浩强创作室
HAO QIANG STUDIO

21世纪高校计算机应用技术系列规划教材

谭浩强 主编

计算机安全技术

宋红 吴建军 岳俊梅 编著

★本着“理论知识够用为度，重在实践应用”的原则进行编写。

★本书内容丰富、重点突出，引导读者掌握计算机安全技术的知识要点。

★适于作为高职高专、成人高校、应用型本科计算机专业及相关专业的教材。

★也可作为计算机网络管理员、信息安全管理员培训和自学的教材。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

21世纪高校计算机应用技术系列规划教材

计算机安全技术

谭浩强 主编

宋红 吴建军 岳俊梅 编著

中国铁道出版社

2003·北京

（京）新登字063号

内 容 简 介

计算机安全主要包括操作系统安全、数据库安全和网络安全3部分。其中网络安全是目前备受关注的问题。本书从计算机安全的基础知识、计算机实体及硬件安全、计算机软件安全、操作系统安全、密码安全、数据库安全、计算机病毒技术、网络安全基础知识、防火墙技术、黑客的攻击和防范技术等几个方面来组织编写。

本书是本着“理论知识以够用为度，重在实践应用”的原则进行编写的，书中提供了大量的操作系统、数据库、网络安全的实例，从实例中引出概念，帮助读者掌握计算机安全的基本原理及胜任计算机和网络安全管理的工作。

本书是作者在总结了多年教学经验的基础上写成的，适合用作高职高专计算机专业、应用型本科计算机专业及相近专业的课程教材，也可供自学者使用。

图书在版编目（CIP）数据

计算机安全技术/宋红，吴建军，岳俊梅编著. －北京：中国铁道出版社，2003.8

（21世纪高校计算机应用技术系列规划教材）

ISBN 7－113－05341－6

Ⅰ.计… Ⅱ.①宋… ②吴… ③岳… Ⅲ.电子计算机-安全技术-高等学校-教材 Ⅳ.TP309

中国版本图书馆CIP数据核字(2003)第078128号

书　　名：计算机安全技术

作　　者：宋　红　吴建军　岳俊梅

出版发行：中国铁道出版社（100054，北京市宣武区右安门西街8号）

策划编辑：严晓舟　魏　春

责任编辑：苏　茜　黄园园

封面设计：孙天昭

印　　刷：北京鑫正大印刷有限公司

开　　本：787×1092　1/16　印张：15.75　字数：375千

版　　本：2003年9月第1版　2003年9月第1次印刷

印　　数：1～5000册

书　　号：ISBN 7-113-05341-6/TP・977

定　　价：24.00元

21世纪高校计算机应用技术系列规划教材

编委会名单

主　　任：谭浩强

副主任：陈维兴　严晓舟

委　　员：（以下排名按姓氏字母的先后顺序为序）

安淑芝　安志远　侯冬梅　李雁翎　吕凤翥

秦建中　宋　红　宋金珂　孙中胜　魏　春

魏善沛　熊伟建　薛淑斌　赵乃真　訾秀玲

丛书序言

21世纪是信息技术高度发展并且得到广泛应用的时代，信息技术深刻地改变了人类的生活、工作和思维方式。每一个人都应当学习信息技术、应用信息技术。人们平常习惯说的计算机教育其内涵实际上已经发展为信息技术教育，内容主要包括计算机和网络的基本知识和应用。

对多数人来说，学习计算机的目的是为了利用计算机这个现代化工具去处理工作和面临的各种问题，使自己能够跟上时代前进的步伐，同时要在学习的过程中努力培养自己的信息素养，使自己具有信息时代所要求的科学素质，站在信息技术发展和应用的前列，推动我国信息技术的发展。

学习计算机课程，有两种不同的方法，一是从理论入手；一是从实际应用入手。不同的人有不同的学习内容和学习方法。大学生中的多数人将来是各行各业中的计算机应用人才。对他们来说，不仅需要解决**知道什么**，更重要的是**会做什么**。因此要以应用为目的，注重培养应用能力，大力加强实践环节，激励创新意识。

根据实际教学的需要，我们组织编写这套**“21世纪高校计算机应用技术系列规划教材”**。顾名思义，这套丛书的特点是突出应用技术，面向实际应用。在选材上，根据实际应用的需要决定内容的取舍，坚决舍弃那些现在用不到、将来也用不到的内容。在叙述方法上，采取**“提出问题——介绍解决问题的方法——归纳结论和概念”**的三部曲，这种从实际到理论、从具体到抽象、从个别到一般的方法，符合人们的认识规律，实践证明已取得了很好的效果。

