21世纪高职高专精品系列规划教材
电子商务专业
21SHIJI GAOZHIGAOZHUAN JINGPIN XILIE GUIHUA JIAOCAI
DIANZI SHANGWU ZHUANYE

电子商务信息安全

DIANZI SHANGWU XINXI ANQUAN

蒋汉生 ◎ 主 编
黄 浩 ◎ 副主编

首都经济贸易大学出版社

21世纪高职高专精品系列规划教材
电子商务专业
21SHIJI GAOZHIGAOZHUAN JINGPIN XILIE GUIHUA JIAOCAI
DIANZI SHANGWU ZHUANYE

电子商务信息安全

DIANZI SHANGWU
XINXI ANQUAN

蒋汉生 ◎ 主 编
黄 浩 ◎ 副主编

首都经济贸易大学出版社
·北京·

出版说明

21世纪是信息化的时代，在全球信息化的大趋势下，各国电子商务在不断发展和完善。随着我国电子商务的蓬勃发展，培养多层次电子商务专业人才成为各界的迫切要求。

国内外教育学者都在积极探寻电子商务专业的教育教学模式，尤其是以培养应用型人才为主的高职高专的教学，更需要一套有别于本科层次的教学模式，那就是在保证基本理论教学的基础上增加实际应用部分的训练。相应的，高职高专教材的编写同过去相比也发生了较大变化，不再是本科教材的简写版，而是在讲解必备理论知识的基础上突出与实际相结合的特点。针对这一变化和要求，我们出版了这套颇具特色的高职高专电子商务专业规划教材。

本套教材有如下特点。

第一，为了让同学们对即将学习的内容有一个感性的认识，每一节都从“引导案例——打开知识的大门”开始，带着引导案例后的问题，展开对本节内容的讲述。

第二，在每一节正文内容讲完之后，设置了“本节内容图表化”，用图表的形式将本节内容作一归纳总结，这样方便学生对本节所讲内容的脉络有一个清晰整体的把握。

第三，在“本节内容图表化”之后安排有“开阔视野——还有你所不知道的”。这一部分介绍与本节内容相关的最新知识或最新应用，尽可能拓展学生们的知识面和眼界。

第四，在“开阔视野”之后安排有“案例学习——看看你的分析能力”。这一部分主要选取现实中的企业案例，让学生在对实际案例的分析中领悟本节所讲的理论知识，并通过回答案例之后的问题来检验自己对本节知识的应用能力。

第五，在“案例学习”之后设置了“班级讨论——加深你的知识理解”。这一部分由几道讨论题组成，最好由老师在完成本节教学内容之后，有准备地组织大家在课堂上展开班级讨论，让学生在轮流发言的过程中加深并补充对知识的理解

第六，在“班级讨论”之后设置了“自己动手——锻炼你的实践能力”。这一部分向学生提出了实际操作的科目，可由老师指导，让学生将其作为课后实践作业来完成，也可以作为平时实践测评的内容。

第七，在每一小节的最后设置“小节复习——牢记本节主要内容”。这一部分归纳出学生应当掌握的重点内容，便于老师进行阶段性知识点考核。

当然，由于不同课程特点不同，有个别教材并不一定同时具备以上所有特点，不过这并不妨碍读者对教材的使用。

本套教材力求有所创新，以便更好地为教师和学生服务，但是由于时间有限、难度较大，疏漏之处在所难免，希望各位老师、同学以及各界同仁们在使用过程中，如有意见和建议随时与我们联系沟通。

·21世纪高职高专精品系列教材规划小组·

前　言

•PREFACE•

Internet 作为通信技术、网络技术和信息技术的载体与表现形式，呈现了爆炸式的增长方式，而基于 Internet 的电子商务应用也得到了空前的发展，电子商务从 20 世纪 90 年代中期诞生以来，已经走过了十几年的发展历程。十几年来，安全问题始终是影响其发展的一个瓶颈，可以说电子商务信息安全是电子商务顺利发展的关键，也是难点。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。当进行电子商务交易、特别是网络支付的时候，在公共的 Internet 网上需要传输消费者和商家的一些机密信息、如用户信用卡号、商家与用户信息和订购信息等，而这些信息一直是网络非法入侵者或黑客的攻击目标。如何保证电子商务交易的安全性，如何对敏感的个人信息提供机密性保障，如何认证交易双方的合法身份，如何保证数据的完整性和交易的不可否认性等，已经成为制约电子商务发展的瓶颈，也成为众多学者、研究开发人员、政府人员和管理人员关注的目标。电子商务信息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、病毒的防治等，也包括相关管理制度的建立，这是一个涉及范围相当广泛的问题，需要各方的协调配合。

