普通高等教育计算机类特色专业系列规划教材

网络安全基础

覃健诚　白中英　编著

科学出版社

普通高等教育计算机类特色专业系列规划教材

网络安全基础

覃健诚　白中英　编著

科学出版社

北京

内 容 简 介

本书立足于网络多层纵深防御体系架构，将网络安全划分成6个层次，并分别介绍了各个层次上的典型技术和理论知识。本书共8章：第1章网络安全概论，第2章安全理论基础知识，第3章物理级安全，第4章操作系统级安全，第5章系统软件级安全，第6章应用程序级安全，第7章业务级安全，第8章内容级安全。

本书以安全防御为主导，将攻击与防御内容相结合，理论基础与实际技术并重。全书结合作者在网络安全方面所做的科研工作，着眼于建立相对完整的知识框架和应用基础，内容既具有基础性，同时又跟踪时代性前沿以启发创新。

本书可作为高等院校计算机和信息类专业高年级本科生及相关专业研究生的专业基础课教材，也可作为信息产业工程技术人员的参考书。

图书在版编目(CIP)数据

网络安全基础/覃建诚，白中英编著. —北京：科学出版社，2011.7
（普通高等教育计算机类特色专业系列规划教材）
ISBN 978 7 03 032204-3

Ⅰ.①网… Ⅱ.①覃…②白… Ⅲ.①计算机网络 安全技术-高等学校-教材 Ⅳ.①TN393.08

中国版本图书馆CIP数据核字(2011)第175337号

责任编辑：巴建芬 刘鹏飞 / 责任校对：包志虹
责任印制：张克忠 / 封面设计：迷底书装

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

骏走印刷厂印刷

科学出版社发行 各地新华书店经销

*

2011年7月第 一 版 开本：787×1092 1/16
2011年7月第一次印刷 印张：17 1/2
印数：1—3 000 字数：436 000

定价：36.00元

（如有印装质量问题，我社负责调换）

前　言

“网络安全基础”是一门以计算机科学与技术专业、信息安全专业为主体，涉及计算科学、密码学、运筹学等多个学科的综合性基础课程。这门课程处于信息时代的前沿，涵盖的知识面广，内容丰富，技术更新快。通过学习这门课程，可以把大量跨学科的知识综合起来，形成一个知识体系的整体框架。

21 世纪是信息化的时代，计算机网络已经成为信息的主要载体，与国计民生密不可分。2009 年，美国国防部建立了三军“网络战司令部”，将网络安全问题的重要性提到前所未有的高度。网络安全问题是当今世界迫切需要解决的重大课题，也应当是信息安全专业学生全力关注的核心。而解决这个问题的一个必要条件是要培养出大量掌握网络安全知识和技能的综合性人才。

顾名思义，计算机网络是由各种类型的计算机通过通信传输线路联接起来的巨大系统。因此，网络安全技术涉及信息传输和信息处理两大领域。就计算机本身而言，又涉及硬件、软件、固件、密钥和智能技术。2006 年，美国国会以国家安全为由，阻止美国政府机构采购和使用中国生产的计算机。美国国会禁止使用中国计算机一事，为我们解决网络安全问题提供了相当清晰的思路。

本书内容理论性和实用性并重。作者根据多年从事网络安全工作的经验认识到，形形色色的安全问题的本质“万变不离其宗”，新技术总是在原有知识的基础上诞生的，只要懂理论就能够理解，也能够想出应对办法。作者在书中提出了多层纵深防御体系架构，将网络安全划分成多个层次，从物理层到内容层，各层可以动态部署各种安全技术，形成纵深防御体系。这种架构可以使孤立防线的网络安全的脆弱性得到有效改观。

本书定位于网络安全的入门教材，着眼于建立相对完整的知识框架和应用基础。书中没有对各种安全技术作深入详尽的论述，仅列举出涉及的理论知识和部分典型技术，点到为止。要想深入学习网络安全的各种具体内容，可以参考相关的专业文献资料。

本书的内容结构如下：第 1 章网络安全概论，第 2 章安全理论基础知识，第 3 章物理级安全，第 4 章操作系统级安全，第 5 章系统软件级安全，第 6 章应用程序级安全，第 7 章业务级安全，第 8 章内容级安全。

在本书编写过程中，北京邮电大学计算机学院杨义先教授、马华东教授的大力支持，也得到辛阳副教授的具体帮助。研究生白媛、王飞杰、吴琨、王玮、于树香、刘俊荣、李姣姣等参与了相应的研究工作和一部分书稿整理工作。在此，作者一并向他们表示衷心感谢。