本丛书采取模块化的结构，根据需要确定一批书目，也就是提供一个课程菜单供各校选用，以后根据信息技术的发展和教学的需要，不断地补充和调整。只要教学有需要，我们就组织编写新的教材，不受任何框框的限制。我们的指导思想是面向实际，面向应用，面向对象。这样比较灵活，能满足不同学校、不同专业的需要。希望各校的老师把你们的要求反映给我们，我们将会尽最大努力满足大家的要求。

本丛书可以作为大学计算机应用技术课程教材以及高职高专、成人高校和面向社会的培训班的教材，也可作为学习计算机的自学教材。

参加本丛书策划和编写工作的专家和老师有：谭浩强、陈维兴、严晓舟、薛淑斌、秦建中、安淑芝、安志远、赵乃真、吕凤翥、李雁翎、宋红、周永恒、熊伟建、宋金珂、陈元春、冯继生、姚怡、沈洪、沈添、李尊朝、王晓敏、侯冬梅、訾秀玲、魏善沛、孙中胜、王丙义、程爱民、史秀璋、李振银、刘涛、李宁等。此外参加本丛书编辑和其他工作的还有：魏春、秦绪好、张艳芳、戴薇、郭晓溪、马建、姜淑静、姜天鹏、杨东晓、于静等。对于他们的智慧、奉献和劳动表示深切的谢意。中国铁道出版社以很高的热情和效率组织了丛书的出版工作。在组织编写出版的过程中，得到全国高等院校计算机基础教育研究会和各高等院校老师的热情鼓励和支持，对此谨表衷心的感谢。

本丛书如有不足之处，请各位专家、老师和广大读者不吝指正。

谭浩强谨识

2003年2月于清华园

前　言

近年来，随着计算机技术和计算机互联网建设的发展与完善，计算机安全问题逐步成为计算机界关注和讨论的焦点。计算机技术和网络技术已深入到社会的各个领域，人类对计算机和计算机网络的依赖性越来越大。那么，普及计算机安全知识就成为保护我国计算机和网络安全的头等大事。对高职高专计算机专业、应用型本科计算机专业及相近专业的学生开设计算机安全技术课是十分必要的。

本书是本着“理论知识以够用为度，重在实践应用”的原则进行编写的。全书主要内容包括计算机硬件和软件的安全、操作系统的安全、密码技术、数据库的安全、计算机病毒技术、防火墙技术、黑客技术和网络安全的基本知识等，共分 10 章。本书的教学内容大约需要 60 学时，书中加*标记的为应用型本科生选讲的内容。

第 1 章主要阐述了研究计算机安全的重要性，简要地介绍了计算机安全等级和安全法规。第 2 章具体介绍了实体及硬件的安全防护，计算机硬件的检测与维修等主要内容。第 3 章介绍了计算机软件安全技术，包括软件分析技术、软件保护技术、反跟踪技术、软件加壳与脱壳等方面的内容。第 4 章阐述了 Windows、Unix、Linux 等操作系统的安全，其中具体介绍了 Windows 系统、Unix 系统、Linux 系统的安全机制、安全管理、安全漏洞和解决方法。第 5 章讲述了数据加密标准 DES、国际数据加密算法 IDEA、RSA 算法等常见的加密算法及其具体的实现过程，同时详细介绍了加密技术的典型应用——数字签名的实现方法。第 6 章简要介绍了数据库安全技术，以 Oracle 数据库为例说明了数据库备份、恢复的方法和具体实施步骤。第 7 章介绍了计算机病毒的结构、类型和工作原理，列举了一些检测、防范和清除病毒的常用技术。第 8 章简要介绍了网络安全的理论基础知识。第 9 章介绍了访问控制中的防火墙技术，包括防火墙的原理、种类和实现策略。第 10 章主要介绍了常用的黑客攻击方法，如口令攻击、放置特洛伊木马程序、Web 欺骗、缓冲区溢出、端口扫描攻击等，同时列举了常用的 6 项防黑措施。