本书共由 15 章组成，第一章介绍了电子商务信息安全的基本概念，第二章介绍了密码技术和密钥管理，第三章进一步介绍了单钥密码体制和双钥密码体制，第四章介绍了密码技术应用，第五章简单介绍了计算机病毒的基本概念和防治策略，第六章介绍了访问控制与口令认证系统，第七章介绍了防火墙技术，第八章介绍了入侵检测技术，第九章介绍了虚拟专用网技术，第十章介绍了身份证明系统和公钥证书，第十一章介绍了公钥基础设施，第十二章介绍了证书机构，第十三章介绍了个人数字证书的申请和使用，第十四章介绍了两种常见的电子商务安全协议——SSL 和 SET，第十五章为实验指导，比较详细地介绍了几种常见的信息安全实验。

本书由蒋汉生任主编，负责第一章至第七章和第九章至第十四章的编写工作；黄浩任副主编，负责第八章和第十五章的编写，并负责各章的引导案例的收集和编写。参加本书资料收集和编写工作的还有研究生王鹏举、李宁等，最后由蒋汉生负责全书的统稿。

本书在编写过程中，借鉴了国内外有关电子商务安全、密码学、信息安全等方面的著作、教材、文章和网站资料，在此对相关作者一并表示感谢。书中疏漏之处敬请广大读者批评指正。

编者

目 录

• CONTENTS •

1 电子商务信息安全基础 / 1

1.1 电子商务的发展 / 2

1.2 电子商务信息安全基础 / 4

1.3 计算机安全等级 / 19

2 电子商务安全需求与密码技术 / 23

2.1 电子商务的安全需求 / 24

2.2 密码技术 / 26

2.3 密钥管理技术 / 30

2.4 密码体制的理论安全性与实际安全性 / 34

3 单钥密码体制和双钥密码体制 / 35

3.1 单钥密码体制 / 36

3.2 双钥密码体制 / 38

4 密码技术的应用 / 42

4.1 数据的完整性和安全 / 43

4.2 数字签名 / 46

4.3 数字信封 / 52

4.4 混合加密系统 / 52

4.5 数字时戳 / 53

5 计算机病毒及其防治 / 56

5.1 计算机病毒定义 / 57

5.2 计算机病毒的特征 / 57
5.3 计算机病毒的分类 / 59
5.4 计算机病毒的主要来源 / 60
5.5 计算机病毒的防治策略 / 61

6 访问控制与口令认证系统 / 64
6.1 访问控制 / 65
6.2 口令认证系统 / 68
6.3 个人特征的身份证明技术 / 70

7 防火墙技术 / 73
7.1 什么是防火墙 / 74
7.2 防火墙的设计原则 / 76
7.3 防火墙的基本组成 / 76
7.4 防火墙的分类 / 77
7.5 防火墙不能解决的问题 / 78

8 入侵检测技术 / 80
8.1 入侵检测的基本概念 / 81
8.2 入侵检测的信息源 / 85
8.3 入侵检测的分类 / 90
8.4 先进的入侵检测技术 / 92

9 虚拟专用网(VPN)技术 / 99
9.1 什么是 VPN? / 100
9.2 VPN 的优点 / 101
9.3 VPN 的基础——隧道协议 / 102
9.4 隧道的基本组成 / 103
9.5 IPSec / 104
9.6 选择 VPN 解决方案 / 105
9.7 VPN 的适用范围 / 106
9.8 VPN 的分类 / 107
9.9 组建 VPN 应该遵循的设计原则 / 111
9.10 VPN 应用中的制约因素 / 112
9.11 VPN 的几种解决方案 / 113

