注册电子商务工程师(CEBE)认证培训教材

电子商务的安全技术

注册电子商务工程师认证培训教材编委会组织编写

劳帼龄　主编

中国水利水电出版社
www.waterpub.com.cn

注册电子商务工程师（CEBE）认证培训教材

电子商务的安全技术

劳帼龄　主编

中国水利水电出版社

内 容 提 要

本书介绍了电子商务安全防范措施，通过对信息加密技术与应用、数字签名技术与应用、TCP/IP 服务与 WWW 安全、防火墙的构造与选择计算机病毒及其防治、系统评估准则与安全策略以及计算机信息系统安全保护制度的详细介绍，使读者掌握目前先进的电子商务安全技术。

本书可作为注册电子商务工程师（CEBE）认证考试的教材，也可以作为电子商务专业的概论性课程教材，或作为计算机专业、信息管理与信息系统专业有关电子商务课程的教材，还可供一般工程技术人员、工商管理人员和社会大众，系统了解和学习电子商务的有关知识。

本书所配电子教案可以从中国水利水电出版社网站上免费下载，网址为：http://www.waterpub.com.cn/softdown/。

图书在版编目（CIP）数据

电子商务的安全技术 / 劳帼龄主编. —北京：中国水利水电出版社，2005
（注册电子商务工程师（CEBE）认证培训教材）
ISBN 7-5084-3200-2

Ⅰ. 电… Ⅱ. 劳… Ⅲ. 电子商务—安全技术—技术培训—教材
Ⅳ. F713.36

中国版本图书馆 CIP 数据核字（2005）第 093009 号

书　　名	**电子商务的安全技术**
作　　者	劳帼龄　主编
出版　发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京蓝空印刷厂
规　　格	787mm×1092mm　16 开本　19.25 印张　465 千字
版　　次	2005 年 9 月第 1 版　2005 年 9 月第 1 次印刷
印　　数	0001—5000 册
定　　价	30.00 元

编　委　会

序

互联网，催生管理和技术革命的火种；它使管理进步、技术升级频频闪现。互联网，深入经济和社会发展的砥柱；它使经济增长、社会前进蒸蒸勃发。互联网，使复杂变得简单，使枯燥变得生动，使遥远变得贴近；世界随之而变，生活随之而变。

互联网让高科技迅速转化为现实生产力，互联网让商务活动高效转化为电子化的执行程序。电子商务正在成为一切经济活动不可或缺的组成元素，实现着过去难以逾越的服务功能和服务手段，信息传递、资讯交流、市场开拓得以在刹那之间成功完成。

电子商务正在成为助推企业发展的核心力量，转变着以往粗放型经济高成本、低收益的产业格局。电子商务正在成为无可替代的时代风向标，超越国界，超越人的想象空间，改变着物理上的衡量尺度。

电子商务的地位和作用已经难以撼动，前瞻未来，其发展更会随着观念的进步、技术的成长，应用能力的提升而走向更高的顶点。

这是一项没有尽头的事业。

电子商务是一门高度复合的科学。电子商务是本土的，更是国际的；电子商务是技术的，更是管理的；电子商务是理论的，更是实践的。新的时代强烈呼唤着电子商务人才快速崛起，新的时代期待着电子商务人才队伍日益壮大。

2005 年，中国的电子商务终于全面走向国际化和本土化整合的专业化发展道路。在中国商业联合会的支持下，中国将首次全面引进国际商务职业资格认证协会（ICPQA）与国际电子商务工程师协会（ICEBE）共同组织实施的专业技术和应用型培训考试项目——注册电子商务工程师考试（CEBE）。中国电子商务专门人才培养体系将由此而真正诞生。

CEBE 是国际电子商务人才的专业化认证体系，遵循国际化执行程序和标准，并采纳适用的本地化建议而设置的专业考试课程，它的引进将极大地提高我国电子商务人才的专业技能，进一步优化电子商务人才结构，加速中国电子商务人才与国际专业的接轨进程。