考虑到书中概念与公共知识领域的一致性，本书涉及概念介绍时，部分引用了互联网上的共知内容。另外书中介绍的部分内容仍处于研发阶段，存在争议也属正常。若书中存在疏漏或不妥之处，敬请读者批评指正。

作　者

2011 年 6 月于北京

目　录

第 1 章　网络安全概论

计算机网络是现代信息的载体。本章全方位地对网络安全的概念加以介绍：纵向——讲述信息安全的历史与发展趋势；横向——讲述网络安全的层次结构划分和多层纵深防御体系；深度——列举网络安全技术的主要相关学科。从而给读者一个网络安全的宏观印象，以便他们系统全面地学习网络安全知识。

1.1　从信息安全到网络安全

1.1.1　信息安全的历史发展

信息安全这一术语的诞生与人类通信技术的进步密切相关。信息安全的研究可分如下五个阶段。

第一阶段：古典密码时代。

如果把信息视作一种客观存在，那么人类历史从很早以前就已经在使用信息。对信息安全的保护也可以追溯到公元前 400 多年，甚至更早。

大约公元前 440 年，在古希腊战争中出现“隐写术”，它将情报写在头上，利用头发掩盖。大约公元前 400 年，斯巴达人用羊皮纸绕在锥形棒上，写上情报。羊皮纸解开之后，信息杂乱无章，只有绕在同样大小的锥形棒上才能够重新呈现出来。

大约公元前 100 年的古罗马时代，凯撒(Caesar)密码是凯撒大帝用来保护重要军事情报的加密系统，它是一种置换密码，通过将字母按顺序推后 3 位起到加密作用，如将字母 A 换作字母 D，将字母 B 换作字母 E。凯撒密码是一种古典密码术，比起现代密码学中的各种加密算法，显然太简单了，但它已经具备了密码学中的一些基本要素。

明文是指原始的、可以直接认知的信息。**密文**是指加密之后得到的、不能直接认知的信息。**密钥**是指加密、解密过程中要用到的关键信息。**加密**是指把原始信息(明文)转化为不可直接认知的信息(密文)的正常过程。**解密**是指把加密后的信息(密文)转化为原始信息(明文)的正常过程。**破解**是指在没有密钥的情况下，以非正常的方式从密文中提取全部或部分明文信息，或者获取到全部或部分密钥信息的过程。

凯撒密码中，全部字母推后 3 位，密钥其实就是 3。这个密钥在当时是不公开的。

【例 1】 解密凯撒密码的密文“KHOOR ZRUOG”。

解：把密文字母推前 3 位，得到明文“HELLO WORLD”。

我国古代也有以藏头诗、藏尾诗、漏格诗及绘画等形式，将要表达的真正意思隐藏在诗文或画卷中的特定位置，从而起到信息隐藏的作用。

北宋《武经总要》作者曾公亮研究出中国古代军事情报通信密码：对 40 条情报短语进行编号，出兵前约定 40 字且没有重字的五言律诗作为解码密钥。发信息时，把情报短语对应的字写到一件普通公文书牒之中，并在那个字上加盖印章。

到了 1860 年，密码系统在外交通信中已得到普遍使用。美国国内战争期间，联邦军队广泛

地使用了换位加密。在第一次世界大战期间，同盟国与协约国双方都使用加密系统，密码本被用在重要的情报通信中。

古典密码时代，信息安全的保护主要通过手工方式，效率很低。

第二阶段：近代密码时代。

20 世纪 20 年代，随着机械和机电技术的成熟，出现了转轮密码机。转轮密码机极大地提高了加密、解密的速度，利用机械转轮可以开发出极其复杂的加密系统。著名的密码机有德国的恩尼格玛(Enigma)，1919 年面世，在第二次世界大战期间曾作为德国陆、海、空军最高级密码机，后来被盟军数学家破译。

第二次世界大战期间的盟军方面，则有英国的 TYPEX 密码机、瑞典的哈格林(Hagelin)密码机等。

转轮密码机的出现，是密码学发展的重要标志之一。密码机用自动计算替代了手工处理，使效率有了质的提升，信息安全的保护水平大大提高，破解已经无法单凭手工，往往也要借助于自动计算。

第三阶段：现代密码学时代。

1937 年，英国数学家图灵(Turing)发表论文《论数字计算在决断难题中的应用》，给“可计算性”下了一个严格的数学定义，并提出著名的图灵机模型。

1950 年，图灵发表论文《计算机能思考吗》，设计了著名的图灵测试，开创了人工智能的先河。

目前已知的世界上第一台电子计算机是英国的科洛萨斯计算机，它从 1943 年 3 月开始研制，用于破译德国密码机的加密，1944 年 1 月 10 日开始运行，比美国的 ENIAC 计算机问世早了两年多。

