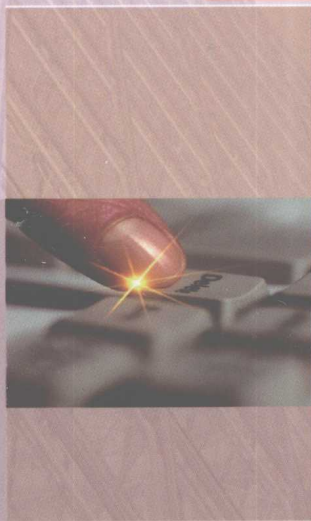




高等院校电子商务专业系列规划教材

电子商务 安全与网上支付



E-Business

Security and Online Payment

刘英卓◎编著



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>



高等院校电子商务专业系列规划教材

电子商务

安全与网上支付

E-Business
Security and Online Payment

刘英卓◎编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有，侵权必究。

图书在版编目（CIP）数据

电子商务安全与网上支付 / 刘英卓编著. —北京：电子工业出版社，2010.7

（高等院校电子商务专业系列规划教材）

ISBN 978-7-121-11233-1

I. ①电… II. ①刘… III. ①电子商务—安全技术—高等学校—教材 ②因特网—应用—银行业务—高等学校—教材 IV. ①F713.36 ②F830.49

中国版本图书馆 CIP 数据核字（2010）第 125214 号

责任编辑：王慧丽 特约编辑：宋兆武

印刷：北京市天竺颖华印刷厂

装订：三河市鑫金马印装有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开本：787×980 1/16 印张：20.25 字数：433 千字

印次：2010 年 7 月第 1 次印刷

定价：35.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zltts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前 言

电子商务的迅猛发展打破了以往企业与企业间、企业与客户间、时间与空间的界限，创造了一个全球性的、没有时间和空间距离的另一个维度的空间。它的出现和发展改变了原有企业的格局、原有的价值体系、原有的经营模式，甚至改变了企业的形式，与此同时，也导致市场对这方面人才的迫切需求。

电子商务是基于计算机因特网的交易行为，网络必须保证大量的经济信息能够安全地传送，资金能够安全地划拨。但是，由于因特网是一个开放系统，网络上传送的信息的完整性可能被破坏，机密可能被窥知，交易的一方可能事后反悔，造成电子合同丧失效力，经济秩序发生紊乱。因此，我们必须学习如何保障电子商务的安全。

本书面向高等院校中的电子商务本科学生；也可供 MBA 学生、经济管理类专业硕士生及本科高年级学生选用；还可为相关人员、相应层次的电子商务安全人员培训时选用。

学生基础分析情况：电子商务本科学生，他们掌握一定的基础知识，学习过计算机网络基础、数据库基本知识等，但是他们对电子商务安全没有完整的概念。对于其他专业学生，他们具有 vfp 的计算机二级基础。因此，在教材编写中兼顾了多方面的考虑。本教材的特点有：一定的基础知识的导引，一定的故事趣味性，一定的知识深度，一定的应用实例；语言简洁明了，知识点突出，层次分明；注意区分学生已经在电子商务概论课程中学习过的知识。

通过本书的学习，使学生能够全面了解计算机信息安全技术的基础理论，初步掌握计算机信息安全防范的基本方法，加强对计算机安全重要性的理解，掌握实现和管理 Windows 2000 网络环境的知识和技能，具备进行故障排除的能力。为学生今后进行进一步学习、研究信息安全技术打下坚实的基础。

本书由刘英卓编写，主要作为高等院校电子商务专业的教材，也可以作为电子商务培训教材和参考书。书中引入了许多实际案例，帮助读者更好地理解内容。本书尽量在广博性的基础上增加可读性，但还是有许多东西限于篇幅舍弃了。本书尽量保留了作者认为重要的、有实用价值的或者有趣的内容，注意了和同类教材内容上的区分。在教材编写过程中，参考了国内外有关的最新著作和资料，南京财经大学电子商务实验室的相关老师也提出了宝贵的建议，刘军老师提供了非常有价值的资料，在此表示衷心的感谢！由于作者的