CEBE 教材和课程体系涵盖《注册电子商务工程师考核大纲》规定的全部内容。本套丛书包括《电子商务导论》、《电子商务的营销技术》、《电子商务的网络技术》、《电子商务的数据管理技术》、《电子商务的安全技术》、《电子商务的应用开发技术》等六大方面的专门技术，以及《电子商务案例分析》。

《电子商务导论》包括电子商务的基本概念和模型、电子商务技术基础、电子商务网站建设、电子商务环境、电子商务运营方式等内容。《电子商务的营销技术》包括电子商务营销的基本理论、网络市场调研、电子商务营销战略与计划、电子商务营销广告、网络销售、网络销售的评价要求等内容。《电子商务的网络技术》包含计算机网络基础、Internet 技术、数据通信基础、网络安全、电子商务金融网络接入方案和电子商务策划与实施等内容。《电子商务的数据管理技术》包括数据库的基本理论、面向对象的数据库、Web 数据

库基础、数据仓库、数据库技术与电子商务、数据库产品等内容。《电子商务的安全技术》包括电子商务安全的现状与趋势、信息加密技术与应用、数字签名技术与应用、TCP/IP 服务与 WWW 安全、防火墙的构造与选择、计算机病毒及其防治、系统评估准则与安全策略、计算机信息系统安全保护制度等内容。《电子商务的应用开发技术》包括电子商务工程及应用框架、HTTP 与超文本标记语言 HTML、客户端技术、服务器端开发技术、网络安全开发技术、XML 应用开发技术等内容。《电子商务案例分析》包括企业建网方案、数据库管理方案、与金融网络的接入方案、商品营销方案、信息安全方案、物流配送方案等。

CEBE 进入中国，受到了中国众多高校的支持，中国水利水电出版社联合解放军信息工程大学、北京理工大学、对外经济贸易大学、郑州大学、北京交通大学、山东大学、上海财经大学等高校电子商务和计算机网络专家对教材体系和认证体系进行了本地化的拓展和完善，以期为中国电子商务专门人才培养提供有效的本土化和国际化整合的认证通路，为 CEBE 培训和考试提供重要、充分的保障。

本系列教材体系有如下几方面的特点：

1．针对性强。主要根据《注册电子商务工程师考核大纲》为注册电子商务工程师考试而编写。

2．实用性强。丛书以技术为主线，突出实际应用，丛书的作者都是长期从事电子商务技术和计算机网络技术教学、研究和开发的专家，书中许多技术就是他们经验的总结，这对电子商务人才的培养具有重要意义。

3．体系结构合理。针对人们认识问题的规律，强调面向应用，注重应用能力培养，层次清晰。

4．适用广泛。由于是为电子商务技术人才培养而编写的丛书，所以这套丛书也适合各高等院校电子商务和计算机相关专业学生，以及社会在职人员学习和使用。

该教材体系和本套丛书将以统一规划、分批组织、陆续出版为原则。希望各位专家和同行及时对本套丛书给予指正，使其进一步完善，以形成适应中国电子商务发展需要的专业化目标。

中国国际商务职业资格认证管理办公室

2005 年 1 月

前　言

电子商务从20世纪90年代中期诞生以来，已经走过了十年的发展历程。十年来，安全问题始终是影响其发展的一个瓶颈。这在中国互联网络信息中心所作的历次调查和发布的《中国互联网络调查统计报告》中可见一斑，历次调查，安全问题一直是电子商务用户特别关注的主题。可以这么说，电子商务安全是电子商务顺利发展的一个关键，也是一个难点。

电子商务作为一种全新的业务和服务方式，为全球客户提供了丰富的商务信息、简捷的交易过程和低廉的交易成本。但是电子商务在给人们带来方便的同时，也把人们引进了安全陷阱。电子商务是利用计算机通过网络来实现的。有关计算机的安全问题早已引起人们的担忧，对于大部分使用过计算机的人可能都遇到过计算机病毒的侵扰，它可能会令你辛苦一天的文档不翼而飞，或者使你的主机系统莫名其妙的崩溃、死机。而对于网络安全问题，目前来自黑客的攻击已越来越多，有关企业网站被黑的新闻时有所闻。