10 身份证明系统与公钥证书 / 116
10.1 身份证明系统 / 117
10.2 公钥证书 / 119

11 公钥基础设施(PKI) / 130
11.1 PKI 概述 / 131
11.2 密钥管理 / 138
11.3 不可否认业务 / 141

12 证书机构 / 148
12.1 证书机构概述 / 149
12.2 国内主要证书机构 / 152

13 个人数字证书的申请和使用 / 159
13.1 个人数字证书的申请 / 160
13.2 个人数字证书的使用 / 167

14 电子商务的安全协议 / 177
14.1 SSL——提供网上交易安全的协议 / 178
14.2 SET——提供安全的电子商务数据交换 / 181
14.3 SET 与 SSL 对比 / 195
14.4 SET 的缺陷 / 196

15 实验指导 / 198
15.1 口令攻击 / 198
15.2 数据加密与鉴别 / 205
15.3 数字证书服务及加密认证 / 214
15.4 防火墙技术 / 224

参考文献 / 233

1 电子商务信息安全基础

【本章要点】

本章主要包含三大部分内容：电子商务的发展；电子商务信息安全基础；计算机安全等级。第一部分内容要点是电子商务的发展历程。第二部分内容有三个要点：一是电子商务的安全隐患；二是电子商务安全性要求；三是各种电子商务安全威胁的原因。第三部分内容有两个要点：一是计算机安全等级的划分；二是计算机安全等级划分的原则。

【学习要求】

了解电子商务的发展历程；了解电子商务的安全隐患和电子商务信息安全的中心内容；了解计算机安全等级的划分。

引导案例——打开知识的大门

少年黑客入侵网站骗奖近5万元。在南昌读初中的学生刘小华，从小对电脑和网络非常感兴趣。他以“云中鹰”的网名加入了南昌高校学生组成的黑客QQ群，与里面的“黑客”交流经验，互相学习。在这个群中，刘小华认识了网名为“夜匪”的王军军和另外几个网友。

2008年2月4日晚，刘小华在上网时，无意中发现某电视台的网站有漏洞。他把这个“新发现”告诉了正在赣州全南县的网友“夜匪”。两人一起首次进入了电视台后台数据库，并篡改了网站首页内容。

2008年2月6日，刘小华在网络上碰到王军军后，表示要给王送上一份春节大礼。刘小华表示他可以修改电视台某中奖栏目的数据库，能窥视到此节目的短信平台。

王军军觉得这是个发财的机会，于是让刘小华进入网站，将发送的短信全部统计出来，2008年2月17日下午，王军军接到电视台的电话，表示其中奖得价值8 750元的笔

记本电脑一台。第二天，王军军来到南昌，将该奖品领走，之后再以5 000元的价格销售出去，并将部分钱分给了刘小华。

2008年2月29日，刘小华再次与江西某学院计算机专业的黄某合谋，从电视台领取了一台价值11 100元的笔记本电脑。为了能领取更多的奖品，刘小华干脆将电视台网站的后门地址告诉了陈某、黄某和何某。2008年3月7日～2008年5月15日，这伙人曾7次入侵电视台后台系统，骗取了近5万元的奖品，奖品均被在不同地点被低价卖出。

- 你了解网络安全的重要性吗？
- 如何能提高网络的安全性？

1.1 电子商务的发展

1.1.1 从电子数据交换到电子商务

电子商务可以分为以建立在专用网基础上的电子数据交换(EDI)为代表的传统电子商务和以因特网为基础的现代电子商务。EDI时代，电子商务系统的建设多半是由大型企业或政府主导的。现代电子商务则为大、中、小企业应用，尤其为中、小企业应用创造了几乎是相同的、平等的机会。

十几年以前，EDI还是电子商务的主要技术，但仅限于企业之间，即B2B模式。EDI采用的是“存储—转发”信息传输方式，类似于电子邮件，再加上结构化的信息内容和功能，以保证被传送信息的可审计性和能可靠送达目的地。EDI的规范、标准十分详尽、全面，几乎涵盖了商业往来所需资料数据的方方面面，因此也就很复杂、烦琐。全面实现EDI，代价太大，对多数中小企业是个沉重负担，不易推广。即使是大中型企业，往往在企业内部也只实现EDI规范的部分子集，只在进行国际贸易时，才将数据转换成标准的EDI格式。同时，由于EDI多半是建立在专用网络上，利用率较低，网络费用昂贵，这就限制了它的广泛应用。正因如此，传统的电子商务并未有过惊人的快速增长。

