问题的关注。随着音像、图像和其他产品的数字化，数字产品的盗版更加容易，这引起了音乐、电影、书籍和软件发行商的极大关注，因此引发了信息隐藏术的重要分支领域“数字水印”和“数字指纹”的研究。前者可以作为版权争端的法律凭证，用来指控盗版者；后者则可以用来追查盗版者。

数字水印技术为电子数据的版权保护等需要提供了一个潜在的有效手段，因而引起了国际学术界与企业界的广泛关注，是目前国际学术界研究的一个前沿热门方向。数字水印是携带所有者版权信息的一组辨别数据。数字水印被永久地嵌入到多媒体数据中用于版权保护并检查数据是否被破坏。数字水印技术作为在开放的网络环境下保护版权的新型技术，它可以确立版权所有者，识别

购买者或者提供关于数字内容的其他附加信息，并将这些信息以人眼不可见的形式嵌入在数字图像、数字音频和视频序列中，用于确认所有权和跟踪行为。另外，它在证据篡改鉴定、数据的分级访问、数据的跟踪和检测、商业和视频广播、互联网数字媒体的服务付费，电子商务的认证鉴定等方面也具有十分广阔的应用前景。自从 1993 年尤其是 1995 年和 1996 年以来，引起了工业界的浓厚兴趣，日益成为国际上非常活跃的研究领域。

尽管版权保护是发展数字水印技术的原动力，但人们发现数字水印还具有其他的一些重要应用，如：版权保护、真伪鉴别、隐蔽通信、标志隐含等等。这些研究预示着商业上的巨大应用前景。例如：数字水印技术在 DVD 的发行中的应用也有很大的市场潜力。DVD 联盟建议提出一个版权保护方案来加强拷贝管理。现有的 DVD 播放器允许 vedio 的无限制拷贝，但不利于版权保护。该建议提出 home vedio 将不作标记，电视广播制品将标识为“一次拷贝”，商业音像制品标识为“禁止拷贝”，播放器将根据这些标记作出相应的动作。

目前国外研究信息伪装的学术机构有麻省理工学院的媒体实验室、IBM 等一些机构和一些大学，研究的重点在如何将信息隐藏到图像、声音和文字之中。目前对于信息隐藏应用在数字产品的著作权保护方面（或称为数字水印）的研究较多。瑞士洛桑联邦工技院信号处理实验室和通信研究所、美国的 NEC 研究所、中国的台湾国立交通大学等都取得了不少成就。除了学术界的研究之外，目前也有一些公司开发出一些软件，如：Fraunhofer's SYSCOP，HIGHWATER FBI，Digimarc Corporation，DICE's Argent Digital Watermark 等等，提供有关数字产品著作权保护的服务。当前国内研究信息伪装的科研院所有：北京邮电大学信息安全中心、中国科学院自动化研究所模式识别国家重点实验室、北方工业大学、清华大学、北京理工大学、北京电子技术应用研究所、国家信息安

全测评认证中心等单位。

基于信息隐藏技术而建立起来的一个安全的信息隐藏系统可以用如下的非正式定义来描述：一个安全的信息隐藏系统应该是，任何了解系统但不知道密钥的敌手不能得到任何有关已发生的通信的证据（甚至怀疑的范围）。它将遵守一个核心准则：被广泛使用的信息隐藏程序步骤应该公开发布，就像商用的密码算法和协议那样。所以人们可以期望：版权标记系统的设计者会公开发布他们使用的系统机制和原理，并且系统的安全性仅依赖于其使用密钥的保密性。

1. 信息隐藏系统的特性

一个理想的信息隐藏系统应该具有以下特性（以载体是静止图像为例）：

（1）隐蔽性

这是信息伪装的基本要求，经过一系列隐藏处理的图像没有明显的降质，隐藏的信息无法看见或听见。

（2）安全性

隐藏的信息内容应是安全的，应经过某种加密后再隐藏，同时隐藏的具体位置也应是安全的，至少不会因格式变换而遭到破坏。

（3）对称性

通常信息的隐藏和提取过程具有对称性，包括编码、加密方式，以减少存取难度。

（4）可纠错性

为了保证隐藏信息的完整性，使其在经过各种操作和变换后仍能很好地恢复，通常采取纠错编码方法。

2. 信息隐藏技术的分类

需要指出的是，对信息隐藏技术的不同应用，各自有着进一步不同的具体要求，并非都满足上述要求。信息隐藏技术包含的内容范围十分广泛，可以作如图 1-1 所示的分类。