大量的事实说明，要保证电子商务的正常运作，就必须高度重视安全问题。电子商务的安全涉及社会的方方面面，不是一堵防火墙或一个电子签名就能简单解决的问题。安全问题是电子商务成功与否的关键所在，也是致命所在。因为电子商务的安全问题不仅关系到个人的资金安全、商家的货物安全，还关系到国家的经济安全、国家经济秩序的稳定问题。大量事实证明，要保证电子商务的正常运作，就必须高度重视安全问题，就必须关注电子商务的安全技术。电子商务安全的相关技术既涉及信息加密解密、网络安全协议、防火墙的构建、病毒的防治，也包括相关管理制度的建立。这是一个涉及范围相当广的问题，需要各方的协调配合。

本书共由8章组成。第1章介绍了电子商务安全的现状和趋势，第2章介绍了信息加密技术与应用，第3章介绍了数字签名技术与应用，第4章介绍了TCP/IP服务于WWW安全、第5章介绍了防火墙的构造与选择，第6章介绍了计算机病毒及其防治，第7章介绍了系统评估准则与安全策略，第8章介绍了计算机信息系统安全保护制度。

本书由劳帼龄主编。参加本书资料收集和编写的还有汤瑛、熊宽、虞佳、徐文琴、钟艳萍，最后由劳帼龄负责全书的统稿。

本书在编写过程中，大量参考和借鉴了国内外有关电子商务安全技术的著作、教材、文章和网站资料，吸收了前人的研究成果，在此一并表示感谢。此外，尽管在本书的编写工作中，作者努力想把与电子商务安全相关的最新知识介绍给读者，但由于作者水平所限，加上电子商务本身发展迅速，书中疏漏之处在所难免，敬请广大读者批评指正。谢谢！

编者

2005年8月

目　　录

第 1 章　电子商务安全的现状和趋势

电子商务从 20 世纪 90 年代中期诞生，到现在已经走过了 10 个春秋。十年来，安全问题始终是影响电子商务发展的一个瓶颈。用户担心网上购物的信用卡及个人资料被盗；或者是交易抵赖；又或者是一旦信用卡账号刚输完，网络受到了攻击，那账户现金该会何去何从等等。因此，电子商务安全是电子商务顺利开展的一个关键，也是一个难点。电子商务的安全问题不仅关系到个人的资金安全、商家的货物安全，还关系到国家的经济安全，关系到国家经济秩序的稳定。我们无法想象一个安全得不到保障的电子商务世界会是一个什么样的情形。所以，对于电子商务的安全问题决不可以等闲视之，必须把它提到重要的议事日程上来，只有这样，才能保证电子商务的健康发展。

大量的事实说明，要保证电子商务的正常运作，就必须高度重视安全问题，就必须关注电子商务的安全技术。电子商务安全的相关技术涉及到方方面面，不仅仅涉及到信息加解密、网络安全协议、防火墙的构建、病毒的防治，也包括相关管理制度的建立。关于电子商务安全技术的更多详细内容将在后续各章节一一介绍。

本章首先提出电子商务的安全问题，重点分析它产生的原因，随后介绍电子商务安全的概念及构成，提出电子商务的安全需求，并针对各项安全需求叙述世界各国的电子商务安全现状，最后介绍安全的防治措施，以及今后的安全举措。

1.1　电子商务安全问题

在电子商务整个运作过程中，会面临各种安全问题。典型的安全问题包括：安全漏洞、病毒感染、黑客攻击、网络仿冒以及来自其他方面的各种不可预测的风险。分析电子商务的安全问题，就要依据实际考察结果，确定各种可能出现的安全问题，分析其不同程度的危害性，找出电子商务中潜在的安全隐患和安全漏洞，从而有的放矢的运用相关电子商务安全的技术来加以控制和管理。

