Y 全国税务系统岗位专业知识与技能培训系列教材

PRACTICAL KNOWLEDGE AND SKILLS OF TAXATION

国家税务总局教材编写组 编

信息系统安全

人民出版社

责任编辑:李春生
装帧设计:肖　辉

图书在版编目(CIP)数据

信息系统安全/国家税务总局教材编写组编.
-北京:人民出版社,2004.8
(全国税务系统岗位专业知识与技能培训系列教材)
ISBN 7-01-004504-6

Ⅰ.信… Ⅱ.国… Ⅲ.税收管理-管理信息系统-安全技术-技术培训-教材
Ⅳ.①F812.42 ②TP309

中国版本图书馆 CIP 数据核字(2004)第 086467 号

信息系统安全

XINXI XITONG ANQUAN

国家税务总局教材编写组　编

人民出版社　出版发行
(100706　北京朝阳门内大街 166 号)

河北省〇五印刷厂印刷　新华书店经销

2004 年 8 月第 1 版　2004 年 8 月北京第 1 次印刷
开本:787 毫米×960 毫米 1/16　印张:14.75
字数:235 千字　印数:1-5,000 册

ISBN 7-01-004504-6　定价:30.00 元

邮购地址 100706　北京朝阳门内大街 166 号
人民东方图书销售中心　电话 (010)65250042　65289539

序　言

由国家税务总局教育中心组织编写的全国税务系统基础知识、岗位分类和更新知识培训系列教材同大家见面了，我衷心地表示祝贺。这套系列培训教材的出版，为全国税务系统广泛深入地开展教育培训工作，全面提高广大税务干部的素质和能力，促进新时期税收事业的发展都将起到积极的作用。

党的十六大确定了本世纪头二十年我国全面建设小康社会的目标。要实现这一目标，需要各方面的共同努力，税收作为国民经济的重要杠杆之一，更要充分发挥好宏观调控作用。这对我们来说，既是机遇也是挑战。能否抓住机遇，迎接挑战，不负使命，关键在人，在于人的素质，而提高素质主要靠培训。为此，必须加大税务教育培训工作力度，按照全国组织工作会议要求，多层次、多渠道、大规模培训税务干部。通过税务教育培训工作，全面提高税务干部队伍的整体素质，圆满完成各项税收任务，为全面建设小康社会而努力奋斗。

教材是做好教育培训工作的基础，教材建设是教育培训工作中的重要组成部分。为全系统编写和提供高质量的教材，对于帮助广大税务干部提高自身素质和业务能力，加强队伍建设，都具有十分重要的意义。正是从这个意义上说，教材建设要锐意改革，勇于创新，与时俱进。要本着符合税收工作实际需要，符合税务教育培训与学习需要的原则，统一规划，认真组织，在求新、求变、求实上下功夫，多出精品佳作。

这套系列教材从策划、编审到出版，历时近三年，凝聚了税务

系统400多名专家学者和业务骨干的心血。这套系列教材分为基础知识（X）、岗位专业知识与技能（Y）和更新知识（Z）三个部分，形成X+Y+Z的新型教材体系。总的看来，这套教材突破了传统教材的风格、模式和结构体系，实现了启发性与适用性、通俗性与趣味性的统一，组合灵活、简便适用，包含了全国税务系统公务员一般应具备的基本知识、各岗位所必须的专业技能以及新的知识和新的技能，也反映了税收工作的发展水平和改革方向。

希望广大税务干部加强学习，努力工作，不断提高理论素养、业务水平和工作能力，为新世纪的税收事业做出新的更大的贡献！

谈旭人

二〇〇三年四月二十一日

编 审 说 明

根据中共中央、国务院关于加强干部教育培训工作的要求和国家税务总局党组的指示，总局教育中心围绕建设一支政治过硬、业务熟练、作风优良的税务干部队伍的目标，注重培训教材建设，加强新形势下教材建设理论与实践的探索，确立了由基础知识（X）、岗位专业知识与技能（Y）、更新知识（Z）三个部分组成的X＋Y＋Z的新型教材体系。这套教材与税收工作紧密结合，通过大量典型案例和图表解释深奥的理论和复杂的问题，力求启发性与适用性、通俗性与趣味性相统一，是组织培训和干部自学的好帮手。

