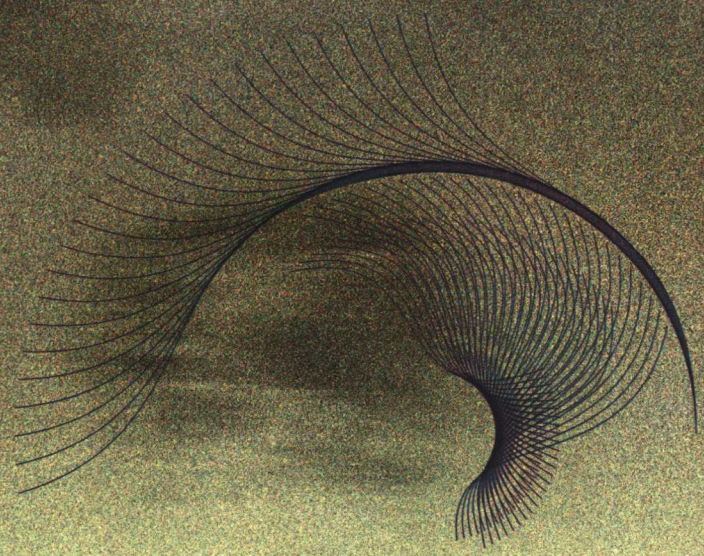
新世纪高等院校精品教材



计算机安全策略

陈天洲　陈 纯　谷小妮　著

浙江大學出版社

新世纪高等院校精品教材

计算机安全策略

陈天洲　陈　纯　谷小妮　著

浙江大學出版社

内容提要

本书从程序员的角度，从较为底层的角度描述了计算机安全问题。兼顾安全理论，分析了计算机安全的各个方面，本书首先简介了计算机安全的概念、标准，然后结合计算机物理硬件介绍了计算机机房、实体安全、用户鉴别、计算机可靠性设计等方面的技术；之后，书中结合安全模型的介绍，阐述了操作系统的访问控制模型、安全操作系统的设计、操作系统漏洞与入侵方法；为了实现软件安全，本书还介绍了软件盗版与反盗版技术中的软件加密、防拷贝技术、反跟踪技术以及对应的攻防技术，并较为详尽地介绍了现有的软件漏洞，主要包括缓冲区溢出与格式化字符串等漏洞，学习这些技术有助于对入侵有更为底层的理解；最后本书介绍了病毒原理以及典型病毒编制方法，病毒防治方法，加解密技术与数据库安全技术。针对现在的网络安全问题越来越突出，本书从物理通讯到网络协议，分析了现代网络硬件、软件、协议中存在的安全问题，提出了防火墙安全模型，阐述了网络扫描、网络监听等技术的实现，结合黑客技术介绍了入侵监测方法。针对电子商务中的安全问题，介绍了CA认证及电子商务中的其他安全技术，以及如何建立有安全保障的计算机系统。

本书在介绍原理之外，还结合一些具体应用系统，并附有源代码例子。

图书在版编目（CIP）数据

计算机安全策略 / 陈天洲，陈纯，谷小妮著. —杭州：浙江大学出版社，2004.5

新世纪高等院校精品教材

ISBN 7-308-03656-1

Ⅰ.计… Ⅱ.①陈…②陈…③谷… 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（2004）第029130号

责任编辑 杜希武 董雯兰

封面设计 俞亚彤

出版发行 浙江大学出版社

（杭州浙大路38号 邮政编码310027）

（E-mail：zupress@mail.hz.zj.cn）

（网址：http://www.zjupress.com）

排　　版 浙江大学出版社电脑排版中心

印　　刷 德清第二印刷厂

开　　本 787mm×1092mm 1/16

印　　张 34.25

字　　数 877千

版 印 次 2004年8月第1版 2006年9月第2次印刷

印　　数 3001—4000

书　　号 ISBN 7-308-03656-1/TP·257

定　　价 48.00元

前言

近年来，随着网络的发展与计算机的普及，信息处理在整个社会中的作用越来越重要，而信息安全在整个信息系统中的作用越来越大。

本书依据作者几年来在电子商务、证券交易系统、浙江省金盾工程、安全加密等方面的工作与研究，结合计算机程序设计技术，从计算机专业人员的角度剖析了计算机安全的各个方面，涉及到计算机安全的物理层、软件层、操作系统、数据库、病毒、通讯、网络、电子商务，并给出了一些程序与系统的例子。