水平和教学经验有限，书中难免有不足之处，希望广大读者批评指正。

教学建议如下表。

	知识点	课时安排	重点讲述内容	选讲内容
第 1 章	电子商务安全的基本知识，客户机的安全，服务器的安全，安全的目标，安全的威胁等	4 课时	客户机的安全设置；服务器的安全原理和设置	安全评估标准
第 2 章	加密和解密基本知识，DES 算法原理，AES 算法，RSA 算法	6 课时	DES 算法、RSA 算法	AES 算法
第 3 章	TCP/IP 基本知识，IPSec 协议、SSL 协议和 SET 协议	8 课时	TCP/IP 基本知识，IPSec 原理，SSL 协议，SET 协议	IPv6, VLAN
第 4 章	防火墙和 VPN 基本知识	8 课时	防火墙基本原理、VPN 原理	GRE VPN 和 MPLS VPN
第 5 章	鉴别和认证基本知识	6 课时	鉴别和认证基本原理，PKI 和 CA	域与活动目录
第 6 章	安全策略和安全实践	3 课时	安全策略和安全实践注意事项	电子商务安全案例
第 7 章	网上支付概论	10 课时	支付与结算基础，电子货币和网上银行	CNFN 和手机银行
第 8 章	安全的网上支付	3 课时	在线支付功能的安全实现	中国金融认证

本建议表是按照一学期 18 周、每周 3 课时来设计的，仅供教师使用时做参考，具体讲解内容可根据实际情况进行适当取舍。每一本书都在面临着内容的老化，即使是最新的书也是难免的。所以，我们的广大教学者和学习者在使用本书时，应该及时更新本书中已经过时的数据，对本书中的不当之处提出指正。

作者

目 录

第 1 章 电子商务安全概述	1	习题	98
1.1 客户机的安全	2	实验（一） 网络嗅探器 Sniffer	99
1.2 服务器的安全	4	实验（二） PGP 操作	102
1.3 电子商务安全问题	10	第 4 章 防火墙与 VPN	108
1.4 系统安全评测标准	12	4.1 防火墙	108
习题	15	4.2 VPN	133
实验（一） PC 的安全配置	15	习题	150
实验（二） 常用网络命令实践	16	实验（一） 配置防火墙	150
第 2 章 加密与解密	18	实验（二） VPN 的配置	157
2.1 加密与解密基本知识	19	第 5 章 认证与管理	161
2.2 对称加密学	23	5.1 报文鉴别与身份认证	161
2.3 非对称加密学	38	5.2 证书与 CA	184
习题	44	5.3 PKI	195
实验（一） DES 加密	44	5.4 域和活动目录	207
实验（二） RSA 加密	45	习题	232
实验（三） 加密软件的使用	45	实验（一） 练习签名	232
第 3 章 安全网络协议	46	实验（二） 配置活动目录	233
3.1 TCP/IP 基本知识	46	第 6 章 安全电子商务应用	237
3.2 IPSec	64	6.1 电子商务安全体系结构	237
3.3 PGP	74	6.2 电子商务安全解决方案	242
3.4 SSL	80	习题	254
3.5 SET	86	实验 证书颁发系统实践	254
3.6 无线网安全	96		

第 7 章 网上支付概论	256	第 8 章 安全的网上支付	301
7.1 支付与结算基础	256	8.1 现代化安全支付系统概述	302
7.2 电子货币	262	8.2 安全网上支付系统的实现	305
7.3 网上银行	280	习题	313
习题	299	实验 网上支付的编程实现	314
实验 网上支付实验	299	参考文献	315

第 1 章

电子商务安全概述



引导案例

据新华网北京 2008 年 4 月 20 日专电, 一个名为“VB 木马点击器变种 ZXY (Trojan. Clicker. Win32. VB. zxy)”的病毒能够伪装成 IE 浏览器图标, 欺骗用户点击运行, 在后台疯狂点击黑客指定的网址, 同时病毒会释放数十个盗号木马、病毒等, 给用户带来很大的安全风险。“VB 木马点击器变种 ZXY”是一个用 VB 语言编写的木马点击器, 它会伪装成 IE 网页图标, 欺骗用户点击运行。通过配置程序修改网页地址, 并在后台点击指定的网址, 这些网址大部分是广告和商业网站, 黑客借此来获取大量利润。由于病毒会在系统 System32 目录下释放多个不同的病毒程序, 会给手动清除带来一定难度。对此, 专家建议用户: ① 养成良好上网习惯, 不打开不良网站, 不随意下载安装可疑插件; ② 开启 Windows 安全中心、防火墙和自动更新, 及时安装最新系统补丁, 避免病毒通过系统漏洞入侵计算机; ③ 将杀毒软件升级到最新版本, 定时杀毒并开启实时监控功能, 防止病毒感染计算机; ④ 定时设置系统还原点和备份重要文件, 并把网银、网游、QQ 等重要软件加入“账号保险柜”中, 这样就可以防止病毒窃取游戏账号、密码等私人资料。