岗位专业知识与技能（Y）部分培训教材分为政策法规类、征收管理类、稽查类、计划会计统计类、信息管理类和综合类等类别。该部分教材针对税务工作各岗位应具备的专业知识与技能组织编写，突出实务性和可操作性，着重提高广大税务干部分析和解决实际问题的能力。

《信息系统安全》为信息管理类教材。由顾伯群、王惠君负责具体策划指导，李芝麓、田炜、黎干、张千等参加编写，李芝麓、黎干统稿，王秀、谢建全主审。刘书明、夏日红、杨慧平、袁立炫、郭晓辉、冷纪佯、刘建国、午锁平、单玉森、薛海波、钱志平、陈梦林等参加了教材的审定。

本书经国家税务总局教材编审委员会审定通过，同意出版发行。书中如有不妥之处，请读者批评指正。

国家税务总局教材编审委员会

二〇〇四年六月

《信息系统安全》策划编审人员

总策划：许善达

策　划：程永昌　王　秀　陈小杭　王维平　孙　泽
顾伯群

协　助：高永清　杨国全

编　导：顾伯群　刘书明　夏日红　王惠君　郭晓辉

编　写：李芝麓　田　炜　黎　干　张　千

统　稿：李芝麓　黎　干

主　审：王　秀　谢建全

前　言

为了满足全国税务系统信息技术干部队伍教育培训工作的需要，切实提高信息技术岗位工作人员的业务素质，根据全国税务系统岗位专业知识与技能培训系列教材编写的要求，我们编写了Y系列信息管理类培训教材丛书。

丛书包括了《网络》、《硬件》、《中间件》、《工具软件》、《应用系统建设与维护》、《信息系统安全》以及《数据库与数据仓库》七本。编写过程中，我们通过会议、座谈等方式，认真听取了基层同志对丛书编写的意见和建议，并经过多次论证和反复修改，逐步形成了现有体系。Y系列信息管理类培训教材丛书针对税务系统现有网络、硬件设备、操作系统、应用软件、信息安全以及数据库系统建设与维护的工作实际，充分把握“创新、务实、灵活”的原则，改变了传统信息技术教材的编写风格体系，在强调基本理论知识的同时，突出了实例分析、工作程序和工作方法的介绍，具有较强的实用性和可操作性。

丛书由国家税务总局教育中心顾伯群、王惠君，信息中心刘书明、夏日红、郭晓辉具体策划。《网络》分册由江苏省国税局刘建国、靳松、尚峻、葛以品、董文虎、潘正明、王晓培，甘肃省国税局午锁平、董立群、朱晓宁等同志编写；《硬件》分册由湖北省武汉市国税局陈锐、钱钢等同志编写；《中间件》分册由大连国税局冷纪侔、丁琳、曲直、刘福刚、董国承、张汇兵等同志编写；《工具软件》分册由河北省地税局岳轩、李同训等同志编写；《应用系统建设与维护》分册由国家税务总局信息中心杨慧平，深圳市国税局陈梦林、王晓明、翟小英、田仲昊、吴玉梅、蔡敬淳，深圳市地税局薛海波、彭文鸿等同志编写；《信息系统安全》分册由贵州省国税局李

芝麓、田炜，湖南省国税局黎干、张千等同志编写；《数据库与数据仓库》分册由国家税务总局信息中心杨慧平、袁立炫、朱会彦、郭晓辉和湖北省国税局朱峻岭等同志编写。

丛书由国家税务总局信息中心王秀主任主审，国家税务总局信息中心刘书明、夏日红、郭晓辉，扬州税务进修学院陆传基，湖南税务高等专科学校谢建全、田绍槐等同志参与审定。

丛书在编审过程中，得到国家税务总局教育中心和信息中心以及江苏、湖北、湖南、四川、贵州、甘肃省国税局，大连、深圳、武汉市国税局，河北省地税局，深圳市地税局，扬州税务进修学院，湖南税务高等专科学校领导及相关人员的大力支持和帮助，在此一并表示感谢。

由于编写工作量大、时间紧迫，加之全国税务系统信息化建设正处于不断改革和完善之中，本书中疏漏与不妥之处难免，敬请读者批评指正。我们的愿望，是努力打造出一套为税务系统信息技术人员“量身定做”的，切实满足信息技术知识学习需求的精品教材。

