高等教育规划教材

电子商务安全

主　编　张　波
副主编　邢苗条　王　园　胡　霞

免费提供电子教案

下载网址 http://www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

高等教育规划教材

电子商务安全

主　编　张　波
副主编　邢苗条　王　园　胡　霞

机械工业出版社

本书围绕保障电子商务活动安全性的核心问题进行讲述，并结合电子商务应用的常见安全问题进行详细介绍。全书共分8章，分别介绍了电子商务安全导论、数据加密与密钥管理技术、公钥基础设施PKI与数字证书、数字签名与身份认证技术、安全协议与安全标准、网络安全技术、数据库系统安全以及电子商务安全评估与管理等方面的内容，并根据每章的具体内容安排了思考题、实战题等特色实践模块。

本书内容新颖，结构严谨，深入浅出，实用性强，突出对基础理论和基本技能的掌握和技术应用能力的培养，可作为高等院校电子商务、市场营销、信息管理与信息系统、管理类、经贸类等相关专业的教材，也可作为电子商务培训用书以及企业管理人员参考用书。

本书配有授课电子课件，需要的教师可登录www.cmpedu.com免费注册，审核通过后下载，或联系编辑索取（QQ：2966938356，电话：010－88379739）。

图书在版编目（CIP）数据

电子商务安全/张波主编. —北京：机械工业出版社，2015.1
高等教育规划教材
ISBN 978－7－111－50208－1

Ⅰ.①电… Ⅱ.①张… Ⅲ.①电子商务－安全技术－高等学校－教材
Ⅳ.①F713.36

中国版本图书馆CIP数据核字（2015）第098573号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
策划编辑：王 斌 责任编辑：王 斌
责任校对：张艳霞 责任印制：刘 岚
三河市国英印务有限公司印刷
2015年6月第1版·第1次印刷
184mm×260mm·15.25印张·378千字
0001－3000册
标准书号：ISBN 978－7－111－50208－1
定价：36.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务	网络服务
服务咨询热线：（010）88379833	机 工 官 网：www.cmpbook.com
读者购书热线：（010）88379649	机 工 官 博：weibo.com/cmp1952
	教育服务网：www.cmpedu.com
封面无防伪标均为盗版	金 书 网：www.golden－book.com

出 版 说 明

当前，我国正处在加快转变经济发展方式、推动产业转型升级的关键时期。为经济转型升级提供高层次人才，是高等院校最重要的历史使命和战略任务之一。高等教育要培养基础性、学术型人才，但更重要的是加大力度培养多规格、多样化的应用型和复合型人才。

为顺应高等教育迅猛发展的趋势，配合高等院校的教学改革，满足高质量高校教材的迫切需求，机械工业出版社邀请了全国多所高等院校的专家、一线教师及教务部门，通过充分的调研和讨论，针对相关课程的特点，总结教学中的实践经验，组织出版了这套“高等教育规划教材”。

本套教材具有以下特点：

1）符合高等院校各专业人才的培养目标及课程体系的设置，注重培养学生的应用能力，加大案例篇幅或实训内容，强调知识、能力与素质的综合训练。

2）针对多数学生的学习特点，采用通俗易懂的方法讲解知识，逻辑性强、层次分明、叙述准确而精练、图文并茂，使学生可以快速掌握，学以致用。

3）凝结一线骨干教师的课程改革和教学研究成果，融合先进的教学理念，在教学内容和方法上做出创新。

4）为了体现建设“立体化”精品教材的宗旨，本套教材为主干课程配备了电子教案、学习与上机指导、习题解答、源代码或源程序、教学大纲、课程设计和毕业设计指导等资源。

5）注重教材的实用性、通用性，适合各类高等院校、高等职业学校及相关院校的教学，也可作为各类培训班教材和自学用书。

欢迎教育界的专家和老师提出宝贵的意见和建议。衷心感谢广大教育工作者和读者的支持与帮助！

机械工业出版社

前　言

电子商务是一种全新的业务和服务方式，为全世界的人们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。自20世纪90年代中期诞生以来，电子商务已经走过了近20年的发展历程。20年来，安全问题始终是影响电子商务发展的一个瓶颈。可以说，电子商务安全是电子商务顺利发展的一个关键和难点。