本书既可以作为高职高专、成人高校和应用型本科计算机专业和相近专业的教材，也适合作为计算机网络管理员、信息安全管理员培训和自学的教材。

本书由宋红担任主编，吴建军、岳俊梅参加编写。吴建军老师编写了第 1 章、第 2 章、第 3 章、第 5 章、第 8 章、第 9 章、第 10 章，岳俊梅老师编写了第 4 章、第 6 章、第 7 章，宋红老师负责全书的统稿，陈贤淑、陈晓娟、廖康良等参与了本书的编排工作。

由于作者水平有限，书中不免有疏漏和不足之处，欢迎各位读者批评指正。我们也会在适当时间进行修订和补充，并发布在天勤网站：http://www.tqbooks.net“图书修订”栏目中。

编著者

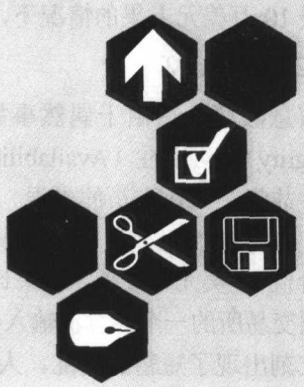
2003 年 8 月

目　录

1

计算机安全概论

随着计算机在社会各个领域的广泛应用和迅速普及，人类社会业已步入信息时代。信息已经成为了人类的一种重要资源，人们生产和生活的质量将愈来愈多的取决于对知识信息的掌握和运用的程度。面对汪洋大海般的信息，计算机成为了信息处理必不可少的工具。在计算机系统中，信息是指存储于计算机及其外部设备上的程序和数据。由于计算机系统中的信息涉及到有关国家安全的政治、经济、军事的情况以及一些部门、机构、组织与个人的机密，因此极易受到敌对势力以及一些非法用户、别有用心者的威胁和攻击。加之几乎所有的计算机系统都存在着不同程度的安全隐患，所以，计算机系统的安全、保密问题越来越受到人们的重视。



1-1 计算机安全研究的重要性

1-1-1 计算机系统面临的威胁

计算机信息系统面临的威胁主要来自自然灾害构成的威胁、人为和偶然事故构成的威胁、计算机犯罪的威胁、计算机病毒的威胁、信息战的威胁等，大体可分为2类：一类是对实体的威胁；另一类是对信息的威胁。其中，有些威胁则包含了对计算机系统实体和信息两方面的威胁和攻击，如计算机犯罪和计算机病毒。

1. 对实体的威胁和攻击

所谓实体，是指实施信息收集、传输、存储、加工处理、分发和利用的计算机及其外部设备和网络。对实体的威胁和攻击是对计算机本身和外部设备以及网络和通信线路而言的。这些威胁主要有：各种自然灾害、人为的破坏、设备故障、操作失误、场地和环境的影响、电磁干扰、电磁泄漏、各种媒体的被盗及数据资料的损失等。

由于实体涉及的设备分布极为广泛，任何个人或组织都不可能时刻对这些设备进行全面的监控。任何安置在不能上锁的地方的设施，包括有线通讯线、电话线、局域网、远程网等都有可能遭到破坏，从而引起业务的中断，如果是包含数据的软盘、光盘、主机等被盗，更会引起数据的丢失和泄漏。因此，做好对计算机系统实体的保护是计算机安全工作的首要一步，也是防止各种威胁和攻击的基本屏障。

2. 对信息的威胁和攻击

由于计算机信息有共享和易于扩散等特性，使得它在处理、存储、传输和使用上有着严重的脆弱性，很容易被干扰、滥用、遗漏和丢失，甚至被泄露、窃取、篡改、冒充和破坏，还有可能受到计算机病毒的感染。威胁和攻击可细分为2类，即信息泄漏和信息破坏。

（1）信息泄漏

信息泄漏即故意或偶然地侦收、截获、窃取、分析和收到系统中的信息，特别是机密和敏感信息，造成泄密事件。例如，环球音乐唱片公司的客户资料曾被一18岁俄罗斯黑客窃取，在索要10万美元未果的情况下，将所有的客户资料信息公布于众，造成了巨大的经济损失。