编 者

二〇〇四年六月

目　录

1 信息系统安全概述

本章重点讲述的基本内容有：信息系统安全的基本概念、影响信息系统安全的主要因素及其造成、信息系统安全的体系结构、保障信息系统安全的机制及其提供的安全服务。并简要介绍了几种常见的攻击方法、信息系统的安全需求及信息系统建设的安全目标。

1.1 信息系统安全概述

随着信息技术的不断发展，网络与计算机在人们的生活中已经占有了一席之地，为人们的生活带来了很大的方便。然而，高科技也不是尽善尽美的，它在给人们带来惊喜的同时，也带来了威胁。黑客、病毒和后门及计算机犯罪等问题严重地威胁着网络的安全。目前信息安全问题已经引起了各国的普遍关注，成为当今信息技术的一个重要研究课题。

信息系统安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全应用技术、应用数学、数论及信息论等多种学科的综合性学科。

信息系统安全是指信息系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的行为而遭到破坏、更改、泄露，确保系统能连续、可靠、正常地运行，系统服务不中断。从广义上说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是信息系统安全的研究领域。

（1）保密性：信息不泄露给非授权用户。

（2）完整性：数据未经授权不能进行更改的特性。即信息在存储或传输过程中保持不被修改、不被破坏和不丢失的特性。

（3）可用性：可被授权实体访问并按需求使用的特性。即当需要时能够存取所需要的信息。

（4）可控性：对信息的传播范围及内容具有控制能力。

1.2 信息系统安全因素及其影响

任何一个信息系统，都是为了完成一定的管理、生产或企业业务等要求而产生的，必然在操作系统环境中运行有各种各样的应用系统或程序。从这点出发，信息系统的安全因素也就由三个方面组成：应用程序自身的安全、所使用的函数的安全及程序运行环境的安全。

1.2.1 应用程序自身的安全

在汇编程序、C 程序设计中，堆栈、数组的溢出将产生不可预测的后果，这也是被不良分子广泛利用的漏洞之一。例如程序的口令检测将用户输入的若干位口令与设定的口令比较，若输入上千位或上万位同样的数则会造成溢出，使输入的数覆盖设定的口令，则口令检测就如同虚设；C 程序库中提供的 gets（）函数，由于其不检测读入的字符串长度，因此，当读入字串长度超过接受空间的范围时，就会使程序的堆栈溢出。Morris 编写的 Internet 蠕虫病毒便利用了守护进程/etc/fingerd 的漏洞，而 fingerd 就是由于使用了 gets（）函数而产生了该漏洞。

对应用程序的源码分析是判定程序安全与否的重要依据，程序的源代码可通过编辑环境提供的调试功能对程序进行跟踪调试，可从以下几个方面来保障应用程序自身的安全。

（1）检测所有的命令行参数。

（2）检查所有的系统调用参数和返回代码。

（3）检查环境参数，不要依赖环境变量。

（4）确保所有的缓存都被检查过。

（5）在变量的内容被拷贝到本地缓存之前对变量进行边界检查。

（6）如果创建一个新文件，首先应检测文件是否已经存在。

（7）使用还没有发现漏洞的函数调用。

（8）程序开始的时候显式地更改目录到合适的地方。

（9）大量地使用日志记录。

（10）程序的核心尽可能地小。

（11）检查用户的输入，确保只有符合规则的字符。

（12）使用各种检测工具。

（13）在网络服务程序中分散和限制过多的负载。

（14）在网络的读写中设定适当的 Timeout 限制。

（15）防止服务程序运行超过一个以上的拷贝。

（16）不要相信任何 IP 地址，必须进行验证，使用密码算法。

（17）不用明文方式验证信息。

（18）其他。

1.2.2 所使用函数的安全

各类程序中调用 Windows API 和 C Runtime 函数最多，这些函数的安全使用对应用程序的安全性影响最大，应注意一些对安全性有较大影响的函数的具体调用和安全防范。

例如：CreateProcess，CreateProcessAsUser，CreateProcessWithLogonW 函数。

以上函数的第一个参数 lpApplicationName 可以为 NULL。在这种情况下，可执行程序的名称必须是 lpCommandLine 中第一个用空格分割的字符串。但是，如果可执行程序的名称或路径名中有空格，则存在一定的风险，因为如果空格处理不当，就可能会运行恶意的可执行程序。例如：CreateProcess（NULL,"C:/Program Files/foo"），这段代码将运行"Program.exe"而不是"foo.exe"。