美籍匈牙利数学家冯·诺依曼参与了美国 ENIAC 计算机的研制，他关于存储程序的设计思想奠定了现代计算机的体系结构。

电子计算机无疑是划时代的产物，其运算速度的飞跃也带动了信息安全的发展。古典密码时代的保护方式在计算机面前变得不堪一击，而新的保护方式的运算量之大是前所未有的，攻防双方都离不开计算机这一先进的工具。

同一时期，信息安全理论也发展到了一个全新的境界，信息安全保护不再是单纯的技术——密码术，而是有了理论基础的科学——密码学。

1948 年，美国数学家香农(Shannon)发表论文《通信的数学理论》，创立了信息论。论文以概率论为基础，阐述了通信工程的一系列基本理论问题，给出了计算信源信息量和信道容量的方法和一般公式，得到著名的编码三大定理，为现代通信技术的发展奠定了理论基础。

1949 年，香农发表论文《保密系统的通信理论》，奠定了现代密码学的基础。论文在信息论的基础上阐明了关于密码系统分析、评价和设计的科学思想，提出了保密系统的数学模型、随机密码、纯密码、完善保密性、理想保密系统、唯一解距离、理论保密性和实际保密性等重要概念，并提出评价保密系统的五条标准，即保密度、密钥量、加密操作的复杂性、误差传播和消息扩展。文中所提出的破译密码的计算量理论已和计算机理论中的计算复杂性理论结合起来，成为评价密码安全性的一个重要准则。

电子计算机的出现和信息安全理论的创立，共同促成了这个现代密码学时代。

第四阶段：网络安全时代。

1969 年，美国国防部开始启动具有抗核打击性的计算机网络开发计划(ARPANET)，这是互联网(Internet)的前身。1971 年后，ARPANET 的技术开始向大学等研究机构普及。

在各种通信网络中，互联网对信息安全的影响最为广泛，因此人们把互联网的诞生看做网络安全时代的开端。

这一阶段，密码技术也发展迅速。1972 年，美国 IBM 公司研制出一种对称密码体制加密算法，在 1977 年得到美国政府正式许可后称为 DES(Data Encryption Standard)算法。DES 算法使用 56 位密钥，进行 64 位分组加密。

1975 年，Merkle 提出公钥交换的概念；1976 年，在 Diffie 和 Hellman 的论文《密码学的新方向》中，提出基于离散对数难题的 Diffie-Hellman-Merkle 密钥交换系统，开创了公开密钥密码编码学的新领域。

1977 年，Ronald Rivest、Adi Shamir 和 Leonard Adleman 利用大数因式分解难题发明了公钥加密算法 RSA。该算法至今还在广泛应用。

在这个网络安全时代，计算机与通信线路融为一体，共同构成计算机网络。计算机是网络的点，通信线路则是网络的边。网络作为一个整体，成为信息安全的重要载体和工具。

第五阶段：大规模网络安全时代。

1991 年后，互联网开始向社会大众普及。这又是网络安全的一个重要进展，因为普及化使互联网的应用规模和种类数量都有极大的提高，网络安全也呈现出多样化和复杂化的状况。

1994 年 3 月，中国获准加入互联网，并在同年 5 月完成全国联网工作。

1997 年，由 MasterCard 和 Visa 联合 Netscape、Microsoft 等公司推出的一种新的电子支付 SET(Secure Electronic Transaction，安全电子交易)协议。SET 具有保证交易数据的完整性、不可抵赖性等优点，成为信用卡网上交易的国际标准。

1997 年，RSA 公司悬赏 1 万美元举行一次破解 DES 加密的活动，结果互联网上 1.4 万台计算机联合行动找到了密钥。这次分布式暴力破解显示 56 位 DES 算法已经不够安全。

1999 年，美国国家标注技术研究所(NIST)将 3DES 指定为过渡的加密算法标准。3DES 是 DES 加密算法的一种模式，使用 3 条 56 位的密钥对数据进行三次加密，因此密钥总长度是 168 位，仍然是 64 位分组加密。

2002 年，NIST 制定了新的高级加密标准(AES)规范。AES 算法可以使用 128、192 和 256 位密钥，进行 128 位分组加密。

这个大规模网络安全时代仍在发展演变中，不仅仅是网络规模在增长，运算性能在提高，更重要的是各种应用的井喷式发展，使网络安全也发生质变。除了加密领域之外，诸如漏洞攻击、恶意代码(病毒、蠕虫、木马)、垃圾信息(邮件、网站)、网络欺诈(钓鱼网站、ARP 欺骗、DNS 劫持)、版权保护等安全问题层出不穷，显示出网络安全领域的活跃形势。