现代电子商务只是近几年才发展起来的，如前所述，因特网的发展带动了现代电子商务。或者说，它们互相推动，现代电子商务也是因特网快速发展的主要驱动力。因特网简化的技术标准(相对于传统电信网开放系统互联的7层协议)、广阔的覆盖面、较低的网络费用、琳琅满目可供选择的TCP/IP及Web等软硬件产品，使众多的企业和消费者

都有可能在其上进行商务活动。例如,因特网与 EDI 相结合,费用降低,使众多的中小企业能利用 EDI 这一有力的电子商务平台,提高其在市场尤其是国际市场中的竞争力。有报告说,网上交易的费用仅是传统商业方式的 1/10。另一方面,市场经济的利益驱动,使眼光敏锐的企业积极将商务活动推到网上,寻找新的商机,使因特网迅速发展,电子商务也因此成了因特网的主要业务。

1.1.2 现代电子商务的发展阶段

有人把现代电子商务的发展分成如下几个阶段,从中也可看出电子商务发展的轨迹、条件和基础。

1.1.2.1 网络基础设施大量兴建的阶段

网络基础设施的重要性很容易理解。当因特网从学术网向商用网转变之时,其规模不适应商业发展的需要,网络设施扩大规模、增加容量是必然的。在美国,首先看到这一巨大市场的主要是某些长途电信公司,他们率先展开了因特网骨干网络的建设,这在 20 世纪 90 年代早期就已经开始。近些年,一些新兴的公司也加入到建设网络设施的行列,建设了大量大容量的光纤网络和巨型路由器等。另有一些厂商则在接入手段上找机会,他们是因特网业务提供商(Internet Service Provider,ISP),他们建设了各种路由器、网站服务器、安全手段等。再有就是一些公司建立的内域网和外域网。以上这些组成了电子商务的网络基础软件和硬件,这是电子商务发展的第一个浪潮。

1.1.2.2 应用软件及服务成为热点的阶段

有了网络设施,人们要在上面进行安全可靠的通信和交往,就需要各种应用软件和服务。例如,使客户能建立他们所需应用的信息传送软件、认证软件、目录软件,各种应用业务的开发软件平台及工具,捆绑在一起解决某种应用的软件包,以及与这些软件有关的培训服务、系统集成服务、支撑服务等。这是电子商务发展的第二波。

1.1.2.3 网址及内容管理的建设发展阶段

接下来,企业要在网上树立自己的形象,推销自己的产品及服务。即在网上制作各种商务内容,如网页站点、生动而引人注目的产品介绍、方便人们寻找有关网址的目录表等。这一段时期的热点是如何在网上制作既能吸引人们又方便人们查找的“节目内容”(Content),出现了许多专门替人做网上内容的公司。更突出的是,当网页站点数急剧增加后,人们不知怎样找到所需的站点或所需的内容,于是出现了一些帮助人们进行搜索的站点,它们用超文本、超媒体等所谓 Web 技术(也许可译为“网罗”技术),将大量站点

集结在一起。人们通过这种“入口门户”站点,就可以容易地访问到所需要的东西。这些站点上有很好的被称为搜索引擎(Search Engine)的软件,人们也常把它们称为内容汇集的(Content Aggregation)搜索引擎站点,其中比较知名的有 google、baidu、AOL、Yahoo、Neteenter(Netscape)、MNS(Microsoft)等。现在,很多这种入口站点已经不只是搜索引擎,而是增加了其他业务,演变成电子商务“主持”、“代庖”公司等。这是电子商务发展的第三波。