◇ 本章学习目标 ◇

1. 了解和掌握造成客户机和服务器安全问题的原因;
2. 掌握如何保护 PC 的安全;
3. 掌握电子商务的安全目标;
4. 学会如何配置安全的 Web 服务器。

在因特网上发展电子商务, 无论是 B2B 模式还是 B2C 模式, 首要关注的问题都是电子商务的安全性, 人们对隐私、产权和钱财等问题是否得到安全保障的担心制约了电子商务的发展。由于电子商务主要是利用网络来进行商务业务往来的处理和管理的, 所以按照实施电子商务的对象可以划分为 3 个部分: 客户机的安全、通信信道的安全和服务器的安

全。按照技术和应用的区别, 又可以将电子商务的安全分为电子商务网络安全和电子商务交易安全。

1.1 客户机的安全

客户机是指一台连接远程服务器的本地机, 通常就是个人计算机 (PC), 也是 B/S 结构中的浏览器那一端。其安全性可划分为两段: 客户机上网前的安全和客户机上网面临的安全。对于客户机上网前的安全, 主要是其硬件、软件的安全问题, 比如, 计算机的各种插卡有没有问题, 是否做到了功能统一、相互匹配, 以及对意外事件的抵御能力等; 软件的安全, 比如, 操作系统是否及时更新了漏洞, 各种应用软件有没有被入侵的风险等。这种客户机上网前的安全性是电子商务安全的前提, 要求必须首先实现 PC 的安全。客户机上网面临的安全, 是指客户机和服务器进行信息往来传送时面临的被攻击问题, 这是电子商务安全的主要关注点。

客户机上网面临的安全性问题主要来源于页面的活动内容。活动内容是指在页面上嵌入的对用户透明的程序。活动页面可显示动态图像、下载和播放音乐或利用插件来执行相关功能模块, 使页面功能更为丰富、形式更为活泼。活动内容形式包括 Java 小应用程序、Active X 控件、浏览器插件、JavaScript、VBScript、活动脚本和包含一些隐含嵌入指令的文件等。小应用程序是可以在另一个程序中执行的程序, 但它不能在计算机上直接执行。Java 小应用程序只要求客户的浏览器兼容 Java, 它就可以在客户机上运行。Java 利用 Java 运行程序安全区来限制 Java 小应用程序的活动, Java 运行程序安全区是根据安全模式所定义的规则来建立的, 这些规则适用于所有不可信的 Java 小应用程序。可信的 Java 小应用程序或者是从本地文件系统中下载的, 或者是带有可信第三方的数字签名。插件是用于解释或执行嵌入下载图形、声音或其他对象中的指令。JavaScript 和 VBScript 都支持页面设计者创建在浏览器端可执行的活动内容, 但这种程序或页面要经过客户的手动启动。Active X 是一个对象 (称做控件), 它由页面设计者放在页面里来执行特定任务的程序, 只能运行在微软的 Windows 操作系统上, 并要求浏览器支持 Active X 控件。浏览器下载到嵌有 Active X 控件的页面时, 会提醒你是否安装执行。Active X 控件一旦执行, 就能访问所有的系统资源。所有形式的活动页面都支持 WWW 页面完成一些特定的任务。例如, 网页的表单 (form) 或表格 (table) 上的按钮可激活嵌入的程序来计算和显示信息, 或将客户机上的数据发给服务器。