（2）信息破坏

信息破坏是指由于偶然事故或人为因素破坏信息的机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）及真实性（Authenticity）。其中，偶然事故包括：计算机软硬件故障、工作人员的失误、自然灾害的破坏、环境的剧烈变化等引起的各种信息破坏。例如，1992年5月8日美联社报道，美国北达科他州的一位农民打算从某政府部门手中领取一张价值31美元的支票，结果计算机在支票上打印的却是4038277.04元！ 1993年9月，米兰股票交易所的一个计算机输入错误使得当时意大利市场上最好的一只股票价格下跌了12%；市场立刻出现了短暂的动乱。人为因素的破坏主要是指，利用系统本身的脆弱性，滥用特权身份或不合法的使用身份，企图修改或非法复制系统中的数据，从而达到不可告人的目的。

这方面最突出的例子，就是越来越频繁出现的黑客活动。

3. 计算机犯罪

计算机犯罪是指行为人运用所掌握的计算机专业知识，以计算机为工具或以计算机资产为攻击对象，给社会造成严重危害的行为。其中，计算机资产包括硬件、软件、计算机系统中存储、处理或传输的数据及通讯线路。

计算机犯罪所造成的损失非常惊人，通常是常规犯罪的几十倍到几百倍。目前比较普遍的计算机犯罪，归纳起来主要有以下一些类型：一是“黑客非法侵入”，破坏计算机信息系统；二是网上制作、复制、传播和查阅有害信息，如传播计算机病毒、黄色淫秽图像等；三是利用计算机实施金融诈骗、盗窃、贪污、挪用公款；四是非法盗用使用计算机资源，如盗用帐号、窃取国家秘密或企业商业机密等；五是利用互联网进行恐吓、敲诈等其他犯罪。

随着计算机犯罪活动的日益新颖化、隐蔽化，未来还会出现许多其他犯罪形式。大部分的计算机犯罪类型分析起来其实就是传统犯罪类型的“网络版”，这些犯罪其内涵在本质上与传统犯罪并无二致，而计算机犯罪与传统犯罪最主要的差异在于：

（1）隐蔽性。由于计算机系统的开放性、不确定性、虚拟性和超越时空性等特点，使得计算机犯罪具有极高的隐蔽性，增加了计算机犯罪案件的侦破难度。据调查已经发现的利用计算机或计算机犯罪的仅占实施的计算机犯罪或计算机犯罪总数的 5%～10%，而且据统计绝大多数计算机犯罪的暴露都是由于偶然因素导致案发或是犯罪嫌疑人疏忽大意所至。

（2）跨国性。计算机网络的发展使得在世界的每一个角落都可能从网络的任何一个节点进入网络，对联接在网络上的任意一部计算机发动攻击，这种攻击不仅可以跨市、跨省甚至可以跨国、跨洲，在全球都可以发起攻击。这样的犯罪一般刑事侦查手段无能为力，甚至被害人也不知道对方是什么模样在什么地点什么时间对自己下手，这给确定犯罪行为地带来了极大困难。

（3）专业性。计算机犯罪属高科技犯罪，罪犯要掌握相当的计算机技术，需要对计算机技术具备较高专业知识并擅长实用操作技术，才能逃避安全防范系统的监控，掩盖犯罪行为。所以，计算机犯罪的犯罪主体许多是掌握了计算机技术和网络技术的专业人士。他们洞悉网络的缺陷与漏洞，运用丰富的计算机及网络技术，借助四通八达的网络，对网络系统及各种电子数据、资料等信息发动进攻，进行破坏。由于有高技术支撑，网上犯罪作案时间短，手段复杂隐蔽，许多犯罪行为的实施，可在瞬间完成，而且往往不留痕迹，给网上犯罪案件的侦破和审理带来了极大的困难。而且，随着计算机及网络信息安全技术的不断发展，犯罪分子的作案手段日益翻新，甚至一些原为计算机及网络技术和信息安全技术专家的职务人员也铤而走险，其作恶犯科所采用的手段则更趋专业化。

（4）连续性。计算机指令一经输入就会自动运行，同样犯罪嫌疑人一旦将指令或程序输入计算机系统，在一定条件下，它就会自动运行。某些计算机犯罪行为就连行为人也无法制止。

（5）诱惑性强。计算机犯罪作案动机多种多样，但是最近几年，越来越多的计算机犯罪活动集中于获取高额利润和探寻各种秘密。这样，计算机罪犯较容易感受到自我优

越感和成就感，而非罪恶感。所以，计算机犯罪对某些人（特别是青少年）有很强的诱惑性。

（6）社会危害性。首先，计算机犯罪造成的经济损失十分巨大，严重扰乱了正常的经济秩序。其次，计算机犯罪对国家安全和社会秩序也会产生严重威胁。通过计算机各种反动、色情的内容得以迅速、广泛地传播，给人们以不良的刺激，腐蚀人们的思想，诱发多种社会问题。

