网络与信息安全

主摇编：李摇峰摇李摇平
副主编：王摇静摇蔡碧野
编摇委：鲁荣波摇邓晓衡摇刘军万摇刘摇青
摇摇摇摇张连明摇谭摇邦摇李梦醒

中南大学出版社

高等院校计算机系列教材编委会

总摇序

圆示世纪，人类社会已经步入信息时代，信息产业推动着全球经济的蓬勃发展，改变着人类的联系与交换方式，从某种意义上说，信息革命是人类历史上又一次深刻的社会变革。无疑，在以信息产业为基础的知识经济社会中，计算机科学与技术具有举足轻重的地位。有鉴于此，当今世界各国皆把培养高素质的创新型计算机科学与技术专业人才作为一项重要的战略任务来抓。早在 灵愿源年，邓小平同志就强调指出：“计算机的普及要从娃娃抓起”，从此开启了中国信息革命的征程。经过 圆园多年的努力，我国的计算机教育虽然取得了令人瞩目的成就，但离知识经济社会的要求还有很大的差距。据 圆园园缘年信息产业部的数据显示，我国的信息化人才资源指数仅为 灵愿源源，每年短缺信息化专业人才达 员园园万之多。因此，快速培养和造就一大批高素质的计算机与信息人才，乃是我国高等教育所面临的一项严峻挑战。为此，我们必须改革和完善现有计算机与信息技术学科的教学计划和课程体系，优化课程结构，精炼教学内容，拓宽专业基础，强化实践环节，注重学生的知识、能力和综合素质的培养。

为了适应计算机科学与技术学科发展和教育的需要，湖南省计算机学会，参照《中国计算机科学与技术学科教程 圆园园缘》，组织了一批长期从事计算机科学与技术专业教学与科研的学者参与编撰了这套由中南大学出版社出版的《高等院校计算机系列教材》，希望在教材中及时反映学科前沿的研究成果与发展趋势，以高水平的科研促进教材建设，以优秀教材促进教学质量的提高。该系列教材具有如下特点：

员．教材参照《中国计算机科学与技术学科教程 圆园园缘》建议的教学大纲、知识领域、知识单元和知识点，结合作者多年教学与科研经验来编写，注重基本理论、基础知识的梳理、推演与挖掘，注意知识的更新，跟踪新技术、新成果的发展，并将之吸收到教材中来，力求开阔学生视野，逐步形成“基础课程精深，专业课程宽新”的格局，努力提高教材质量。

圆．注重理论联系实际，注意能力培养。力图通过案例教学、课堂讨论、课程实验设计与实习，训练学生掌握知识、运用知识分析并解决实际问题的能力以满足学生今后从事科研和就业的需要。

猿．在规范教材编写体例的同时，注重写作风格的灵活性：每册的每个章节包括教学目的、本章小结、思考题与练习题，每门教材都配有 学栽电子教案，并做到层次分明、逻辑性强、概念清楚、图文并茂、表达准确、可读性强。

这套教材的编写吸纳了广大计算机科学与技术教育工作者多年的教学与科研成果，凝聚了作者们的辛勤劳动，也得到了湖南省各高等院校相关专业领导和专家的大力支持。我相信这套教材的出版，对我国计算机科学与技术专业本科教学质量的提高将有很好的促进作用。

由于编委和作者们水平与时间的限制，教材中难免还有不足之处，恳请广大读者批评指正。

二〇一〇年 苑月

前摇言

随着互联网络的迅猛发展，安全问题越来越引起人们的关注。由于其开放性和匿名性的特点，互联网络在改变着人们的工作效率和生活方式，给社会、企业乃至个人带来了前所未有的便利的同时，也决定了单纯的互联网不可避免地存在信息安全隐患。从当初的计算机网络病毒的产生和传播，到现在网络犯罪、信用欺诈等带有明显破坏性的网络恶意行为的出现，无一不说明了信息网络安全绝不仅是 [illegible] 行业内的问题，而是一个社会问题，是一个包括多学科的系统安全工程问题。

从学科研究的角度来看，信息安全是一个综合性强、交叉性广的学科领域，涉及数学、通信、计算机等诸多学科的知识和研究成果。正由于网络与信息安全问题是当前研究的热点以及网络应用的焦点问题，越来越多的高等院校先后开设了信息安全等相关课程。本书作为湖南省计算机学会组织编写的《湖南省高等院校计算机课程系列教材》之一，根据安全技术的最新研究成果和研究进展，结合平时的教学体会，编写而成。