本书在浙江大学计算机学院与软件学院的教学中也得到了4年多的锤炼，通过教学反馈获得了第一手资料，并且在教学过程中不断摸索新型的安全模型与安全机制，经过反复修改实践，最终完成本书的写作。近几届的计算机专业、软件专业的本科生、硕士生都为本书的完成作了不少贡献。

本书整体框架得到浙江大学计算机学院、软件学院副院长何钦铭教授帮助制定。在撰写过程中，得到浙江大学计算机与软件学院朱金英老师、陈丽老师、姚青老师的帮助。同时，还得到胡威、尹彦、戴鸿君、黄颖、楼骥洲、冒海霞、甘泉、赵良乾、王澄、鄢宏杰、贺臻杰等同志帮助修订。

本书适用于从事电子商务、电子政务等方向的科技人员阅读，也是从事计算机网络与因特网、系统集成、系统维护的工作人员必要的参考书。有志于计算机安全方向研究的本科生、硕士生也有必要阅读本书，可以结合汇编、微机原理、程序设计语言、操作系统等知识，从而对计算机安全有更加深入的理解。本书是适合于计算机专业、软件专业的本科、硕士阶段学习计算机安全的参考书、教材，也适合于非计算机类学生深入学习计算机安全的资料。

目 录

第1章

概 论

1.1 计算机安全与社会

近年来，随着计算机在社会各领域的广泛应用，信息安全成为人们关注的重要问题。随着金融信息化、电子政务、电子商务等信息化建设的快速发展，在政治、经济、文化等重要领域信息系统都出现了信息安全问题。信息安全技术可以提高安全保护水平，增强信息安全积极防御与反应能力。

信息安全技术主要研究信息安全核心、关键和共性技术，以形成自主的信息安全防护能力、隐患发现能力、应急反应能力以及信息对抗能力，为建立国家信息安全保障体系提供技术支撑。

信息安全技术的主要目标是通过对信息安全基础、核心和关键技术的研究攻关以及对急需的信息安全产品和系统的研究开发，为我国信息化建设的安全保障体系提供关键核心技术和平台，增强对国家信息基础设施和重点信息资源的安全保障能力，基本满足国家和重要部门的信息安全需求。信息安全促进与信息安全相关的技术标准体系和具有自主知识产权的、具有创新实力的信息安全科研与产业体系的形成，并显著提高我国信息安全的综合保障能力，推动我国信息化建设的健康发展。

由于目前信息的主要载体是计算机，所以信息安全在一定意义上与计算机安全有相通之处。

计算机应用模式，从早期的主机计算，到分布式 C/S 计算，以至现在的互联网计算，其演变过程伴随着计算机软硬件的发展。主机终端方式处在程序设计、结构化程序设计、软件工程时代，以单机计算为主，安全问题未能凸现。随着局域网的推广与计算机的普及，开始出现分布式 C/S 计算模型，以客户端/服务器运行方式在 Intranet 上进行信息处理。由于Intranet具有一定的封闭性，计算机安全问题虽然严重，但是还没有到危害全球的程度。互联网计算带来了信息的大爆炸，各种信息以及信息获取手段应运而生，网格计算、Web/Browser、三层结构、中间件等新技术诞生，同时催化了计算机安全问题的凸现。

安全问题可以分为两类：

1. 硬件。自然灾害，人为破坏，操作失误，硬件故障，电磁干扰，丢失被盗等。

2. 软件。软件数据或资料泄漏，被窃取，黑客病毒攻击等。

计算机的安全是一个越来越引起世界各国关注的重要问题，也是一个十分复杂的课题。随着计算机在人类生活各领域中的广泛应用，计算机病毒也在不断产生和传播，计算机网络被

不断非法入侵，重要信息资料被窃取，甚至由此造成网络系统的瘫痪等，已给各个国家以及众多公司造成巨大的经济损失，甚至危害到国家和地区的安全。因此，计算机系统的安全问题是一个关系到人类生活与生存的大事情，必须给予充分的重视并设法解决。

许多人对计算机安全只具有最粗浅的认识，认为计算机安全问题就只是如何查杀电脑病毒，其实病毒制造者是造成计算机安全问题的根本原因。如今，计算机病毒已渗透到计算机世界的每个角落，病毒的发作给计算机系统造成巨大损失。