1.1.2.4 网上零售业及其他交易蓬勃发展阶段

1998 年前后,零售业上网及更多企业在网上开展其电子商务成为电子商务发展的热点。许多零售商(如网上书店 Amazon 等)成了几乎人人皆知的电子商务成功的例子。零售商是面向消费者的,他们采用的电子商务模式主要是 B2C 方式。但 B2B 方式也有迅速的发展。按市场收益分配,B2B 占到 2/3 以上,B2C 占不到 1/3。这是电子商务发展的第四波。

这样划分现代电子商务发展的阶段,可能不够准确,也不是唯一的。但从中可以看出发展电子商务的各项要素及其准备和成熟的过程,有助于准备开展电子商务的经理人员的预先思考和规划。与其他事物的发展规律一样,电子商务的发展也是波浪形前进,每次都要经过:消化吸收—分析酝酿—计划试点—建设突破—快速增长—寻找新突破口这样一个过程,从量变到质变不断向前、不断上升。据国外权威机构统计,全球 1998 年电子商务达 800 亿美元,2000 年近 4 000 亿美元,2002 年达 2 万亿美元,2006 年世界电子商务交易额达 12.8 万亿美元。电子商务占全球商贸总额的比例,2003 年为 5%,2006 年 18%。从总体上看,现代电子商务尚处于其发展的初级阶段,还只是传统商业销售渠道的补充,即使在电子商务最发达的美国,网上的交易占整个商务总量的比例也低于 5%。但是,生产力是历史发展中最活跃的因素,新技术终将推动包括商务在内的人类社会活动的变革。若干年后,也许百货公司会变成仓库、货栈,汽车商店会变成只是汽车的展示场地,金钱及货品的交换将主要经互联网进行。古语说,“凡事预则立,不预则废”,预测到可能的变革而有所准备,总比被动跟着跑要好。

1.2 电子商务信息安全基础

1997 年 6 月 21 日,在美国内华达州的一个空军基地的计算机中心控制室内,基地的

100多名校级以上军官和来自美国空军部的决策者们静静地坐着，观看着控制中心大屏幕显示器的变化。来自美国CIA(中央情报局)的三位专家正在攻击该基地的一个指挥子系统，通过该指挥子系统可以上联美国五角大楼的指挥系统，下联美国太平洋舰队的司令部指挥系统。

经过一个多小时的测试，三位专家手中的一台笔记本电脑联入了该空军基地的指挥网络中心，另外两台上联美国五角大楼的指挥中心，下联美太平洋司令部的指挥系统，通过另一个在五角大楼的指挥中心的计算机授权，授予它可以拥有对美太平洋舰队的舰只调度权。这样它就可以调动美太平洋舰队的舰只驶向瓦胡岛(美属西太平洋上的一个小岛)。

这时，通过接通的五角大楼的军情通报中心，在场的军官们已经看到美太平洋舰队驻扎在离瓦胡岛五十海里的“NeLy”号驱逐舰已经出发。最初一部进入空军基地的指挥中心的笔记本电脑，则向空军指挥中心申请使用导弹许可证。几秒钟过后，完成导弹许可证申请，轰炸型歼击机开始准备，目标瓦胡岛的地理坐标已经被输入，攻击命令已经发出。一切已经准备就绪，这时输入一条“Cancel”(取消)指令，一切就此结束。

原来这只是一场演习。由美国中央情报局的技术专家向军方演示如何通过地方的公众网络进入军方的网络系统，并且可以篡改军方的指令，修改自己的用户授权。而且也可以施放病毒，使军方的网络在几秒钟内陷于瘫痪。这个演示使自以为“老子天下第一”的美国将军们大吃一惊，感到一种前所未有的恐惧。原来最早使用网络的美国国防部的网络竟是如此脆弱，不堪一击。这是一个真实的事件。近来，接二连三的网络黑客进入美军五角大楼网络系统，修改指令，盗走数据。试想连安全级别最高的美国国防部网络系统都能被侵入，那么一般的商业网络又怎么能避免呢？因此，当电子商务的基础建立在网络上时，只有网络的安全才能确保电子商务的安全。

1.2.1 电子商务存在的安全隐患

1.2.1.1 计算机系统的安全隐患

(1)硬件系统。计算机是现代电子科技发展的结晶，是一个极其精密的系统，它的每一个零件都是由成千上万个电子元件构成的。这一方面使计算机的功能变得十分强大，另一方面又使它极易受到损坏。