本书注重跟踪网络与信息安全领域内的最新研究成果，比较全面系统地介绍了 [illegible] 安全基础理论，包括信息安全理论基础、对称及非对称加密体系、数字签名及安全验证机制等 [illegible] 互联网络中常用的安全技术，包括 [illegible] 技术、网络安全的集成技术、[illegible] 体系、[illegible] 及电子邮件的安全性，以及操作系统的安全等 [illegible] 新型网络应用中的信息安全技术，如在无线及 [illegible] 网络中的安全应用研究等。本书紧紧围绕“互联网络中的信息安全”这个中心主题，以基础理论、技术机制再到应用实践为线索对信息安全进行了有重点的阐述，力图使读者能够较全面地了解网络与信息安全领域内要研究的问题、相应的解决机制，并能逐渐地培养出运用安全技术在具体实践中解决实际问题的能力。

全书共分 [illegible] 章。教学过程中教师可根据具体情况酌情选用本书的相关章节。同时，本书也配备了相应的多媒体课件，供授课教师参考。全书由李峰教授和李平博士担任主编，其中第 [illegible] 章由李峰编写，第 [illegible] 章由李平编写，第 [illegible] 章由鲁荣波编写，第 [illegible] 章由刘青编写，第 [illegible] 章由蔡碧野编写，第 [illegible] 章由李梦醒编写，第 [illegible] 章由王静编写，第 [illegible] 章由张连明编写，第 [illegible] 章由邓晓衡编写，第 [illegible] 章由刘军万编写，第 [illegible] 章由谭邦编写，另外，王静、蔡碧野还参与了全书的统稿工作。本书在编写过程中得到了湖南省计算机学会和中南大学出版社的大力支持，孙星明教授、肖建华教授、曾碧卿副教授认真审阅了全书，提出了大量宝贵的修改意见。在此深表感谢！

随着安全技术研究的深入和应用领域的延伸，网络与信息安全的内涵在不断地丰富和充实。由于编者水平有限，我们对这一新兴领域的研究还不很深入，书中难免存在错误和不足之处，欢迎广大读者和专家提出批评改进意见。

本书配有 [illegible] 电子课件，需要使用的教师请与出版社联系。电子邮箱 [illegible]

编摇者

[illegible] 年 [illegible] 月

目摇录

第 员章摇概摇论

本章介绍了如下几个方面的内容：①信息安全的基本概念；②网络的脆弱性及安全威胁；③安全机制与安全策略；④安全评估标准；⑤网络安全模型。通过本章的学习，要求学生达到以下几点教学要求：

(员) 掌握信息安全的基本概念，了解网络与信息安全的背景及研究的主要问题。

(圆) 了解网络系统的脆弱性和信息安全面临的安全主要威胁。

(猿) 掌握安全机制与安全策略中的基本要素。

(源) 了解安全评估标准，掌握网络安全模型。

员援员摇信息安全基本概念

人类已进入 圆员世纪，无处不在的计算机网络连接了科研、文化、经济与国防等各个领域，数字化、信息化、网络化正在冲击、影响、改变着人类社会的各个方面。以 [illegible] 为代表的全球性信息化浪潮日益深刻，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全问题日益成为影响网络效能的重要问题，而 [illegible] 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求。这主要表现在：开放性的网络，导致网络技术是全开放的，任何个人或团体都可能获得，因而网络所面临的破坏和攻击可能是多方面的，如可能来自物理传输线路的攻击，也可以对网络通信协议和实现实施攻击，可以是对软件实施攻击，也可以是对硬件实施攻击。随着计算机及网络技术的飞速发展，网络中不安全因素也在逐渐增加。因此，不强化网络化的信息安全保障，不解决信息安全问题，信息化将不可能持续、健康地发展。

究竟什么是信息安全呢？根据词典上的解释，“安全”有两层含义：其一指“平安，无危险”；其二是“保护，保全”。在具体应用和实践中，情况就相当复杂了。从安全需求角度来讲，信息安全应包括以下六个基本要素：机密性、完整性、可靠性、可用性、可控性和不可抵赖性等，其主要特征表现如下：