现有杀毒软件不足以从根本上解决这些计算机安全的问题。目前，绝大多数的杀毒软件都在扮演"事后诸葛亮"的角色。当电脑被病毒感染后才忙不迭地用杀毒软件去发现、分析、治疗。这种被动防御的消极模式远远不能彻底解决计算机安全的问题。安全软件应该是立足于拒病毒于计算机门外的"健康专家"。频繁升级杀毒软件的结果毫无疑问就是花更多的钱和精力去和病毒"赛跑"，这种无休止的"道高一尺，魔高一丈"的升级大战，意味着原有的杀毒软件技术理念已经走到了尽头。

病毒只是影响计算机安全运行的一个重要因素，远非计算机安全课题的全部。计算机安全课题包括了软件漏洞、加密、防黑客、非法操作、系统物理故障等等多方面的专业技术问题。例如目前使用最为广泛的网络协议 TCP/IP 恰恰存在着安全漏洞，对运行 TCP/IP 的网络系统，存在着五种类型的威胁和攻击：欺骗攻击、否认服务、拒绝服务、数据截取和数据篡改。

2001 年底给全球带来超过 30 亿美元损失的"红色代码"病毒，便是利用微软 IIS 网络服务器软件的一个漏洞进行大肆攻击和破坏的病毒。我国著名的信息安全专家、中国工程院院士沈昌祥指出，软件漏洞是一切信息安全问题的根源。即使没有病毒的攻击，它也可能给计算机带来巨大的隐患和危险。数据库数据信息的误删除，其不可恢复性也能使生产陷入瘫痪状态。系统物理故障更是包括多种多样，虽然有的故障只影响某一个或几个功能，但全局性的故障则会影响到整个计算机，使其丧失全部功能。如简单的时钟故障就能使计算机不能工作，千万不可小视。

对网络安全的进一步认识就要深入理解网络安全产品。网络安全不仅仅是防火墙，也不是防病毒、入侵监测、防火墙、身份认证、加密等产品的简单堆砌，而是包括从系统到应用、从设备到服务的比较完整的、体系性的安全系列产品的有机结合。如果认为只要有了诸如防火墙、漏洞扫描、入侵检测、数据加密等多种软硬件安全产品，安全工作就做到位了，那是大错特错。

网络安全产品的市场主要有三个部分：网络安全硬件、网络安全软件、网络安全服务。

网络安全硬件包括：防火墙和 VPN、独立的 VPN、入侵检测系统、认证令牌、生物识别系统、加密机和芯片。

网络安全软件包括：安全内容管理(防病毒、网络控制和邮件扫描)、防火墙/VPN、入侵检测系统、安全 3A(授权、认证和管理)、加密。

网络安全服务包括：顾问咨询、设计实施、运行管理、紧急响应、教育培训等。

安全产品的投资和使用，只是信息安全工作实施中的一部分。在选择需要什么样的安全产品之前，必须首先为信息系统制定周全的安全策略，并根据安全策略，对安全产品的使用制定具体的管理流程。信息安全工作还应该重视管理。

管理问题包括三个层次的内容：组织建设、制度建设和人员意识。组织建设问题是指有关信息安全管理机构的建设。信息安全的管理包括安全规划、风险管理、应急计划、安全教育培训、安全系统的评估、安全认证等多方面的内容。

一个比较容易出现的看法就是，认为完整的安全产品安装后就万无一失，高枕无忧，忽视

了监控和分析。事实上,在整个信息安全防范体系中,必须强调多种手段的综合使用,其中安全监控和审计是重要的一环。对于信息安全的管理,不能只停留在设备的安装工作方面。正确安装配置产品,只是安全措施实施的第一步。产品的功能和性能使用如何、有无入侵痕迹等问题的核实,需要管理者实时或定期跟踪。这样,管理者才能总体了解信息网络系统当前的安全状况。

网络或应用管理平台、设备内置的管理功能是安全监控和分析的有效工具。其中,对日志记录的跟踪和分析是主要的手段。信息网络系统中存在着针对多种对象的日志记录,如:操作系统日志、数据库日志、应用系统日志、路由器日志、交换机日志、防火墙日志、入侵监测服务器日志、代理服务器日志、邮件服务器日志等等,每一对象的日志又有容量大小、类别、详细程度之分。这些日志记录是你对系统进行监控和分析的好帮手。它们能够显示出系统的详细运行数据,如性能使用参数、出错告警、访问时间、访问方式、访问源及目的地址、故障事件资料、非授权使用记录等等。