电子商务的出现使人们从原有面对面的交流方式转变成通过网络实现交流，不仅大大缩短了信息交流的时空距离，而且对人们的生活方式、企业经营方式、商业模式都产生了一定影响。电子商务这种新型的商务活动正是借助于网络技术发展起来的，它继承了网络的开放性和全球性，在提高商务效率、降低交易成本的同时，随之也带来了一些安全性问题。确保交易过程等方面的安全，保证电子商务活动中的隐私数据的安全，为客户在网上从事商务活动提供信心保证等，是电子商务全面发展的前提。

电子商务作为一种全新的企业经营模式，具有开放性，同时也带来了诸多困扰，比如病毒入侵、黑客攻击、信息抵赖、假冒信息等，这些问题给企业带来的损失不可估量，因此要想更高效地利用电子商务平台，这类问题就必须引起高度重视。要想保障电子商务各方面的安全，需要对电子商务系统的计算机硬件、网络访问、文件输出和接收以及电子商务平台等众多环节进行全面的控制和监测，也需要相关安全法律法规和物理安全机制的配合。

电子商务发展的保障就是提高安全性。若无法解决这一问题，电子商务将无法发展，更谈不上实现电子交易。保障电子商务的安全不仅应从技术角度采取措施，更重要的是从管理和法律的角度着手。我国政府已逐渐完善了电子商务运行和管理的有关法律法规，在电子商务的管理体系上力求做到四个一致，即经济体制一致，经济安全监督一致，信息安全保密管理一致，信用体制一致。政府相关机构也已明确了自身在电子商务中的政策引导、密码控制、交易监督等作用。

本书力求突出电子商务安全的特色与技术需求。一方面，考虑到电子商务专业学生学习的基础与实践的需求，将密码学与网络安全中涉及较深数学知识及较复杂的密码算法部分略去，保留一些基本的密码学原理和一些必要的数学知识；另一方面，处理好电子商务安全原理和应用之间的关系。原理是基础，本书对电子商务安全的基础问题，如加密和认证等技术做了较详细、通俗且符合认知逻辑的阐述，使读者能更深刻地理解电子商务安全问题产生的根源。虽说“三分技术、七分管理”，但目前绝大多数电子商务安全教材在篇幅安排上都是“七分技术、三分管理”。因为大学教育的主要目的是为学生打基础，对技术知识，学生自学掌握比较困难，因此有必要重点阐述，使学生能理解技术知识，而管理知识学生可以通过将来在实际工作中掌握，只有有了一定的实践经验才能更有效地学习和理解安全管理方面的内容。

本书最大的特点在于立足电子商务的安全问题，系统、全面地阐述了电子商务的安全知识和应用技术，可以使读者对电子商务安全有一个完整的认识。本书系统性强、内容新颖、实用性和可操作性强，复杂的概念、过程、原理等都配有图解，非常便于讲解和自学。此

外，本书每章结尾都配有思考题、实战题等，便于教学和启发思维。

本书的知识结构可分为导论、原理与应用三大块，共由 8 章组成。其中第 1 章为导论部分，第 2 ~5 章为原理部分，第 6 ~8 章为应用部分。第 1 章主要介绍了电子商务安全导论，第 2 章讲述了数据加密与密钥管理技术，第 3 章阐述了公钥基础设施 PKI 与数字证书，第 4 章是关于数字签名与身份认证技术方面的知识，第 5 章重点介绍了安全协议与安全标准，第 6 章是关于网络安全技术方面的内容，第 7 章侧重介绍了数据库系统安全知识，第 8 章从评估、立法、管理的角度阐述了电子商务安全评估与管理的内容。

本书第 1 章由西安财经学院邢苗条编写，第 2、3 章由西安财经学院谢晶编写，第 4 章由集美大学王园编写，第 5、6 章由安徽理工大学张波、黄红兵编写，第 7、8 章由电子科技大学成都学院胡霞编写。邵康、张红霞、王向前、徐超毅、杨超宇、沈长霞、方仁友、陶静、陈亚树也参与了本书的部分编写或者对编写工作提供了帮助。