- 机密性 ([illegible])：机密性是网络信息不被泄露给非授权的用户、实体或过程，不被非法利用，即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性，如信息的加密传输、数据的保密存储等。机密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。
- 完整性 ([illegible])：完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持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。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

- 可靠性（[illegible]）：可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定的功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。可靠性可以用公式描述为 [illegible]，其中 [illegible] 表示可靠性，[illegible] 表示平均故障间隔时间，[illegible] 表示平均故障修复时间。因此，增大可靠性的有效思路是增大平均故障间隔时间或者减少平均故障修复时间。增大可靠性的具体措施包括：提高设备质量，严格质量管理，配备必要的冗余和备份，采用容错、纠错和自愈等措施，选择合理的拓扑结构和路由分配，强化灾害恢复机制，分散配置和负荷等。可靠性测度主要有三种：抗毁性、生存性和有效性。
- 可用性（[illegible]）：可用性是网络信息可被授权实体访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。
- 可控性（[illegible]）：可控性是指可以控制授权范围内的信息流向及行为方式，对信息的传播及内容具有控制能力。为保证可控性，首先系统能够控制谁能够访问系统和网络上的数据，以及如何访问（是只读还是可以修改等），通常通过访问控制列表等方法来实现；其次需要对网络上的用户进行验证，可通过握手协议和鉴别进行身份验证；最后要将用户的所有活动记录下来便于查询审计。
- 不可抵赖性（[illegible]）：不可抵赖也称作不可否认性，是指在网络信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

概括地说，网络与信息安全的核心是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的消息的机密性、完整性、可靠性、可用性、可控性和不可抵赖性等。

国际标准化组织（[illegible]）对信息安全的定义是：“为数据处理系统建立和采用的技术和管理上的安全保护，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。”此定义偏重于静态信息保护，而且没有考虑网络的因素。另一种考虑到网络因素的定义是：“保护网络系统中的各种资源（包括计算机和网络设备、存储介质、软件、数据等）不因偶然或恶意的原因而遭到占用、毁坏、更改和泄露，系统能够连续正常运行。”此定义侧重于动态意义的描述。

网络与信息安全是一门涉及计算机科学、网络技术、密码技术、通信技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。信息安全是一个关系国家安全和主权、社会稳定、民族文化的继承和发扬的重要问题。并且其重要性正随着全球信息化步伐的加快而变到越来越重要，信息安全问题刻不容缓。

员员摇网络的脆弱性和安全威胁

员员援员摇网络信息系统的脆弱性

员员援员援员摇系统脆弱性的主要原因

从技术的角度看，网络信息系统脆弱的主要原因有三个方面：

- 网络的开放性。

从网络的本质性来看，网络的根本就是实现所有信息和资源的共享。但在实现共享的同时，也就为攻击者对于资源的访问提供了便利。

从网络协议体系的实现机制来看，网络上承载的业务都是基于公开的协议。协议算法可能侧重在实现某种特定功能，而在一定程度上忽视了安全防范。

从信息传输的机制来看，如构成网络基本单元的局域网采用的是共享传输介质的广播信道，特别是无线局域网采用的是空间信道，使得消息截获相对容易。

- 黑客（与[illegible]及病毒等恶意程序的攻击。

当今的黑客是指那些专门闯入计算机网络系统，非法的入侵和破坏、窃取信息的攻击者。而计算机病毒是指能利用系统进行自我复制和传播，通过特定事件触发破坏系统的程序，根据其自我复制和传播的方式又分为引导型、文件型、宏病毒、邮件传播等类型。除此之外还有一些有害程序，如程序后门、特洛伊木马、“细菌”程序、蠕虫等。

- 系统平台与系统软件的自身缺陷。

操作系统是硬件和软件应用程序之间接口的程序模块，它是整个网络信息系统的核心控制软件，系统的安全体现在整个操作系统中。数据库是从操作系统的文件系统上派生出来的用于大量数据管理的系统。数据库的全部数据都记录在存储媒体上，并由数据库管理系统（[illegible]）统一管理、维护和恢复。由于人们的认知能力和实践能力的局限性，在系统设计和开发过程中会产生许多的错误、缺陷和遗漏，成为安全隐患，而且系统越大、越复杂，这种安全隐患越多。

员员援员援圆摇[illegible]分层体系结构的脆弱性分析

现有网络信息系统都不可避免地存在安全缺陷，为了便于理解，下面从典型的[illegible]网络[illegible]参考模型入手，简单描述在各协议层次上系统的脆弱性：