1.2.3 程序运行环境的安全

程序设计有时会用到一些系统调用功能，例如 system（）和 popen（）。系统调用有赖于系统本身的设置，如果系统变量 PATH 的设置为当前目录，则像 system（"ls-l"）这样的 C 程序代码就是不安全的。当入侵者在该 C 程序运行的当前目录中放置一个名为 ls 的程序时，则该 C 程序调用的不是系统中提供的 ls 命令，而是当前目录中的 ls 程序，该程序可能是一病毒程序或木马程序，即使 PATH 设置是安全的，但在应用程序中使用了类似 system（）系统调用，也为该程序埋下潜在的安全隐患，黑客可通过修改 PATH 设置，使应用程序变得不安全。在程序设计时对所输入的参数应进行绝对限定，防止意外输入造成程序的非法执行。

由 SUN 公司开发的 Java，是一种真正的、完善的、面向对象的、与平台

无关的解释性语言。Java 代码要求目标机上有 Java 解释器，Java 可以用来生成完全独立的程序。它的与平台无关性，使之成为开发跨平台应用程序的最佳工具。它又具有不支持指针和内存自动管理等安全措施，因而成为并行处理程序、网络程序、智能终端程序的理想开发工具。Java 的这些特性也使其成为编辑网络安全防御程序和攻击程序的利器。尽管 Java 与现有的程序设计语言相比其安全性比较高，但仍存在一些安全隐患，可能造成拒绝服务、系统崩溃和内存溢出等问题。另外有些恶意的 Java 程序作为网页中的元素，可以轻易地穿越防火墙，被下载到客户端执行，而且能冒充内部网应用程序的身份，开放主机禁止的端口，从而在防火墙上打“洞”。

对于这些系统环境的安全防范，应该做到经常升级操作系统，使用经严格测试的正版软件，安装及升级杀毒软件、防黑客软件或其他检测程序进行监测。

1.3 信息系统安全体系结构

关于网络安全体系结构的划分有很多种方式，下面我们介绍一种较有代表性的结构划分。这种方式将信息系统安全划分为系统物理安全、网络安全和信息安全三个层次。

1.3.1 系统物理安全

物理安全是指用一些装置和应用程序来保护计算机硬件和存储介质的安全。物理安全非常重要，它负责保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故，以及人为操作失误、错误和各种计算机犯罪行为所导致的破坏过程。它主要包括三个方面：

（1）环境安全：对系统所在环境的安全保护，如区域保护和灾难保护。参见国家标准 GB50173—93《电子计算机房设计规范》、国标 GB2887—89《计算站场地技术条件》、GB9361—88《计算站场地安全要求》。

（2）设备安全：主要包括设备的防盗、防毁、防电磁辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

（3）媒体安全：包括媒体数据的安全及媒体本身的安全。

正常的安全防范措施有三个方面：

（1）对主机房及重要信息存储、收发部门进行屏蔽处理，即建设一个具有高度屏蔽效能的屏蔽机房，用它来安装运行主要的设备，以防止电磁信号外泄。屏蔽室与外界的各种连接均要采取相应的隔离措施和设计，如网络线、电话、空调、消防控制电路、通风管道、门禁等均要采取相应的防止电磁信号外泄的措施。

（2）对本地网、局域网传输线路传导辐射的抑制。例如可以考虑使用无电磁辐射的光缆传输方式。

（3）对终端设备抑制辐射的措施。终端机，尤其是 CRT 显示器，其辐射具有极强的信号外泄，而终端分散使用就无法采用屏蔽室的方法。目前多数采用主动式干扰（如干扰机）来破坏信息窃取。

1.3.2 网络安全

网络安全主要包括系统（主机、服务器等）安全、网络运行安全。可以采取的安全措施有：

1. 内外网隔离及访问控制技术

在内部网和外部网之间，设置防火墙（包括分组过滤和应用代理）实现内外网的隔离，而访问控制是保护内网安全的最主要、最有效、最经济的措施之一。无论采用何种防火墙产品，从总体上看，它们都应该具有以下的几个基本功能：