4．计算机病毒

计算机病毒是由破坏者精心设计和编写的，能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活的具有对计算机资源进行破坏作用的一组程序或指令集合。计算机病毒的破坏行为体现了病毒的杀伤能力。其破坏行为的激烈程度取决于病毒作者的主观愿望和他所具有的技术能量。数以万计、不断发展扩张的病毒，其破坏行为千奇百怪，例如，计算机病毒可以攻击系统数据区、文件和内存，可以攻击磁盘、CMOS，可以扰乱屏幕显示，干扰键盘、打印机的正常工作等，以至于使计算机硬件失灵、软件瘫痪、数据损坏、系统崩溃，造成无法挽回的巨大损失。所以，计算机病毒是计算机系统安全运行的大敌，决不能对其掉以轻心。

可以看出，计算机系统面临着诸多严重的威胁和攻击，这已经成为了计算机系统发展和应用的极大障碍，我们必须深入研究并采取切实有效的措施。

1-1-2　计算机系统的脆弱性

计算机系统之所以面临诸多的威胁和攻击，是由于其本身的抗打击能力和防护能力比较弱，极易受到攻击和伤害。因此，当我们评判一个计算机系统的安全性时，应该尽可能多的了解其脆弱性，以找出有效的措施来保证系统的安全。

计算机系统的脆弱性主要表现在以下几个方面：

1．操作系统安全的脆弱性

操作系统是一切软件运行的基础，也是唯一紧靠硬件的基本软件。作为信息系统最基础、最核心的部分，各种操作系统却又都存在着这样或那样的安全隐患。操作系统的不安全是计算机不安全的根本原因。其脆弱性主要表现在：

（1）操作系统的体系结构造成操作系统本身的不安全。操作系统的程序是可以动态连接的，包括 I/O 设备的驱动程序与系统服务，都可以用打补丁的方式进行动态连接。许多 UNIX 操作系统的版本升级都是采用打补丁的方式进行的。这种方法厂商可以使用，“黑客”也可以使用，而且这种动态连接也是计算机病毒产生的好环境。一个靠渗透与打补丁开发的操作系统是不可能从根本上解决安全问题的。但操作系统支持程序与数据的动态连接与交换又是现代系统集成和系统扩展必备的功能，因此可升级性与安全性是相互矛盾的。

（2）操作系统不仅支持在网络上加载和安装程序，而且支持在网络的节点上进行远程进程的创建与激活，这样就具备了在远端服务器上安装“间谍”软件的条件。如果再

加上把这种间谍软件以打补丁的方式“打”在一个合法的用户上，尤其“打”在一个特权用户上，间谍软件就可以做到系统进程与作业的监视程序都监测不到它的存在。

（3）操作系统通常都提供 daemon 软件，这种软件实质上是一些系统进程，它们总在等待一些条件的出现，一旦有满足要求的条件出现，程序便继续运行下去。这样的软件都是“黑客”可以利用的。而且这种 daemon 在 UNIX 以及 Windows NT 操作系统上具有与操作系统核心层软件同等的权力。

（4）操作系统提供远程调用（RPC）服务，而对于此类服务的安全验证功能却做得非常有限。

（5）操作系统提供 Debug 与 Wizard 使许多研制系统软件的人员有条件从事“黑客”可以从事的所有事情。

（6）操作系统安排的无口令入口是为系统开发人员提供的便捷入口，但它也可能被作为“黑客”的通道。另外，操作系统还有隐蔽信道。

（7）操作系统开发过程中形成的系统漏洞严重地影响到操作系统的安全性。虽然可以通过不断的升级版本来弥补缺陷，但就像木桶原理所说的，只要有 1%的不安全，就等于 100%的不安全。

2. 网络安全的脆弱性

计算机网络尤其是互联网络，由于网络分布的广域性、网络体系结构的开放性、信息资源的共享性和通信信道的共用性，而使计算机网络存在很多严重的脆弱点。它们是网络安全的严重隐患。这些脆弱点主要表现为：