Java Applet 的下载执行过程, 如图 1.1 所示。

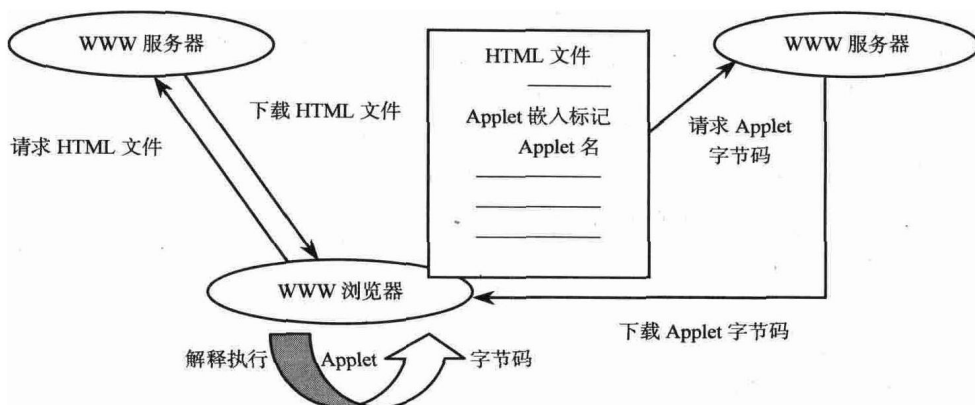


图 1.1 Java Applet 的下载执行过程

ASP 文件的处理，如图 1.2 所示。

如果活动内容是特洛伊木马、网络蠕虫、病毒等，就将为电子商务带来多种安全风险。HTTP 协议是无状态的，即它不能记忆从一个页面到另一个页面间的响应，所以它要借助于一种叫做 Cookie 的技术来解决需要记忆关于客户订单信息或用户名与口令等问题。Cookie 是用户在访问某些站点时，其 Web 服务器在用户计算机中所写入的一些文件。这些小文件可能记录了关于用户的个人信息，比如，何时访问该网站，在网站从事过哪些活动等，当用户再次访问该网站时，Web 服务器只要查询 Cookie 的记录就会记得是谁。有恶意的活动内容会利用 Cookie 将客户机的文件泄密。

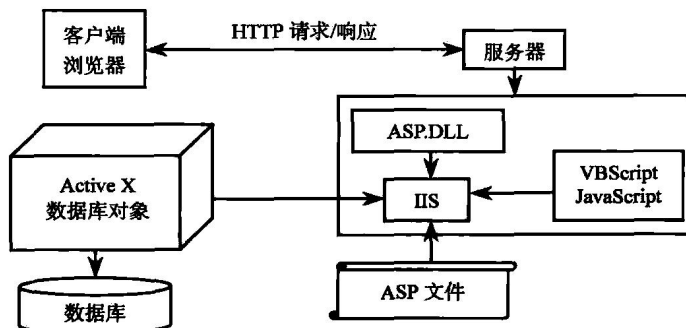


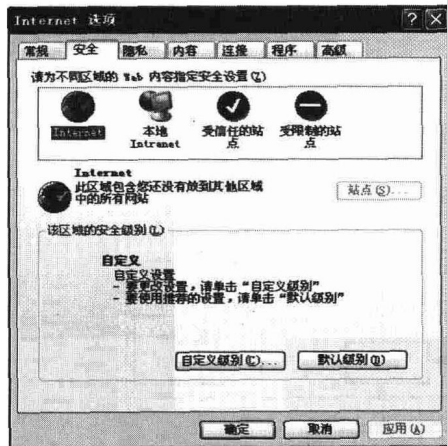
图 1.2 ASP 文件的处理

除了活动内容，那些被用户有意下载的文件、软件、电子邮件的附件等都有可能带来安全隐患，这些下载后的文件中都有可能包含病毒、木马等。对每一台计算机来说，两个

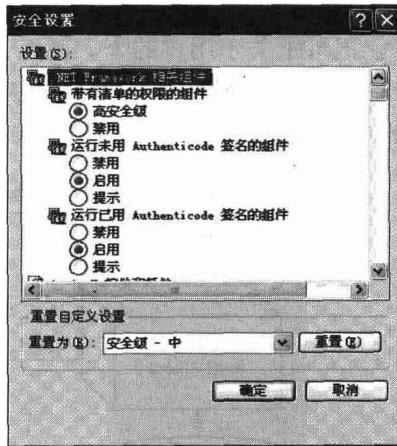
最大的威胁是病毒和蠕虫，其实它们就是计算机程序，有些人出于好玩或好奇而编写这些程序，有些人则把它作为一项挑战，要编出最具毁灭性的病毒或蠕虫。虽然有些病毒和蠕虫完全无害，但大多数的病毒和蠕虫会带来各式各样的麻烦，从在屏幕上显示无意义的信息，到让键盘工作反常，以致删除文件，甚至整个硬盘发生紊乱。