现在人们把计算机系统的漏洞或错误称为“Bug(臭虫)”，你知道为什么吗？有这样一种解释：

在计算机发展的初期，庞大的计算机在运行一个任务时往往发生错误而停止工作。

于是操作人员查遍了它的每一部分电路,最终发现原来只是一只臭虫死在某块电路板上,导致了短路,所以后来人们开始用“Bug”比喻系统错误。由此也可以看出计算机的硬件系统是如何的脆弱。

当然,现代的计算机硬件已经“健壮”了许多,但它毕竟属于精密仪器,震荡、静电、潮湿、过热等都会使它受到严重的损伤。而且,现代的计算机硬件体积很小,很容易被人偷窃。试想一下,如果你用来存放重要数据的硬盘被人偷走,后果将会怎样?

所以,不要过于信赖你的机器配置,要充分了解你的系统,并采取相应的措施加以保护,具体的方法我们后面还将详细讨论。

(2)软件系统。软件是用户与计算机硬件联系的桥梁。我们正是通过它来管理计算机内部的硬件,让它们执行命令的。任何一个软件都有它自身的弱点,而大多数安全问题都是围绕着系统的软件部分发生的,既包括系统软件也包括应用软件。

这里有两个有趣的例子。

最近发现,Microsoft 的 Windows NT 中的加密机制可以被有效地关闭。这个攻击方法现在已被称做是“Youalenowin France”。其工作方式是:由于法国不允许普通公众对具有高度保密信息的站点进行访问,因此如果 Windows NT 把用户的工作地点解释为法国,那么,NT 强大的加密机制就被禁止了,所以 NT 也不安全。

1996 年 1 月,加州大学伯克利分校计算机系的两个学生公开了 Netscape 加密方案中的一个严重缺陷。文章的题目是“随机性和 Netscape 浏览器(Ran-domness and the Netscape Browser)”,作者是 Goldberg 和 David。在文章中,他们解释了 Netscape 中的称为安全套接层(SSL)的加密协议实现方式中有一个内在的缺陷。这个缺陷使得当安全通信在万维网上被截获时可能被破译。这是一个绝好的基本缺陷的例子。

可见,软件系统的漏洞可谓多种多样、防不胜防。遗憾的是,到目前为止,人们还没有找到能够彻底查出或纠正软件所有漏洞的方法。所以,从安全的角度考虑,我们必须熟悉各种软件的特点,正确选择并配置和使用自己的平台。关于这方面的内容我们会在后面详细探讨。

1.2.1.2 电子商务的安全隐患

电子商务系统的安全问题不仅包括了计算机系统的安全隐患,还包括了一些自身独有的问题。

(1)数据的安全。一个电子商务系统必然要存储大量的商务数据,这是其运转的核心。一旦发生数据丢失或损坏,后果不堪设想。尤其这些数据大部分是商业秘密,一旦

泄露,将造成不可挽回的损失。

(2)交易的安全。这也是电子商务系统所独有的。在我们的日常生活中,进行一次交易必须办理一定的手续,由双方签发各种收据凭证,并签名盖章作为法律凭据。但在电子商务中,交易在网上进行,双方甚至不会见面,那么一旦一方反悔,另一方怎样才能够向法院证明合同的存在呢?这就需要一个网上认证机构对每一笔业务进行认证,以确保交易的安全,避免恶意欺诈。

1.2.2 电子商务系统可能遭受的攻击

一般说来,电子商务系统可能遭受的攻击有以下几种。

1.2.2.1 系统穿透

系统穿透是指未经授权的人通过一定手段假冒合法用户接入系统,对文件进行篡改、窃取机密信息、非法使用资源等。他们一般采取伪装(Masquerade)或利用系统的薄弱环节(如绕过检测控制)、收集情报(如口令)等方式实现。这也是大多数黑客使用的办法。