1.1.1　安全漏洞

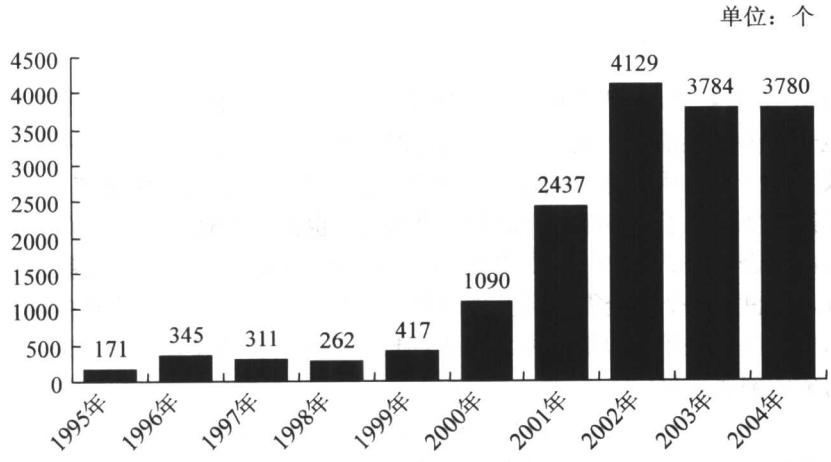
根据国际权威应急组织 CERT/CC 统计，2004 年公布漏洞数 3780 个，平均每天超过 10 个。从图 1.1 中可以很清楚地看出，在近几年来，计算机系统的漏洞越来越多。而且值得注意的是，图中数量是保守估计，实际的漏洞数量将更多。漏洞的大量存在，使得目前电子商务的安全形势趋于严峻。

2004 年比较典型的安全漏洞主要有：

（1）Windows 惊现高危漏洞，新图片病毒能攻击所有用户。该漏洞可能发生在所有的 Windows 操作系统上，如 IE 浏览器、Office 软件等，在用户浏览特定的 JPG 格式图片时，会导致缓冲区溢出，进而执行病毒攻击代码，包括格式化硬盘、删除文件等。

（2）WinXP SP2 发现迄今最严重的安全漏洞。当用户将一个文件或一幅图像从网页上复

制下来时，IE 里的 ActiveX exploit 就会运行，它会向用户的计算机上下载能够绕过 SP2 中“本地计算机”安全设置的代码。该缺陷被丹麦安全专家定为“高度危急”的危险级别。



数据来源：CNCERT/CC2004 年网络安全工作报告

图 1.1　1995 到 2004 年漏洞公布数量

（3）采用 SP2 的系统发现 10 个严重安全漏洞。

（4）苹果的漏洞补丁程序不起作用。一个恶意的网页可以利用苹果 MacOS 操作系统中存在的两个漏洞向用户的 Mac 电脑发送代码，在 MacOS 的默认设置下，Safari 和 IE 浏览器都会自动下载和执行攻击者的代码，使攻击者轻易达到攻击的目的。

（5）Solaris 现存致命漏洞，补丁迟迟不发布。利用 Solaris 操作系统的该漏洞，只要用户打开被做过手脚的 xpm 格式图片，黑客就可以取得远程执行任意代码的权限。

（6）IE 惊现最新地址欺骗漏洞。利用该漏洞，黑客可以在网页中制作一个特殊的超级链接，当用户在 IE 中浏览网页，用鼠标指向该链接时，状态栏中显示的 URL 可以是由黑客指定的任意地址，但当用户点击链接后，却可以被连接到恶意网站上。这为网页仿冒提供了高度的便利性。

（7）IE 和 Mozilla 等浏览器发现 cookie 漏洞。正常的情况下，网络浏览器只有在访问发送 cookie 的服务器（也称域）时才会发送该 cookie,如由www.china-pub.com所发送的 cookie 只有在访问该网站时才会被发送回其服务器。但是，IE 和 Mozilla 等浏览器有时会将某个域发送的 cookie 发送给其他域，如将正规网站www.china-pub.com 的 cookie 发送给恶意网站，导致个人资料的泄露。

（8）Mozilla 旗下浏览器 Firefox 和电子邮件客户端出现三个安全漏洞。在 Mozilla 庆祝 Firefox 的商业使用者超过了浏览器市场的 10%的同时，Mozilla 和 Firefox 都被发现存在漏洞。利用这些漏洞，黑客可以在用户电脑上安装恶意代码，或者是窃取用户下载对话框中显示的原始信息并可伪造下载对话框中的 URL。