如何保护上网的客户机呢？第一，对活动页面的活动内容要有所限制，设置好用户的浏览器安全选项，如图 1.3 所示。微软的 IE 浏览器采用 Authenticode 技术来验证所下载活动内容的身份。Authenticode 取下活动页面的证书（或签名块），验证认证中心的身份，验证这段内容是否来自发布者并确认此程序在此之后未被修改过。Authenticode 扫描 IE 内置的可信认证中心的清单及其公开密钥，找到提供证书的认证中心。如果清单上的公开密钥和证书上的相符，就可认为认证中心的身份是真实的。但是 Authenticode 没有对运行状态代码的监测功能。第二，对活动内容喜欢访问的 Cookie，用户要加以控制。第三，对用户有意下载的文件、软件和电子邮件的附件等，要进行签名消息或签名代码的检查，同时用防病毒软件查杀病毒。

因特网是电子商务的通信信道，如何让这个信道变得安全，进行安全传输？主要包括保证因特网信道通信保密性、消息完整性和渠道可用性，因特网信道的安全性要靠各种网络协议来保障。



(a) Internet 安全选项



(b) 安全设置

图 1.3 IE 浏览器的 Internet 安全选项和安全设置

1.2 服务器的安全

服务器是客户机的信息资源不对等实体，它对外提供资源的共享和访问。对于电子商

务的实施,建立安全的电子商务服务器系统是至关重要的。要防止服务器被破坏和非法获取信息,重点要考察其入口。服务器的入口包括 WWW 服务器及其软件、公共网关接口 (CGI) 程序、asp、jsp、pl、php 等其他工具程序,以及任何有数据的后台程序,如数据库和数据库服务器。

1.2.1 服务器的安全威胁

1. 对 WWW 服务器的安全威胁

WWW 服务器软件涉及的主要目标是支持 WWW 服务和方便使用,即响应 HTTP 请求进行页面传输。其面临的安全威胁主要有:

① WWW 服务器如果以高权限状态运行,就构成对 WWW 服务器的安全威胁,破坏者就可利用 WWW 服务器的能力执行高权限的指令。

② WWW 服务器如果不更改目录显示的默认设置,它的保密性就会大打折扣。如果一个服务器的文件夹名能让浏览器看到,就会破坏保密性。

③ WWW 服务器要求输入的用户名和口令可能被泄露, Cookie 信息有可能被窃听者复制。

④ 嵌入由服务器执行的页面上的小程序会造成服务器的不安全,比如,黑客入侵网站使用的“小马”和“大马”。

⑤ FTP 程序会对 WWW 服务器的完整性带来安全威胁。如果对 FTP 用户可浏览的文件夹没有进行保护,就可能发生未经授权的信息泄露。

⑥ 存放用户名和口令的文件可能没有得到保护。

⑦ 用户所选的口令也会构成安全威胁。

Microsoft Active Server Pages (ASP) 是服务器端脚本编写环境,使用它可以创建和运行动态的、交互的 Web 服务器应用程序。使用 ASP 可以组合 HTML 页、脚本命令和 Active X 组件以创建交互的 Web 页和基于 Web 的功能强大的应用程序。现在很多网站,特别是电子商务方面的网站,在前台上大多用 ASP 来实现,以至于目前 ASP 在网站上的应用很普遍。