黑客们常常利用各种试探软件反复猜测某个网站的用户密码,一旦成功就可假冒该用户进入系统。更高级的黑客则会利用系统的缺陷巧妙地绕过检测机制,进入系统。1998 年 2 月,五角大楼的关键主机遭到了"迄今为止最有组织、有系统的攻击"。这次攻击是由一个以色列年轻人领导的,他向两个加州的年轻人演示了进入五角大楼安全分支的不同方法,于是那两个年轻人在数天之内进入了全美数以百计的网络。

1.2.2.2 违反授权原则

一个被授权进入系统做某件事的用户,在系统中做未经授权的其他事情,表面看来这是系统内部的误用或滥用问题,但这种威胁往往与外部穿透有关。一个攻击者可以通过猜测口令接入一个非特许用户账号,进而发现系统的薄弱环节,取得特许接入系统权,从而严重危及系统的安全。

1.2.2.3 植入

在系统穿透或违反授权攻击成功后,入侵者常会在系统中植入一种能力,为其以后攻击系统提供方便。如,向系统中注入病毒、蠕虫、特洛伊木马、陷阱、逻辑炸弹等来破坏系统正常工作。特洛伊木马为攻击者服务,例如一种表面上合法的字处理软件能将所有编辑过的文档复制存入一个隐蔽的文件夹中,供攻击者检索。曾经流行过的"美丽莎"病毒就是一种典型的植入攻击。黑客把病毒作为电子邮件的附件发给受攻击者,一旦对方

运行了该附件,其系统就会感染该病毒。更有甚者,如果附件不是病毒,而是远程控制程序,如有名的 B002K,则被攻击方的系统将完全被黑客控制,黑客可以随心所欲地浏览和删改对方的文件,甚至执行关机、重启等操作。

1.2.2.4 通信监视

这是一种在通信过程中从信道进行搭线窃听的拦截(Interception)方式。通过搭线和电磁泄漏等对机密性进行攻击,造成泄密,或对业务流量进行分析,获取有用的情报。侦察卫星、监视卫星、预警卫星、间谍飞机、隐身飞机、预警飞机、装有大型合成孔径雷达的高空气球和无数微型传感器都可用于截获和跟踪信息。

1.2.2.5 通信窜扰

通信窜扰攻击者对通信数据或通信过程进行干扰、对其完整性进行攻击、篡改系统中数据的内容、修改消息次序和时间(延时和重放)、注入伪造消息等。

1.2.2.6 中断

中断对可用性进行攻击,破坏系统中的硬件、硬盘、线路、文件系统等,使系统不能正常工作,破坏信息和网络资源。例如,高能量电磁脉冲发射设备可以摧毁附近建筑物中的电子器件,正在研究中的电子生物可以吞噬电子器件等。

1.2.2.7 拒绝服务

拒绝服务指合法接入信息、业务或其他资源受阻。例如,一个业务口被精心地策划进行滥用而使其他用户不能正常接入,又如 Internet 的一个地址被大量信息垃圾阻塞等。在 1999 年北约入侵南联盟期间,南斯拉夫的黑客们集中向北约的邮件服务器发送“PING”指令,使其系统因不得不全力接收并处理成千上万的该指令而无力处理正常的邮件业务,最终被迫关闭。

1.2.2.8 否认

一个实体进行了某种通信或交易活动,稍后却否认曾进行过这一活动,不管这种行为是有意还是无意的,一旦出现,再要解决双方的争执就不太容易了。

1.2.2.9 病毒

由于 Internet 的开放性,病毒在网络上的传播比以前快了许多,而且 Internet 的出现又促进了病毒制造者间的交流,使新病毒层出不穷,杀伤力也大有提高。著名的 CIH 病毒出现不久,其源码就在网上传开。很快,根据它改编的更隐蔽、更厉害的变种病毒大量出现,并造成了巨大的损失。

1.2.3 电子商务安全的中心内容

电子商务安全的中心内容主要有六项(如图 1 - 1 所示),包括机密性(Confidentiality)、完整性(Integrity)、认证性(Authentication)、不可否认性(Non-repudiation)、不可拒绝性(Denial of service)和访问控制性(Access control)。

电子商务安全的内容对于理解整个电子商务安全是非常重要的,所有的安全威胁都是针对这六项内容的,所有的安全技术也都是为了保证这六项内容。下面逐一说明六项电子商务安全的具体内容。