（1）过滤进、出网络的数据。

（2）管理进、出网络的访问行为。

（3）封堵某些应禁止的业务。

（4）记录通过防火墙的信息内容和活动。

（5）对网络攻击的监测和警告。

注意：防火墙只是整体安全防范体系的一个重要组成部分，而不是全部。因此必须将防火墙的安全保护融合到系统的整体安全策略中，才能实现真正的安全。

2. 内部网不同网络安全域的隔离和访问控制

在这里，防火墙被用来隔离内部网络的不同网段。这样，就能防止一个网段的问题影响整个网络。针对某些网络，在某些情况下，它的一些局域网的某个网段比另一个网段更受信任，或者某个网段比另一个网段更敏感。而

在它们之间设置防火墙就可以限制局部网络安全问题对全局网络造成的影响。

3. 网络安全检测

网络系统的安全性是整个网络安全中最薄弱的环节。如何及时发现网络系统中最薄弱的环节，如何最大限度地保证网络系统的安全，最有效的方法是定期对网络系统进行安全性分析，及时发现存在的弱点并修正漏洞。

4. 审计与监控

审计是记录用户使用计算机网络系统进行所有活动的过程，它是提高安全性的重要工具。它不仅能够识别谁访问了系统，而且还能指出系统正在被怎样地使用。对于确定网络是否遭受攻击，审计信息对于确定问题和攻击源是很重要的。同时，系统时间的记录能够更迅速和更系统地识别问题，并且它是事后进行事故处理的重要依据。另外，通过对安全事件的不断收集、积累和分析，对其中的某些站点和用户进行审计跟踪，以便对发现或可能产生的破坏性行为提供有力的证据。因此，除使用一般的网络管理软件和系统监控管理系统以外，还应使用目前较为成熟的网络监控设备或实时入侵监测设备，以便对进出各级局域网的常见操作实施检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为。

5. 网络反病毒

在网络环境下，计算机病毒有不可估量的威胁性和破坏力，计算机病毒的防范是网络安全性建设中重要的一环。网络反病毒技术包括预防病毒、检测病毒和消除病毒三种技术。

● 预防病毒技术

它通过预防病毒程序常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有加密可执行程序、引导区保护、系统监控和读写控制等。

● 监测病毒技术

它是利用计算机病毒的特征来进行判断是否有病毒入侵的技术，如利用自身校验、关键字、文件长度的变化，等等。

● 消除病毒技术

它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。网络消除病毒技术的具体实现方法包括对网络服务器中的文件进行频繁的

扫描和检测；在工作站上使用防病毒硬件或软件和对网络目录及文件设置访问权限等。

6. 网络备份系统

备份系统的目的是：尽可能快地全面恢复运行计算机系统所需要的数据系统信息。根据系统安全需求可以选择的备份机制有：系统内高速度、大容量自动数据存储、备份和恢复；系统外的数据存储、备份和恢复；对系统设备的备份。备份不仅在网络系统硬件故障或人为失误时起到保护作用，同时也是系统灾难恢复的前提之一。

在进行备份的过程中，常常使用备份软件，它一般应具有以下功能：

（1）保证备份数据的完整性，并具有对备份介质的管理能力。

（2）支持多种备份方式，可以定时自动备份，还可以设置备份自动启动和停止日期。

（3）支持多种校验手段（如字节校验、CRC 循环校验、快速磁带扫描），以保证备份的正确性。

（4）提供联机数据备份功能。

（5）支持 RAID 容错技术和图像备份功能。

1.3.3 信息安全

Internet 是信息的革命。在方便享用信息的同时，也带来安全方面的问题。由于 Internet 从建立开始就缺乏安全的总体构想和设计，而 TCP/IP 协议也是在可信环境下为网络互连专门设计的，同样缺乏安全措施的考虑，加上黑客的攻击及病毒的干扰，使网络存在很多的不安全因素，如口令猜测、地址欺骗、TCP 盗用、业务否决、对域名系统和基础设施的破坏、利用 Web 破坏数据库、邮件炸弹等等。采取必要的措施和手段，来保护网络与信息的安全是非常必要的。

所谓信息安全就是要保证数据的机密性、完整性、抗否认性和可用性。主要涉及到信息传输的安全、信息存储的安全以及对网络传输信息内容的审计等三个方面。

安全级别有四等级：绝对可信网络安全、完全可信网络安全、可信网络安全、不可信网络安全。

安全的层次有四层：企业级安全、应用级安全、系统级安全、网络级安