ASP 脚本是一系列按特定语法(目前支持 VBScript 和 JavaScript 两种脚本语言)编写的与标准 HTML 页面混合在一起的脚本所构成的文本格式的文件。当客户端的最终用户用 Web 浏览器通过 Internet 来访问基于 ASP 脚本的应用时,Web 浏览器将向 Web 服务器发出 HTTP 请求。Web 服务器分析、判断出该请求是 ASP 脚本的应用后,自动通过 ISAPI 接口调用 ASP 脚本的解释运行引擎(ASP.DLL)。ASP.DLL 将从文件系统或内部缓冲区获取指定的 ASP 脚本文件,接着就进行语法分析并解释执行。最终的处理结果将形成 HTML 格式的内容,通过 Web 服务器“原路”返回 Web 浏览器,由 Web 浏览器在客户端形成最终的结果呈现。这样就完成了一次完整的 ASP 脚本调用。若干个相关的 ASP 脚本调用就组

成了一个完整的 ASP 脚本应用。

当使用 ASP 时,必须将存放.asp 文件的目录设置为“Excute (执行)”。建议在设置 Web 站点时,将 HTML 文件同 ASP 文件分开放置在不同的目录下,然后将 HTML 子目录设置为“读”,将 ASP 子目录设置为“执行”,这不仅方便了对 Web 的管理,而且最重要的是提高了 ASP 程序的安全性,防止了程序内容被客户端访问。

2. 对数据库的安全威胁

把电子商务、电子贸易的着眼点集中于 Web 服务器、Java 和其他新技术的同时,应该记住这些以用户为导向和企业对企业的系统都是以 Web 服务器后的关系数据库为基础的。它的安全直接关系到系统的有效性、数据和交易的完整性与保密性。系统的延时会降低效率欠佳,不仅影响商业活动,还会影响公司的信誉。不可避免地,这些系统受到入侵的可能性更大,但是并未对商业伙伴和客户敏感信息的保密性加以更有效的防范。此外,ERP 和管理系统,如 ASPR/3 和 PeopleSoft 等,都是建立在相同标准的数据库系统中的。无人管理的安全漏洞与时间拖延、系统完整性和客户信任等问题有直接的关系。

数据库的安全威胁主要包括事务内部的故障、系统范围内的故障、介质故障、计算机病毒与黑客。其中,数据库系统故障又称数据库软故障,是指系统突然停止运行时造成的数据库故障,如 CPU 故障、突然断电和操作系统故障。介质故障又称数据库硬故障,主要指外存故障,如磁盘磁头碰撞和瞬时的强磁场干扰等。

① 数据库系统的安全性要求:包括物理上的完整性、逻辑上的完整性、元素的完整性、可审计性、访问控制、用户认证、可获(用)性,如表 1.1 所示。

表 1.1 数据库系统对安全性的要求

安全问题	说 明
物理上的完整性	预防数据库数据物理方面的问题,如掉电,以及被灾祸破坏后能重构数据库
逻辑上的完整性	保持数据的结构,例如,一个字段的值的更改不至于影响其他字段
元素的完整性	包含在每个元素中的数据是准确的
可审计性	能够追踪谁访问修改过数据库的元素
访问控制	允许用户访问被批准的数据,以及限制不同的用户有不同的访问模式,如读或写
用户认证	确保每个用户被正确地识别,既便于审计追踪,也为了限制对特定的数据进行访问
可获(用)性	用户一般可以访问数据库及所有被批准访问的数据

② 数据库系统信息安全性依赖于两个层次:一层是数据库管理系统本身提供的用户名

/ 口令字识别、视图、使用权限控制、审计等管理措施；另一层就是靠应用程序设置的控制管理。

③ 数据库保护：主要是指数据库的安全性、完整性、并发控制和数据库恢复。

3. 公共网关接口（CGI）程序、asp、jsp、pl、php 等其他工具程序的安全威胁

公共网关接口（CGI）程序、asp、jsp、pl、php 等其他工具程序，都可以实现从 WWW 服务器到另一个程序的信息传输，如果滥用就会带来安全威胁。它们能够提高运行权限，以至于能自由访问系统资源；同时，它们很难追踪和管理。攻击者能够追踪这些工具程序，检查并了解它们，然后加以利用。

4. 服务器所运行程序的安全威胁

① 通过客户机传输给 WWW 服务器或直接驻留在服务器上的 Java 或 C++ 程序造成的缓存溢出性攻击。

② 服务器被用做攻击跳板的攻击威胁，如邮件炸弹。

1.2.2 保护电子商务服务器

电子商务服务器软件包括 WWW 服务器、FTP 服务器、电子邮件服务器、远程登录服务器、数据库服务器、域名服务器和主机上的操作系统等。每种服务器软件都需要单独考虑制定其安全模式，还要做到整体上的统一协调。