表 1.1 是信息安全五个历史阶段的概括。

表 1.1　信息安全的历史阶段

信息安全阶段	时间	安全手段	典型代表
古典密码时代	公元前～20 世纪初	手工方式	Caesar 密码
近代密码时代	20 世纪 20～40 年代	机电方式	Enigma 密码机
现代密码学时代	20 世纪 40～60 年代	电子数字计算机、信息安全理论	ENIAC 计算机、信息论、现代密码学
网络安全时代	20 世纪 60～90 年代	计算机网络	ARPANET、DES 加密、RSA 加密
大规模网络安全时代	20 世纪 90 年代至今	全球化互联网络	Internet、AES 加密

1.1.2 信息安全的概念

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然或者恶意原因的影响而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

信息安全的本质是对信息价值的保护。信息是一种资产，对一个组织来说是有价值的，因此需要妥善进行保护。信息安全就是要用各种有效手段，保护信息免受各种威胁攻击，保证业务连续性，将业务损失降至最少，同时最大限度地获得回报。

信息安全的基本要求如下。

(1)**真实性**：确认和识别一个主体或资源就是其所声称的，被认证的可以是用户、进程、系统和信息等。

(2)**保密性**：确保信息不被非授权的个人、实体或者过程获得和访问。

(3)**完整性**：保证数据不被篡改和销毁，保证系统以无害的方式按照预定的功能运行，不受有意的或者意外的非法操作所破坏。

(4)**抗抵赖性**：网络实体对自己的行为无法否认。

(5)**可用性**：保证授权实体在需要时可以正常地访问和使用系统。

(6)**可控性**：信息被访问的权限可以被有效控制。

(7)**可稽核性**：确保一个实体的访问动作可以被唯一的区别、跟踪和记录。

信息安全关心的是安全保护的成本与效益。安全总是相对的，没有绝对的安全。如果安全保护的成本低于受保护信息的价值，并且破解安全保护的代价超过信息的价值，那就可以认为是**相对安全**的。

【例 2】 DES(Data Encryption Standard，数据加密标准)算法是 IBM 公司于 20 世纪 70 年代中期研究成功并公开发表的。假设采用分布式穷举法破解，每个高性能结点的运算成本是 0.25 美元/小时，密码搜索能力是 2^{40} 个/小时。那么，对于 56 位 DES 加密的信息，价值超过多少才值得尝试破解？对于 168 位 3DES 加密的信息呢？

解：56 位 DES 加密的密码空间是 2^{56}，等概率情况下平均搜索 $2^{56}\times 50\%=2^{55}$ 个密码就能找到正确的那个。

按成本计算的破解能力是 $2^{40}\div 0.25=2^{42}$ 个/美元。

破解 56 位 DES 加密的平均成本是 $2^{55}\div 2^{42}=2^{13}$ 美元$\approx$8 千美元。

破解 168 位 3DES 加密的平均成本是 $2^{168}\times 50\%\div 2^{42}=2^{125}$ 美元$\approx 4.25\times 10^{23}$ 万亿美元。

当加密信息的价值超过上述破解成本，就值得去尝试破解。

【例 3】 RSA 算法是 R. Rivest、A. Shamir 和 L. Adleman 于 1977 年在美国麻省理工学院开发，于 1978 年首次公布的。假设用 512 位 RSA 加密，密钥(大素数)在 512 位整数中的平均密度是 0.12%，而当前以特殊优化过的分布式穷举法破解的成本是 2^{64} 密钥/美元。根据摩尔定律，计算能力每 18 个月性能加倍，且成本减半。那么多少年之后，512 位 RSA 加密保护价值 8 万亿美元的信息就不再安全了？

解：当前破解平均成本是 $2^{512}\times 0.12\%\times 50\%\div 2^{64}\approx 4.36\times 10^{17}$ 万亿美元。

根据摩尔定律，成本降低的速度是每 18 个月降为 1/4，则每年降为 $(1/4)^{2/3}=2^{-4/3}$。

设 x 年之后，平均破解成本会降低到 8 万亿美元，则 $4.36\times 10^{17}\times 2^{-4x/3}=8$，$x=\log_2(8\div(4.36\times 10^{17}))\times(-3/4)=(3-(\lg 4.36+17)/\lg 2)\times(-0.75)\approx 41.7$ 年。