（1）漏洞和后门。由于我们使用的机器设备、计算机软件、网络系统，甚至有些安全产品大都是国外产品，关键技术掌握在别人手里，安全得不到可靠保证。

（2）电磁辐射。电磁辐射在网络中表现出两方面的脆弱性。一方面，电磁辐射物能够破坏网络中传输的数据。另一方面，网络的终端、打印机或其他电子设备在工作时产生的电磁辐射泄露，即使用不太先进的设备，在近处甚至远处都可以将这些数据，包括在终端屏幕上显示的数据接收下来，并且重新恢复。

（3）线路窃听。无源线路窃听通常是一种没有检测的窃听。它通常是为了获取网络中信息内容。有源线路窃听是对信息流进行有目的的变形，能够任意改变信息内容，注入伪造信息，删除和重发原来的信息。也可以用于模仿合法用户，或通过干扰阻止和破坏信息传输。

（4）串音干扰。串音的作用是产生传输噪音，噪音能对网络上传输的信号造成严重的破坏。

（5）硬件故障。硬件故障势必造成软件中断和通信中断，带来重大损害。

（6）软件故障。通信网络软件一般用于建立计算机和网络的连接。程序里包含有大量的管理系统安全的部分，如果这些软件程序受到损害，则该系统就是一个极其不安全的网络系统。

（7）网络规模。网络安全的脆弱性和网络的规模有密切关系。网络规模越大，其安全的脆弱性越大。资源共享与网络安全互为矛盾，网络发展资源共享加强，安全问题越加严重。

（8）通信系统。通信系统始终是最严重的脆弱性的课题。对于一般的通信系统，获得访问权是相对简单的，并且机会总是存在的。一旦信息从生成和存储的设备发送出去，它将成为对方分析研究的内容。

3．数据库安全的脆弱性

由于数据库系统具有共享性、独立性、一致性、完整性和可访问控制性等诸多优点，因而得到了广泛应用，现已成为了计算机系统存储数据的主要形式。与此同时，数据库应用在安全方面的考虑却很少，容易造成存储数据的丢失、泄漏或破坏。具体表现在：

（1）在数据库中一方面存放着大量的数据，这些数据从其重要程度以及保密级别来讲可以分成好几类；另一方面这些数据由许多有着不同职责和权利的用户共享。因此，从安全保密的角度来讲，如何严格限制数据库的用户只是得到一些他们所必需的，与他们权利相适应的数据，是比较困难的。

（2）由于数据库具有数据共享的特性，因此如果一个用户在未经许可的情况下修改了数据，就会对其他用户的工作造成不良的影响。

（3）在数据库中，数据的更新都是在原地进行的，因此新值一产生，旧值就被破坏了，使得在系统或者程序出现故障后，几乎没有冗余的数据来帮助重新恢复原来的数据库。

（4）由于数据库是联机工作的，可以支持多个用户同时进行存取，因此，还必须考虑由此引起的破坏数据库完整性的问题。

（5）数据库管理系统的安全必须与相应操作系统的安全进行配套，即两者应处于同样的计算机安全等级。例如 DBMS 的安全级别是 B2 级，那么操作系统的安全级别也应当是 B2 级。但现实应用中却往往不是这样。

4．防火墙的局限性

防火墙可以根据用户的要求隔断或连通用户的计算机与外界的连接，避免受到恶意的攻击，但防火墙不能保证计算机系统的绝对安全，它也存在许多的局限性。例如：防火墙不能防范绕过防火墙的攻击。防火墙不能防范来自于网络内部的攻击，以及由于口令泄露而受到的攻击。防火墙也不能阻止受病毒感染的软件或文件的传输。

除以上 4 点之外，计算机系统的脆弱性还表现在环境和灾害的影响、电子技术、电磁泄漏等诸多方面。总之，这些脆弱性为攻击型的威胁提供了可乘之机，找到和确认这些脆弱性是至关重要的。

1-1-3　计算机系统安全的重要性

随着人们对计算机信息系统依赖程度的越来越大，应用面的越来越广，计算机系统安全的重要性也越来越突出。

（1）计算机系统安全与我国的经济安全、社会安全和国家安全紧密相连。涉及到个人利益、企业生存、金融风险防范、社会稳定和国家安全诸多方面，是信息化进程中具有重大战略意义的问题。

（2）伴随计算机系统规模的扩大和网络技术的飞速发展，系统中隐含的缺陷和漏洞越来