利用这些资料,我们很容易分析出系统中存在的某些安全问题或趋势,也为安全事件原因调查提供了具体的依据。每天或每周定期查阅这些日志记录,确实是繁琐和耗时的工作,但也是信息安全管理工作中必须做的工作。

计算机安全是不是仅仅涉及到计算机领域的技术问题?其实它不仅涉及到技术问题,而且涉及了法律政策问题和管理问题。技术问题虽然是最直接的保证信息安全的手段,但离开了法律政策和管理的基础,纵有最先进的技术,信息安全也得不到保障。要使网络安全运行,信息安全传递,还需要依靠法制建设,以法制来强化网络安全。这主要涉及有关网络规划与建设的法律,网络管理与经营的法律,网络安全的法律,用户(自然人或法人)数据的法律保护,电子资金划转的法律认证,计算机犯罪与刑事立法,计算机证据的法律效力等法律问题。同时,还要有法必依,有法必行。所以可以说——法律是网络安全的第一道防线。

仅仅注意了计算机软硬件,而轻视物理场所的安全问题,认为它不会影响大局,这种看法也是非常错误的。对物理场所的安全管理工作的忽视,会给企业信息安全工作产生致命性的打击。在信息系统网络中,分布着众多大小不一、功能不同的机房场所,有数据中心、网络中心、备份中心、数据或网络分中心、网络配线间、高保密等级用户区域等等。各中心内部可能又分为不同的功能区域。对于这些机房或区域的非授权接触,使攻击者更轻易进入关键业务系统或网络,容易造成直接的、严重性的安全事故。例如,切断电源或损坏设备、中止系统服务、进入系统管理控制台、制造系统或网络陷阱、利用网络设备物理缺陷控制和渗透网络、保密资料泄露等等。总之,对物理场所的管理失控,容易使其他方面的安全措施失效。

有多种手段和措施用于加强物理场所的安全管理,包括:制订相应的机房出入管理制度,使用门卫、闭路电视系统、门禁系统等等,来监控人员的进出、对出入人员进行登记;实行机房设备登记制度和严格的设备操作规程;按国家标准做好机房、设备和线路的防电磁辐射泄露;对高密级的计算机网络系统与其他网络部分实行物理隔离;做好物理场所的电源、消防、防雷接地等环境保障工作等等。

因此,相关人员必须认真掌握和实践计算机安全有关的技术和方法。同时,全面加强安全技术的应用,也是网络安全发展的一个重要内容。因为即使有了网络安全的理论基础,没有对网络安全的深刻认识,没有广泛地将它应用于网络中,那么谈再多的网络安全也是无用的。

1.2 计算机安全的基本概念

本节介绍计算机安全的基本概念。本书剩下的部分会详细阐述计算机安全各个方面的内容。

安全机制是用来探测和防止进攻、自我保护的一种机制。对一个系统进行安全分析，需要了解安全机制，该机制用来加强安全策略。这需要一些有关联的假设和信任，了解导致威胁的原因，以及对原因了解的程度。

风险分析就是设计更佳的机制和策略来压制那些威胁。人类社会是在任何系统中安全机制最脆弱的系统，因此，策略和程序必须考虑人的因素。

1.2.1 基本构成

计算机安全要考虑机密性、完整性和可用性。在特定的环境中，它们的含义被个人、习惯和法律所规定。

一、机密性

机密性是信息和资源的隐秘程度。这要求计算机在一些敏感的领域比如商业、军事等领域使用时使信息保密。举个例子，军事和政府机关经常限制信息的获取范围。在计算机安全中最传统的工作是，为了保密而实施访问控制机制。这也应用于那些想保密自己的产品设计不被自己的竞争对手所窃取的企业公司。更进一步，所有的机构都要保守自己的秘密。

存取控制机制支持机密性。存取控制机制用于实现机密性的技术是密码学，密码学把数据弄得杂乱无章从而使得数据不可见。

例如：把财务信息译成密文可以防止其他人阅读它。如果主人想看这些信息，就必须解开密码。只有拥有密码钥匙的人才能把它解密。然而，如果另外有些人进入程序时获取了钥匙，就会影响财务的机密性。

另外，系统依靠访问控制机制可以避免进程不正当的获取信息。不像把数据译成密码，数据受到保护仅允许被访问控制机制所读取。但这些控制可能失败或被迂回，因此，访问控制机制也有较大隐患。它可以比密码学更彻底地保护数据的安全性，但是一旦它失败了，数据就可见了。