因此 42 年后，512 位 RSA 加密保护价值 8 万亿美元的信息就不再安全了。

思考题 信息的价值都是显式意义上的吗？怎样理解那些“不惜代价”的尝试破解行为？

1.1.3 网络安全的知识体系

历史的原因，信息安全这一术语远比网络安全更早使用。但是当今的世界以计算机网络为信息载体，因此信息安全的核心问题主要体现在网络安全上。

网络安全是一个整体性的概念，并非学会几样黑客技术或加密算法就是懂得网络安全。技术会不断更新变化，所谓的先进技术也会快速没落和淘汰。在网络安全领域，利用别人的黑客工具和技术来实施攻击或防御操作属于低层次的技术活动，值得注意的是幕后那些研究安全漏洞、研发攻防工具、设计安全体系的人物。

学习是分不同层次的，由低到高依次是：

(1)**知道**：能够高效率地获取、筛选、存储各种信息。这一层次的创新性体现在需要吸收未知领域的信息时，高效率方法的灵活运用能力上。

(2)**知识**：能够把信息融会贯通，用来解决各种问题。这一层次的创新性体现在遇到前所未见的难题时，巧妙地解决问题的能力上。

(3)**求知**：能够提出自己的问题，从而引导对未知领域的探索。这一层次的创新体现在别人想不到的地方，能够发现有意义、有价值问题的思索能力上。

要真正全面掌握网络安全的知识并不容易，这是一个横跨多个学科的综合性领域。本书作为入门性的参考书籍，力图建立一个网络安全的知识体系框架，为以后的系统化深入学习打下基础。

图 1.1 是网络安全知识体系的一个立体坐标系。横向的 X 轴表示信息安全的历史发展趋势，如古典密码时代、网络安全时代等；纵向的 Y 轴表示网络安全的层次结构，如物理级安全、应用程序级安全等；深度方向的 Z 轴表示网络安全的相关学科，如运筹学、现代密码学等。

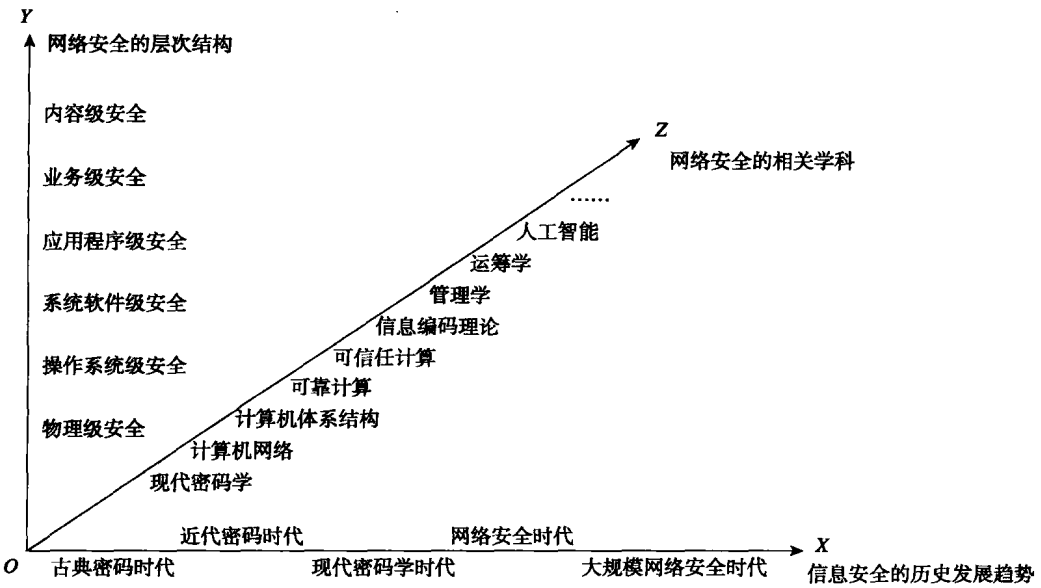

图 1.1 网络安全的知识体系

这是一个开放性的、动态的知识体系架构，随时处于演化更新之中。宏观上掌握好网络安全的知识体系，有助于迅速理解和把握现有和未来安全技术的细节。虽然技术在快速更新变化，但