1. 商务服务器的安全解决方案

（1）访问控制和认证

访问控制和认证是指控制访问商务服务器的人和访问内容。服务器可用多种方式对用户进行认证。第一，证书是用户的许可证；第二，服务器检查证书上的时间标记以确认证书是否过期，并拒绝为过期证书提供服务；第三，服务器可使用呼叫系统，即根据用户名和为其指定的客户机地址的清单来核对用户名和客户机地址。

服务器若采用用户名与口令对用户进行认证，就必须维护合法用户的用户名与口令的数据库。以明文形式保存用户名，而用加密方式来保存口令。

WWW 服务器一般是以提供访问控制列表的方式来限制用户的文件访问权限。访问控制列表是文件和其他资源及有权访问这些文件和其他资源的用户名的清单或数据库。每个文件都有自己的访问控制列表。当客户机请求 WWW 服务器以便访问一个已设置好访问检查的文件时，WWW 服务器即检查此资源的访问控制列表以确定此用户是否有权访问此文件。

（2）操作系统控制

操作系统为运行在其上的 WWW 服务器提供了安全子系统，UNIX 和 Windows 操作系

统是大多数 WWW 服务器的运行平台。

UNIX 系统的资源访问控制是基于文件的,为了维护系统的安全性,系统中每一个文件都具有一定的访问权限,只有具有这种访问权限的用户才能访问该文件,否则系统将给出 Permission 或 Denied 的错误信息。有 3 类用户:用户本人、用户所在组的用户、其他用户。允许权:R—读,W—写,X—执行。允许权组:A—管理员(所有权利),V—属主,G—组,O—其他每个人。

Windows 的 NTFS 文件系统是一种安全的文件系统,因为它支持文件访问控制,人们可以设置文件和目录的访问权限,控制谁可以使用这个文件,以及如何使用这个文件。5 个预定义的许可为:拒绝访问,读取,更改,完全控制和选择性访问。

(3) 为电子商务服务器配置防火墙

防火墙在内网和外网之间建立了一层保护,通常也是第一道保护。公司同因特网间的通信都要经过防火墙,要保护的网络和计算机放在防火墙内,其他网络则处在防火墙之外。防火墙相当于一个过滤设备,它允许特定的信息流入或流出被保护的网络。

2. 如何配置 Web 服务器的安全特性

(1) 检查危及安全的漏洞

通常,如果 IP 地址设置不正确,就不能转换。一旦 Web 服务器获得 IP 地址和客户可能的域名,它就开始执行一系列验证手段。这里,有 3 个安全漏洞:

① 客户可能永远得不到要求的信息,因为服务器伪造了域名。客户可能无法获得授权访问的信息。

② 服务器可能向另一用户发送信息,因为客户伪造域名。

③ 误认闯入者是合法用户,服务器可能允许闯入者访问。

(2) 加强服务器的安全的具体措施

① 认真配置服务器,使用它的访问和安全特性。

② 可将 Web 服务器当做无权的用户运行。

③ 检查驱动器和共享的权限,将系统设为只读状态。

④ 可将敏感文件放在基本系统中,再设二级系统,所有的敏感数据都不向因特网开放。

⑤ 充分考虑最糟糕的情况后,配置自己的系统。

⑥ 检查 HTTP 服务器使用的 Applet 脚本和客户交互作用的 CGI 脚本。防止外部用户执行内部指令。

⑦ 建议在 Windows NT 类服务器上运行 Web 服务器,这样会比较安全,尽管它不能提供像 UNIX 和 Sun 那样多的功能。

3. 如何排除站点中的安全漏洞

最基本的安全措施是排除站点中的安全漏洞,使其降到最少,通常表现为以下 4 种方式。

① 物理的漏洞由未授权人员访问引起,由于他们能浏览那些不被允许的地方。用户不仅能浏览 Web,而且可以改变浏览器的配置并取得站点信息,如 IP 地址、DNS 入口等。

② 软件漏洞是由“错误授权”的应用程序引起的。例如,脚本和 Applet,它会执行不应执行的功能。一条首要规则是:不要轻易相信脚本和 Applet。使用时,应确信能掌握它们的功能。