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，编者努力想把有关电子商务安全的最新知识介绍给读者，但由于编者水平所限，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

2015 年 1 月

目　录

第1章　电子商务安全导论

本章要点

- 了解电子商务安全的基本概念与安全现状。
- 掌握电子商务面临的安全威胁及安全需求。
- 了解电子商务中常用的安全技术。
- 掌握电子商务安全体系结构。
- 了解电子商务的安全服务及相关安全协议。

引例

淘宝网1元“错价门”事件——电子商务安全不容忽视

中国IDC评述网2009年9月14日报道：互联网上从来不乏标价1元的商品。近日，淘宝网上大量商品标价1元，引发网民争先恐后哄抢，但是之后许多订单被淘宝网取消。随后，淘宝网发布公告称，此次事件为第三方软件“团购宝”交易异常所致。部分网民和商户询问“团购宝”客服得到自动回复称：“服务器可能被攻击，已联系技术紧急处理。”这起“错价门”事件发生至今已有两周，导致“错价门”的真实原因依然是个谜，但与此同时，这一事件暴露出来的电子商务安全问题不容小觑。

电子商务（Electronic Commerce）是指政府、企业和个人利用现代电子计算机与网络技术实现商业交换全过程，它是一种基于互联网，以交易双方为主体，以银行电子支付结算为手段，以客户数据为依托的全新商务模式。电子商务的参与者包括企业、消费者和中介机构等。它的本质是建立一种全社会的“网络计算环境”或“数字化神经系统”，以实现资源在国民经济和大众生活中的全方位应用。

时至今日，电子商务已经逐渐深入到人们的日常生活中，越来越多的人通过互联网进行电子商务活动。电子商务的发展给人们的工作和生活带来了新的体验和更多便利，前景十分诱人，也为人们带来了无限商机。但仍有许多商业机构对电子商务持观望态度，主要原因是对网上运作的安全问题存有疑虑。在竞争激烈的市场环境下，电子商务的一些信息可能属于商业机密，一旦信息失窃，企业的损失将不可估量，因此，在运用电子商务模式进行贸易的过程中，安全问题就成为电子商务最核心的问题，电子商务安全包括有效保障通信网络，信息系统的安全，确保信息的真实性、保密性、完整性、不可否认性和不可更改性等方面。

本章主要介绍电子商务安全概念，以及电子商务面临的安全威胁、安全特点、安全环境、安全技术、安全体系结构和安全服务及安全协议等。

1.1 电子商务安全概况

近年来，网络技术和电子商务迅猛发展，人们在互联网上进行的商务活动的范围和数量与日俱增，如，日常生活用品、书籍的购买；家具、汽车、房产交易；股票、期货、资金运作等等。在这一过程中，电子商务赖以运行的互联网的安全问题。成为人们持续关注的话题，电子商务安全的重要性已不言而喻。网络安全问题是电子商务推进中的关键因素，营造信誉良好、安全可靠的网络交易环境才能让众多的企业和消费者支持电子商务，否则消费者不信任网上交易，企业没有把握在网上营销，电子商务便只能是“水中花、镜中月”。尽管政府以及一些企业已意识到这一问题，但因为一直缺乏一个网络安全保护的完整概念，所以很多人在安全认知上仅限于对网络“防火墙”的了解，而网络防火墙只是网络安全保护的一个方面，绝不是全部，这也正是很多个人或企业的实施了防火墙的网络仍有漏洞存在的原因。

网络安全事件在国内外时有发生。2000 年 2 月 7 日、8 日、9 日这三天，美国许多著名的网站先后遭到互联网历史上最严重的计算机黑客攻击，在美国社会引起了强烈震动。