万变不离其宗，各种各样的技术可纳入上述知识体系中，在立体坐标系上找到相应的位置。

1.1.4 信息安全的未来趋势

未来是不确定的，但可以从历史发展的情况中推测信息安全的一些未来趋势。

在密码发展的新动向中，混沌密码、椭圆曲线密码、量子密码、DNA 密码都可能成为未来加密技术的代表。

(1)**混沌密码**是利用混沌理论(俗称蝴蝶效应)来进行加密。其特点是对初始条件非常敏感，非线性的加密特征有利于保障加密的安全性。

(2)**椭圆曲线密码**是利用椭圆曲线上点群的离散对数问题来进行加密。目前公钥密码体制根据其所依据的数学难题分为三类：大整数分解问题类(如 RSA)、离散对数问题类(如 ElGamal)、椭圆曲线类。有时也把椭圆曲线类归为离散对数类。而椭圆曲线密码体制(ECC)是目前已知的公钥体制中，对每比特所提供加密强度最高的一种体制。

(3)**量子密码**是根据量子力学的原理进行加密。其中一种方法是利用量子纠缠现象，把量子态作为密钥来传送，并且利用量子态不可克隆及测量会引起波函数塌缩的特性来保障秘密性。

(4)**DNA 密码**是以脱氧核糖核酸(DNA)为信息存储的载体，借助 DNA 的生物化学特性来进行加密。一种方法是把密钥人工合成到 DNA 序列中，再隐藏到大量冗余 DNA 序列中去，利用大海捞针式的搜寻密钥难题来保障秘密性。

信息计算能力的进步推动着信息安全的发展，在经历了手工处理、密码机、电子计算机、计算机网络、大规模网络的阶段之后，未来很有可能迈进并行计算的阶段。分布式计算、函数计算、量子计算、DNA 计算都有希望成为并行计算的代表。

(1)**分布式计算**是把大计算量的任务分配给许多计算机同时计算，从而提高整体速度。在大规模网络中已经出现分布式计算的应用，如 1997 年的互联网破解 DES 加密、GIMPS 寻找大素数项目等。

(2)**函数计算**是用函数式编程取代过程式编程，用丘奇(Church)的函数模型(λ 演算系统)代替等价的图灵模型(图灵机)，从而简化图灵机的状态存储引起的并行计算同步问题，使并行计算可以安全地扩展。例如，Erlang 就是一种函数式编程语言。

(3)**量子计算**是利用量子态叠加原理，使处于叠加态的所有分量同时进行运算操作，形成量子并行性。量子态的数目能够以几何级数迅速变大，从而达到大运算量并行计算的效果。量子计算的算法例子有 Shor 的大数因子化、Grover 的数据库量子搜索等。

(4)**DNA 计算**是利用 DNA 的生物化学反应原理进行的并行计算。一种方式是用 DNA 双螺旋结构和碱基互补配对规律进行信息编码，将要运算的对象映射成 DNA 分子链，通过生物酶的作用，生成各种数据池，再按照一定的规则将原始问题的数据运算高度并行地映射成 DNA 分子链，进行可控的生化反应。例如，用 DNA 计算来解决“七顶点哈密顿路径问题”等。

人工智能也在信息安全领域大有用武之地。人工智能使计算机网络能够思维、决策、学习和求解问题，从而能够自动处理大量的网络安全问题。网络的智能化，将会使网络安全再次产生质的飞跃。

人工智能的众多分支领域中，与信息安全密切相关的有搜索推理、逻辑证明、问题求解、专家系统、机器学习、神经网络、进化计算、分布式智能代理、数据挖掘与知识发现、博弈决策等。1997 年，IBM 的“深蓝”计算机战胜国际象棋冠军卡斯帕罗夫，表明人工智能在某些领域已经达到实用的水平。

总体而言，上述前沿技术多数还处于理论研究阶段，距离实际应用还有一段时间，但是它们

的前景光明。

而在更贴近现实的信息安全的实用领域，五花八门的安全技术已经在走向大众。抵御恶意代码、入侵攻击方面，有入侵检测系统(IDS)、入侵防御系统(IPS)、主机入侵防御系统(HIPS)等。生物特征认证方面，有指纹识别、虹膜识别、语音识别等产品。还有信息隐藏伪装、数字版权管理(DRM)、可信任计算(Trusted Computing)、可靠计算(Dependable Computing)等方面的各种技术和产品，都为信息安全发挥着重要的作用。

信息战是信息安全攻防的一种激烈对抗形式。从信息安全的历史阶段看来，其实信息安全早就和战争密不可分，战争对信息安全的需求推动了信息安全的历史发展。凯撒密码、密码机、电子计算机、互联网都和战争或冷战直接相关；反过来，又需要和平利用这些工具来创造价值，遏制战争。为保卫数字化疆土的安全，目前，各国开始设置信息战指挥机构。例如，美国在2009年成立网络战司令部，日本也计划建立网络空间防卫队。