（员）物理层

到目前为止，大部分的网络联接设备采用的是双绞线和铜缆，它们不可避免地会产生电磁干扰（[illegible]）和电磁辐射，如果有足够的设备和耐心，完全可以接收到通信链路中传输的信号并加以还原，窃取重要信息，甚至插入、删除信息。无线信道的安全性更加脆弱，几乎不可避免地会遭受到被窃听或劫持等攻击。采用光纤方式，由于传播的是光信号而不是电信号，不会产生电磁辐射，安全性能有所提高，但仍然面临被截断和搭线的威胁。

（圆）数据链路层

数据监听是数据链路层最常见的攻击手段。目前的局域网基本上都采用以广播为技术基础的以太网，各主机处于同一信任域，传输信息可以相互监听。因此，只要接入以太网上的任一节点，就可以捕获在这个以太网上发送的所有数据包，从而窃取关键信息，这是以太网

所固有的安全隐患。要解决这个问题，首先，应当尽可能地划分网段，将非授权用户与敏感的网络资源相互隔离，从而防止可能的非法监听。其次，以交换式集线器代表广泛使用的共享式集线器，减少数据监听的设备基础。再者，还可以运用虚拟局域网技术，把所有服务器和用户节点都放在各自的虚拟局域网内，将以太网通信变为点对点通信，互不干扰。

(2) 网络层

[illegible]协议是[illegible]世纪[illegible]年代以来发展最为迅速的协议，尽管它们在网络互联方面取得了巨大的成功，但是由于[illegible]在设计之初并没有考虑到安全性问题，因此在协议层次上具有相当多的安全漏洞。网络层典型的安全问题有：

- [illegible]欺骗，伪造[illegible]地址以获取非法权利；
- 利用源路由选项，侦听数据；
- 对路由协议，如[illegible]等进行攻击；
- 利用[illegible]的[illegible]报文破坏路由机制。

为了尽可能解决这些安全性问题，[illegible]的技术管理机构[illegible]提出了一种新版本[illegible]协议[illegible]，通过[illegible]数据包首部后面的扩展首部实现安全特性，在鉴别和保密两个方面制定了一系列标准，并强制性地要求支持这些安全标准。

(3) 传输层

[illegible]协议的实现为黑客们留下了攻击空间，它的三次握手建链方式，成为实现[illegible]拒绝服务攻击方式的基础，而且[illegible]连接很容易被欺骗、截取和破坏。除此之外，伪造[illegible]中的源地址、源端口也是一种常见的地址欺骗方式。

(4) 应用层

应用层存在认证、访问控制、完整性、保密性等所有安全问题。如应用层的许多协议缺少严格的加密认证机制，[illegible]便是一例。[illegible]提供主机名与[illegible]地址的映射关系，它从出现以来就缺乏加密认证机制，所以黑客很容易在监听、伪造的基础上进行攻击。其他比较常见的网络软件与网络服务的漏洞有：[illegible]的[illegible]调用、[illegible]漏洞、匿名[illegible]和远程登录，等等。

综上所述，尽管计算机网络迅速发展并提供了各种各样的应用，但其技术基础是不安全的。下面将分析网络面临的主要威胁和可能遭受的攻击，目的是使我们全面了解网络信息系统的脆弱性及所面临的危险，从而提高安全意识。

3. 操作系统及数据库的脆弱性

操作系统不安全是系统不安全的根本原因，绝大部分的攻击都借助了操作系统本身的漏洞。操作系统及数据库系统安全的弱点主要表现在以下几个方面：

- 操作系统支持系统继承和扩展的能力给系统自身留下了一个漏洞。操作系统的程序允许进行动态连接，[illegible]的驱动程序与系统服务都可以用动态连接的方式挂接到操作系统上。这种方法虽然给系统的扩展和升级带来了方便，同时也为黑客和计算机病毒产生打开了方便之门。
- 操作系统支持在网络上传输文件，上传可执行文件方便了病毒和黑客程序的加载。
- 操作系统支持创建进程，特别是支持在网络的结点上进行远程的创建与激活，被创建的进程还可以继承创建进程的权力。将此功能与第二点结合可以实现黑客程序的远程安装。
- 操作系统的守护进程具有与操作系统核心层软件同等的权利，另外，操作系统提供的[illegible]与[illegible]都是黑客可以利用的程序。