在当时，黑客 3 天的袭击造成的直接和间接经济损失达 10 亿美元。2 月 7 日，除了免费电子邮件和三个站点未受影响外，雅虎的大部分网络服务及站点陷于瘫痪。雅虎是当时全球第二大搜索引擎网站，每天被浏览页次达 465 亿次，其股市价值达 930 亿美元；8 日上午，先是当天股票交易公司网站瘫痪，再接着是网上电子拍卖网站电子港湾（ebay）和网上书店及商品销售网站亚马逊（Amazon）告急。ebay 的注册用户达 1000 万，是每月浏览达 15 亿次的网上拍卖网站，8 日下午 6 时，该网站的商品买卖一度停止数小时。当晚，美国有线电视新闻网（CNN）宣布，其网站因负荷超载，从下午 7 时至 8 时 45 分信息传送被阻断；2 月 9 日，一些电子交易类网站再度遭殃，在股市开市前遭到持续 1 小时的攻击，科技新闻网站 ZDNet 约有 70% 的内容中断 2 小时，上网者无法接触到包括网站新闻和产品浏览等内容的信息。

引人注目的是，这也是互联网历史上第一次有黑客大规模、有目的地袭击商业网站。美国联邦计算机案件处理中心主任大卫·加诺说：“全美至少有数百台计算机受到袭击。所幸的是，黑客并未进入这些网络内部，窃取业务和客户资料。如此众多的大型网站，特别是新兴的电子商务网站，在 3 天的短时间内连续遭到黑客攻击，这在互联网历史上还是第一次。”

2006 年 12 月初，我国互联网上大规模爆发了“熊猫烧香”计算机病毒及其变种。一只憨态可掬、颔首敬香的“熊猫”在互联网上疯狂“作案”，在病毒卡通化的外表下，隐藏着巨大的传染潜力，短短三四个月，“烧香”潮波及上千万个人用户、网吧及企业局域网用户，造成直接和间接损失超过 1 亿元。

作为高科技犯罪的典型代表之一，银行网络安全事故近两年来在国内频频发生。2010 年年末，互联网上连续出现的假银行网站事件曾经轰动一时。一个行标、栏目、新闻、图片样样齐全的假冒中国银行网站，竟然成功划走了呼和浩特一名市民银行卡里的 2.5 万元。且随后不久，假工行、假农行、假银联网站也相继跟风出现。而早在 2003 年下半年，我国香港地区也曾出现不法分子伪冒东亚、花旗、汇丰、宝源投资及中银国际网站骗取用户钱财。

有一些黑客，专门盗窃大量的游戏装备、账号，虽然这些游戏装备、账号并不能马上兑换成人民币，但通过网上交易，这些盗来的游戏装备、QQ 账号甚至银行卡号资料被中间批发商全部放在网上游戏交易平台公开叫卖，一番讨价还价后，虚拟货币得以兑现，网友们通过网上银行将现金转账，就能获得那些盗来的网络虚拟货币。

在我们身边也时常发生一些网络安全问题：如：不断有人户抱怨 QQ 密码被更改，邮箱邮件被别人收走，网站栏目信息被入侵者修改等。

2014 年 4 月 8 日，安全协议 OpenSSL（Open Secure Sockets Layer）被曝出现严重安全漏洞，这个漏洞被黑客命名为“heartbleed”，意思是“心脏流血”——表示最致命的内伤。黑客利用该漏洞，坐在自己家里的电脑前，就可以实时获取约 30% 以 HTTPS（Hypertext Transfer Protocol over Secure Socket Layer）开头网址的用户登录账号密码，包括大批网银、购物网站、电子邮件等。这个事件更加引起了全球对网络安全问题的极大关注。

由以上案例可见，电子商务安全是一个不容忽视、涉及范围极广的社会问题，这些问题将长期存在，并时刻干扰电子商务的正常健康运行。

1.1.1 电子商务安全概念与特点

1. 电子商务安全的定义

电子商务的一个重要技术特征是利用计算机网络来传输和处理商业信息，因此，电子商务安全从整体上可分为两大部分：计算机网络安全和商务交易安全。

计算机网络安全的内容包括：计算机网络设备安全、计算机网络系统安全、数据库安全等。其特征是针对计算机网络本身可能存在的安全问题，实施网络安全增强方案，以保证计算机网络自身的安全为目标。

商务交易安全则紧紧围绕传统商务在互联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，保障以电子交易和电子支付为核心的电子商务的顺利进行。即实现电子商务保密性、完整性、可鉴别性、不可伪造性和不可抵赖性等。

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，商务交易安全就犹如空中楼阁，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。