信息战不仅限于狭义上的战争范畴，也不仅限于信息系统破坏和密码破解上的攻防。实际上，情报采集、信息伪造、舆论攻势、心理战等都属于信息战范畴。非战时环境下，一些团体(包括政府机构、企业等)与个人也会出现信息战的形态，规模未必很小。因此，在网络安全的未来趋势之中，信息战是不可忽视的一部分。

1.2 网络安全的层次结构

网络安全是一个整体性概念，涵盖了各种纷繁复杂的安全问题。把网络安全划分出层次结构，有助于系统地理解和解决网络安全的种种问题。图1.2是网络安全六层模型，从低到高依次是：物理级、操作系统级、系统软件级、应用程序级、业务级、内容级。这是参考了OSI七层网络模型、计算机体系结构六层模型而得到的，与计算机系统的多层次结构、网络模型的分层理念一脉相承。

图1.3是OSI七层网络模型，从低到高依次是：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。

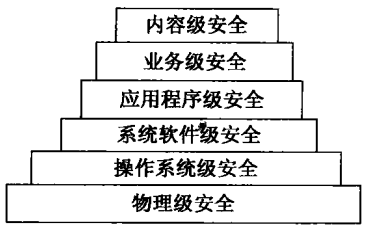

图1.2 网络安全六层模型

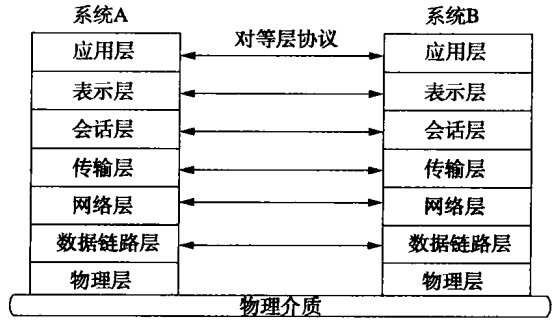

图1.3 OSI七层网络模型

正如OSI七层网络模型只是一个比较完善的理论模型，现实中的TCP/IP等网络结构并不完全与它吻合，网络安全六层模型也只是理论上的一种划分，实际情况下的网络安全层次不必严格遵循这种模型。

图1.4是计算机体系结构六层模型，从低到高依次是：微程序级、机器语言级、操作系统级、汇编语言级、高级语言级、应用语言级。

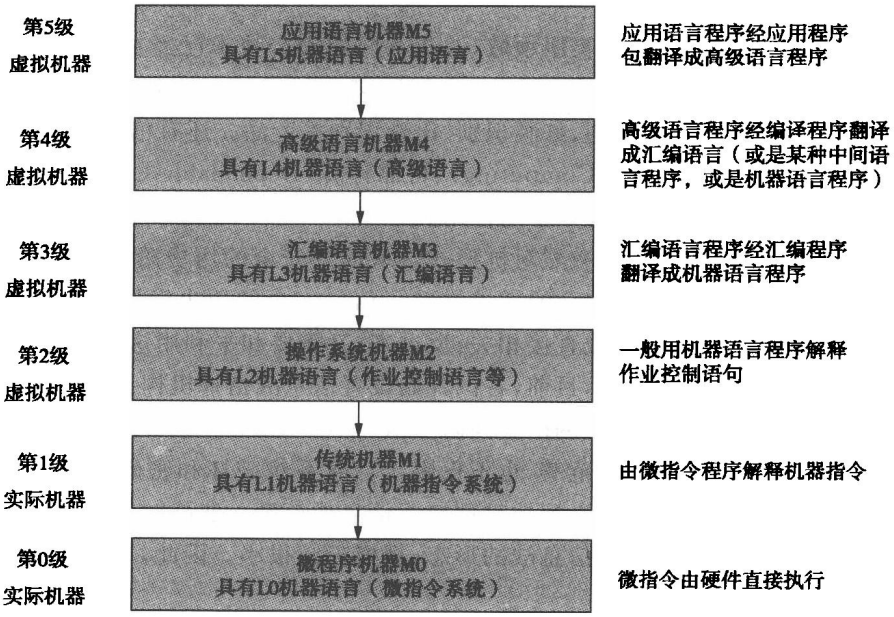

图 1.4　计算机体系结构六层模型

下面对网络安全的六层模型作简单介绍。

1. 物理级

物理级安全：包括计算机硬件、网络线路、操作人员等的安全因素。这其实是整个信息安全体系最重要的立足之本，但往往被人们所忽视。这一层的常见安全事件是敏感系统受到人为的物理接触，线路窃听，操作人员受社交工程学欺骗等。