③ 不兼容问题漏洞是由不良系统集成引起的。一个硬件或软件运行时可能工作良好,一旦和其他设备集成后(如作为一个系统),就可能出现問題。这类问题很难确认,所以对每一个部件在集成进入系统之前,都必须进行测试。

④ 缺乏安全策略。如果用户用他们的电话号码作为口令,无论口令授权体制如何安全都没用。必须有一个包含所有安全必备(如覆盖阻止等)的安全策略。

4. 防止和追踪黑客闯入和内部滥用

为了防止和追踪黑客闯入或内部滥用,需要对 Web 站点上的出入情况进行监视控制。

(1) 监控请求

① 服务器日常受访次数是多少?受访次数增加了吗?

② 用户从哪里连接的?

③ 一周中哪天最忙?一天中何时最忙?

④ 服务器上哪类信息被访问?哪些页面最受欢迎?每个目录下有多少页被访问?

⑤ 每个目录下有多少用户访问?访问站点的是哪些浏览器?与站点对话的是哪种操作系统?

⑥ 更多的选择是哪种提交方式?

(2) 测算访问次数和访问者数目

以下两个指标直接影响安全保护,也会促进安全性的提高和改善。

① 确定站点访问次数。访问次数是一个原始数字,仅仅描述了站点上文件下载的平均数目。

② 确定站点访问者数目。将访问次数与主页文件联系在一起时,该数字接近于某个时期内访问者数目,但不是百分之百的准确。

(3) 传输

Web 由传输协议、数据格式(HTML)及浏览器组成。使用协议、数据格式或浏览器,无须任何特别要求。

(4) 传输更新

Web 站点的连接信息必须不停地更新、重建与改变,否则,将严重限制 Web 站点的服务质量。一般来说,Web 站点只允许单一种类的文本作为连接资源。

Apache 是一个非常优秀的 Web 服务器。Apache 的安装维护中需要注意以下问题:

- ① 检查文件和目录的权限是否恰当。
- ② httpd.conf、srm.conf 和 access.conf 文件的设置是否适当。
- ③ 使服务器日志文件能够记录尽可能详细的信息。
- ④ 对某些需要特别保护的目录使用密码保护 (.htaccess)。
- ⑤ 对 CGI 脚本或者程序进行封装。
- ⑥ 如果 CGI 使用 Perl 编写, 要详细检查其安全性。
- ⑦ 检查 SSI 命令。
- ⑧ 使用 TCP Wrappers 和 Tripwire。

1.3 电子商务安全问题

1. 电子商务活动的内容

从商务活动的角度看, 电子商务活动整体上大致包括以下 3 个方面:

- ① 电子商务信息必须通过计算机网络进行传输。
- ② 在网络上传输的信息需要进行加密。
- ③ 进行商务活动的双方必须得到某种身份认证, 保障交易的安全性。

因此, 电子商务的安全性体现在网络安全、信息加密技术及交易的安全。电子商务交易安全紧紧围绕传统商务在因特网上应用时产生的各种安全问题, 在计算机网络安全的基础上, 如何保障电子商务过程的顺利进行。计算机网络安全与商务交易安全实际上是密不可分的, 两者相辅相成, 缺一不可。没有计算机网络安全作为基础, 商务交易安全就如空中楼阁, 无从谈起; 没有商务交易安全保障, 即使计算机网络本身再安全, 仍然无法达到电子商务所特有的安全要求。

在因特网设计之初, 只考虑方便性、开放性, 使得因特网非常脆弱, 极易受到黑客的攻击或有组织的群体的入侵, 也会由于系统内部人员的不规范使用和不满意雇员的恶意破坏, 使得网络信息系统遭到破坏, 信息泄露。

2. 电子商务网络主要的安全问题

- ① 物理实体的安全问题, 包括设备的机能失常、电源故障、由于电磁泄漏引起的信息失密、搭线窃听、自然灾害等。
- ② 未进行操作系统相关安全配置。
- ③ 软件的漏洞和“后门”。
- ④ 网络协议的安全漏洞。
- ⑤ 黑客的恶意攻击。
- ⑥ 计算机病毒的攻击。