（9）黑客可以利用 PHP“危急”漏洞控制 Web 服务器。

（10）Java 插件安全漏洞可能致使 Windows 和 Linux 受攻击。Java 的一个小插件能够让小型网络程序在用户的计算机上安全运行，但它允许恶意网站绕过安全措施通过浏览器在用户计

算机上运行恶意程序，它能够让病毒通过 Windows 和 Linux 进行传播。我们知道，Windows 和 Linux 占据了操作系统市场的半壁江山，如果黑客抓住该漏洞不放，那病毒的影响力将是巨大的。

（11）Real 系列播放器发现危险级漏洞。如果用户读取做过手脚的皮肤文件，系统有可能执行任意程序，无法自控。

1.1.2　病毒感染

我国计算机病毒感染率自 2001 年以来就一直处于较高的水平。2004 年，蠕虫等病毒在网上传播仍十分的猖獗，计算机感染率从 2001 年的 73%跃到了 2004 年的 87.93%。蠕虫主要是利用系统的漏洞进行自动传播复制，由于传播过程中产生巨大的扫描或其他攻击流量，从而使网络流量急剧上升，造成网络访问速度变慢甚至瘫痪，这对依赖于网络的电子商务是一个严重的威胁。

2004 年没有爆发对整个网络运行安全造成重大影响的蠕虫等病毒事件，而主要是造成大量用户无法正常使用。尽管如此，蠕虫等病毒传播对局部网络造成的影响还是不容乐观的。2004 年以来蠕虫出现了一些新特点。蠕虫被黑客用来驱动预定的拒绝服务攻击，如冲击波（2003 年）、Mydoom 蠕虫等，如果这种方法被应用于对互联网上的关键节点服务器、路由器进行拒绝服务攻击，将会导致整个互联网业务的瘫痪，且在理论上，并没有有效的方法来应对该类攻击。蠕虫也逐渐被用来植入木马程序和后门软件，如震荡波系列蠕虫等，给感染蠕虫的用户带来严重的泄密威胁，同时也造成大量潜在的可受黑客控制的主机。一旦某个黑客或黑客组织集中控制了这些主机，将给各种网络应用系统带来不堪设想的严重威胁。

1.1.3　黑客攻击

1. 网页篡改

从 2001 年日本首相小泉纯一郎参拜靖国神社以来，该神社的网页就断断续续遭到黑客的攻击，有时在一分钟内就遭到 90 万次围攻。2004 年一年由于黑客攻击，神社网页瘫痪了 5 次。2004 年 10 月末，黑客入侵负责托管巴西所有政府网站的互联网服务供应商，在 200 多个巴西政府网站上留下了反政府言论。

2004 年 10 月 28 日，索尼中国的网页被篡改，加入了辱骂美国总统布什的字语，并对其发动的伊拉克战争进行了抨击。2004 年 12 月 25 日和 27 日麦当劳中文官方网站三次被黑客篡改，或是将主页颜色更改，添加抗议麦当劳分裂中国与中国台湾省的标语，或是用简单的页面替换掉麦当劳主页。接下来的 29 日，耐克中文网站也被黑客篡改，见图 1.2。2005 年 4 月 15 日，新力（SONY）在中国北京的当地法人索尼（中国）有限公司的网页一度遭人篡改，服务器短时间内陷入瘫痪状态。面对频繁的网页篡改事件，黑客们表示，他们并非为中国而来，只是想告诉全世界，“You don’t have security”。从图 1.3 的网页篡改情况统计可以看出，网页篡改事件频繁发生，平均每天发生 6 起。

2. 僵尸网络

僵尸网络也称为 BotNet。Bot 是 robot 的简写，通常是指可以自动地执行预定义的功能，可以被预定义的命令控制，具有一定人工智能的程序。它可以通过溢出漏洞攻击、蠕虫邮件、网络共享、口令猜测、P2P 软件等途径进入用户主机。一旦用户主机被植入 Bot，就主动和互联网上的一台或多台控制节点取得联系，进而自动接收黑客通过这些控制节点发送的控制命令，这些受害主机和控制服务器就组成了 BotNet。