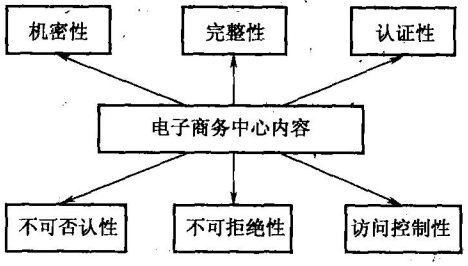

图 1 - 1 电子商务安全的六项中心内容

1.2.3.1 商务数据的机密性

商务数据的机密性或称保密性是指信息在网络上传送或存储的过程中不被他人窃取、不被泄露或披露给未经授权的人或组织,或者经过加密伪装后,使未经授权者无法了解其内容。机密性可通过加密和信息隐匿技术实现,使截获者不能解读加密信息的内容。机密性还包括保护通信流特性(通信源、目的地、频率、长度等),以防止被分析。电子商务的信息几乎都有加密的要求,如信用卡账号、用户名和密码、订货信息、付款信息等,这些信息被人窃取后,会造成直接经济损失。

1.2.3.2 商务数据的完整性

商务数据的完整性或称正确性是保护数据不被未授权者修改、建立、嵌入、删除、重复传送或由于其他原因使原始数据被更改。在存储时,要防止非法篡改,防止网站上的信息被破坏。在传输过程中,如果接收端收到的信息与发送的信息完全一样,说明在传输过程中信息没有遭到破坏,具有完整性。加密的信息在传输过程中,虽能保证其机密性,但并不能保证不被修改。

1.2.3.3 商务对象的认证性

商务对象的认证性是指网络两端的使用者在沟通之前相互确认对方的身份。保证身份的正确性,分辨参与者所声称身份的真伪,防止伪装攻击。认证性通过数字签名和身份认证技术实现。

1.2.3.4 商务服务的不可否认性

商务服务的不可否认性是指信息的发送方不能否认已发送的信息,接收方不能否认已收到的信息,这是一种法律有效性要求。交易一旦达成是不能否认的,否则必然会损害对方的利益。信息的不可否认性主要用于帮助通信用户对付来自其他合法用户的威胁,如发送用户对他所发的消息否认、接收用户对他已收的消息否认等,而不是对付来自未知攻击者的威胁。一般情况下,不可否认性不能制止某合法用户对某业务的否认,但可以提供足够充分的证据迅速地辨别出谁是谁非。在传统的商务系统中有法律作用的书面文件(如合同、报价、标书、订货单、发票、支票等),在处理过程中常会出现各种各样的问题,如票据丢失、损坏、被涂改、签章不全或不符、持票人身份不符、时戳不符、票据伪造等。为了解决这类问题常采用各种手段,如签名、柜台签名、仲裁签名、收据、邮戳、挂号邮件等。好的商务系统都会采用适当的书面文件来解决可能出现的争执,必要时可提供足够的证据,有时需要第三者(如邮局、代理人、仲裁等)的协助。当然,在电子商务系统中也需要不可否认业务,但解决起来比传统商务更为困难,需要采用新的技术如数字签名等。

1.2.3.5 商务服务的不可拒绝性

商务服务的不可拒绝性或称可用性是保证授权用户在正常访问信息和资源时不被拒绝,即保证为用户提供稳定的服务。可用性的不安全是指“延迟”的威胁或“拒绝服务”的威胁,这类威胁的结果是影响计算机的正常处理速度或完全拒绝处理。降低服务速度会把自己网站的顾客赶到竞争者的手中,或者在竞争交易中(如证券市场、拍卖市场)错过商机。

“拒绝服务”的攻击往往使整个网络暂时不能使用。最有名的例子是1988年的蠕虫病毒使5 000多台计算机不能工作达几个小时。

1.2.3.6 访问控制性

访问控制性是指在网络上限制和控制通信链路对主机系统和应用系统的访问。用于保护计算机系统的资源(信息、计算和通信资源)不被未经授权人或以未授权方式接入、使用、修改、破坏、发出指令或植入程序等。