信息隐藏也是机密性的一个重要方面。很多站点经常希望隐藏他们的信息，就像隐藏他们使用的系统一样。他们可能不希望其他的人知道他们特定的设备（因为设备可能会不受权限控制被使用，或由不合适的方法使用），也不希望其他人知道自己是从哪里得到的信息。控制机制能提供这方面的功能。

所有用来增强安全性的机制都需要得到系统的服务支持。假定安全服务可以得到内核的响应和由其他机制来提供正确的数据。因此，假设和信任是安全机制的基础。

二、完整性

完整性涉及到数据或资源的确定性，经常被描述成防止对数据进行不合理和无权限的修改。完整性包括数据完整性（信息的内容）和完整性起源（数据的来源，经常叫做验证）。数据的来源可在准确性和可信性上产生动力，来验证是否信任发布信息的人。这种二分法描述了一个众所周知的原则，那就是将完整性的一个方面作为可信性。

完整性机制可以分成两个方面：防止机制和保护机制。

防止机制试图阻止任何无权限修改数据的企图，或任何使用无权限的方法来修改数据的企图，来维持数据的完整性。这两种企图的区分是很重要的。前一种是当一个用户企图改变

数据但是他没有权限去改变。后一种是当一个用户有某种特定的权限来修改数据但是他想用其他的方法来修改数据。举个例子，假设一个机上有一个账户系统，有人想闯入这个系统，试图修改账户数据。这个未授权的用户试图违反账户数据库的完整性。如果账户人员是该公司维护名册的人员，想把资金转移到海外，企图隐藏处理事务从而挪用公款，这个人员就是试图用未授权的方式修改数据库。一个适当的验证和存取控制可以防止从外面的入侵，但是防止第二种企图就比较难以控制。

保护机制不试图防止对完整性的侵害，它只是简单地报告数据安全性已经不可信了。保护机制可以分析系统事件(用户或系统动作)来发现问题，或更多的时候如果需要或者预测到约束，分析数据本身。保护机制可以报告正确的安全性侵犯的原因(一个文件改动的详细清单)或者简单的报告一下文件现在已经不安全了。

完整性工作要比可信性工作要难。在可信性方面，数据要么可信要么不可信。但是在完整性方面需要包括数据的正确性和可信性。数据的起源(怎么样得到，谁得到的)，当数据未到达当前的机器时，数据是怎么进行保护的，数据在当前的机器里是怎么保护的，包含各个方面的数据完整性。因此评价完整性经常很困难，因为这依赖于假设数据的来源和对数据资源的信任，而在这两方面的加强是经常被忽视的。

三、可用性

可用性就是使用信息和得到资源的能力。可用性是可靠性的一个重要方面。就像系统设计一样，一个可用性不好的系统和没有系统的一样。可用性的一个方面对应于安全性，有人故意使系统不可用从而导致拒绝获得数据和提供服务。系统设计通常假设一个标准的模型来分析被预测的使用种类和保证机制。有些人可能通过收集结果(或者控制结果的参数，比如网络通信量)进行分析，因此那些对标准模型的假设将不再安全有用。这意味着用来保持资源或者数据可用性的机制将要面对不在标准模型中的环境，所以这些机制容易失败。

例如：假设张三已经破坏了用来支持银行账目平衡的银行辅助系统服务器，当其他人需要服务器提供信息时，张三可以提供任何他所设计的信息。客户用银行开户的私人账户认证支票。如果一个顾客得不到任何响应，这个辅助服务器就会被要求提供数据。张三阻止客户向基本账目平衡服务器的连接，这样所有的客户询问就去辅助系统服务器。张三不让认证返回，则可以不管实际的账目平衡。

可用性堵塞，又称为拒绝服务攻击，是最不容易发现的，因为分析人员必须确定是否有不正常的读取参数来访问资源或环境。一个使资源不可用的伪装访问可能就像一个非典型性的事件。

1.2.2 威胁

威胁就是潜在的对安全的危害，而危害不一定发生。危害可能发生就意味着那些可能造成危害的行为必须得到防止。这些危害行为被称做攻击。

威胁可以分成四个广义的部分：

1. 泄密，没有授权获得信息；
2. 欺骗，就是接受错误信息；
3. 中断，就是阻止正确的操作；
4. 篡夺，就是不授权地控制系统的一部分。

这四个部分包含很多普通的威胁。那些威胁到处存在，以下罗列几个：

监听(或称窥探)：是没有授权地中途拦截信息，这是被动地，简单实现一些窃听交流或者