物理级的安全防护需要针对具体的事物，如硬件上的电磁屏蔽、芯片级的加密认证、人员的专业训练等。

在整个网络安全防御体系中，人是必不可少的一环。而人又不同于机器，具有易出错、易动摇、易受骗等弱点。因此，对人的训练和管理非常重要。

2. 操作系统级

操作系统级安全：这是软件系统的最底层，包括操作系统、虚拟机、机群等一系列相关平台的安全。这一层的常见安全事件是通过漏洞入侵，病毒、木马、蠕虫等恶意代码感染，窃取系统控制权等。

2005 年以前比较常见的端口扫描、主机漏洞扫描入侵，就是针对操作系统层的攻击方式。对应的常用防御方式是防火墙、补丁升级。近年来由于实时自动升级、防火墙部署普遍加强，这类攻击的成功率有降低的趋势，攻击重心转向应用程序等更高层次。

但是有一类称为零日攻击(Zero-day Attack)的新兴手法，是利用每个新出现漏洞的升级补丁尚未推出的时间差，实现迅速入侵。零日攻击并非不可抵御，利用纵深防御可以阻止操作系统层的漏洞扩散。

Rootkit 也是一种恶意代码，比普通病毒、木马、蠕虫更强的地方是 Rootkit 处于操作系统层的核心，普通的防病毒等软件很难发现。但 Rootkit 同样并非不可抵御，仍然利用纵深防御，根源于物理层的可信任计算模块(如 TPM、TCM)就能克制 Rootkit。

操作系统级的安全防护方式，常见的有系统补丁、入侵检测系统(IDS)、入侵防护系统(IPS)、主机入侵防护系统(HIPS)等。比较新的安全措施则有虚拟机机群等。

3. 系统软件级

系统软件级安全：系统软件是介于操作系统和应用程序之间的一层，包括各种 Web 服务器软件、电子邮件系统、DNS 域名服务系统、数据库、中间件和其他相关软件的安全。这一层的常见安全事件是网页篡改、邮件欺诈或泄漏、域名劫持、数据库入侵等。

系统软件级的常见攻击方式有数据库入侵、网页篡改、DNS 劫持、邮件账号窃取等。例如，2010 年的百度网站篡改事件，就是由 DNS 劫持而引起的。

系统软件级的常规防御措施仍然是软件升级、漏洞补丁。而正确的软件安全设置也必不可少，往往一个适当的文件目录权限设置就能够阻止绝大多数的入侵企图。

4. 应用程序级

应用程序级安全：涉及应用层功能，包括各种为项目定制开发的应用程序的安全。这一层的常见安全事件是各种漏洞攻击。例如，缓冲区溢出、SQL 注入、文件上传漏洞等。

操作系统级、应用软件级的基础平台相对比较统一，而应用程序级的软件则五花八门，是根据形形色色的个性化需求，由各种各样技术水平高低不同的人开发而成。这就导致了应用程序的质量良莠不齐，难免出现各种漏洞。

近年来的入侵攻击重心转向应用程序级，正是因为这一层的漏洞较多，攻击成功率较高。例如，SQL 注入攻击就是利用了开发者没有严格控制输入数据的合法性，通过构造特殊的 SQL 指令来实现入侵。

应用程序级的常规防御措施分两种，一种是亡羊补牢式的，如给现有应用程序加入防 SQL 注入补丁；一种是原生防护式的，就是在应用程序开发之初就严格控制软件质量，防止漏洞的产生。无论是安全成本还是效益，亡羊补牢式都比不上原生防护式的防御。

本书后面的应用程序级安全一章所介绍的国际机场安检模式，就是一种原生防护式的防御方法。

5. 业务级

业务级安全：涉及具体的业务应用，如用户登录、业务权限分配等的安全。这一层的常见安全事件是业务员越权操作、账户权限泄露、管理员密码丢失等。

这一层的安全问题不再纠缠于具体软件，而是集中在实际的业务流程中。诸如身份认证、权限控制、数字签名、安全多方计算等，都是业务流程里的常见环节，也是安全保护的重点领域。业务级的常见攻击方式有密码破解、散列碰撞、伪造签名等。例如 2004 年，王小云找到 MD5 散列强碰撞的方法。

业务级的常规防御措施仍然是算法的改进，利用更强的密钥、更坚固的算法来抵御攻击。利用不断提高的计算机硬件性能，可以在保障速度的前提下提高加密强度。近年来 DSP、GPU 等高速运算硬件技术的发展，允许密钥长度显著增长，而速度不会大幅下降。

6. 内容级

内容级安全：涉及业务系统的信息内容安全，如有版权保护的图书网站内容等。这一层的常