电子商务安全以网络安全为基础，但是，电子商务安全与网络安全又是有区别的。首先，网络不可能绝对安全，在这种情况下，还需要在其之上运行安全的电子商务；其次，即使网络绝对安全，也不能保障电子商务的安全。所以，电子商务安全除了基础要求之外，还有特殊要求。

从安全等级来说，由下至上有密码安全、局域网安全、互联网安全和信息安全之分，而电子商务安全属于信息安全的范畴，涉及信息的机密性、完整性、认证性等方面。这几个安全概念之间的关系如图 1-1 所示。同时，电子商务安全又有它自身的特殊性，即以电子交易安全和电子支付安全为核心，有更复杂的机密性概念，更严格的身份认证功能，对不可拒绝性有新的要求，有法律依据性和货币直接流通性特点，还有网络特有的其他服务功能（如数字时间戳服务）等。

2. 电子商务安全特点

电子商务安全具有如下四大特点：

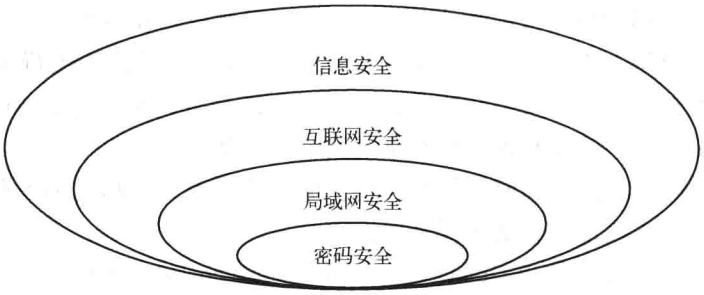

图 1-1　电子商务安全基本关系示意图

（1）电子商务安全是一个系统概念

电子商务安全问题不仅仅是个技术性的问题，更重要的是管理问题，而且它还与社会道德、行业管理以及人们的行为模式都紧密地联系在一起。

（2）电子商务安全是相对的

就像家里的房子安上防盗门后，一般说来就相对安全了，但是小偷非要用专门的工具去破坏或打开，那防盗门也就不安全了，但我们不会因为防盗门能被小偷破坏或打开而怀疑它的安全性，防止小偷破坏或打开防盗门还需要相应的管理机制。同样，不能追求一个永远也攻不破的安全系统，安全与管理始终是联系在一起的。也就是说，安全是相对的，而不是绝对的，要想以后的网站永远不受攻击、不遇到安全问题是不可能的。

（3）电子商务安全是有代价的

要维护电子商务安全，就必须有一定的资金投入，包括购买安全设备、安装安全软件等。作为一个电子商务应用者，应该综合考虑安全技术的成本，作为安全技术提供者，在研发技术时也要考虑到成本代价问题。

（4）电子商务安全是发展的、动态的

今天安全，明天不一定安全，因为网络的攻防是此消彼长、道高一尺魔高一丈的事情，尤其是网络安全技术，它的敏感性、竞争性以及对抗性很强，需要不断地检查、评估和调整相应的安全策略。没有一劳永逸的电子商务安全，也没有一蹴而就的电子商务安全。

1.1.2　电子商务面临的安全威胁

要了解电子商务面临的安全威胁，需要考查从客户机到电子商务服务器的整个过程。在考查“电子商务链”上每个逻辑链条时，可以看出，必须保护的资产包括客户机、在通信信道上传输的消息、Web 和电子商务服务器（包括服务器端所有的硬件）等。

1. 对客户机的安全威胁

在实时的、动态的、可交互的 Web 内容出现前，网页是静态的。静态页面是用 Web 标准页面描述语言 HTML 编制的，其作用只是向客户机提供显示内容并链接到其他页面。为了增加页面的生动性以及客户机与服务器之间的交互能力，同时也为了分担服务器端的负载，动态网页技术得以广泛应用，相应地网页的安全状态也随之发生了变化。客户机面临的安全威胁主要是以动态页面形式从网上传来的活动内容带来的安全威胁，还有一些非法网站，伪装成合法网站，诱骗用户提供敏感信息，使得用户信息被盗取等。此外，一些其他的相关技术也成为威胁客户机安全的不确定性因素，如被 Java、JavaScript、Active X 等控件恶

意利用，也会招致病毒、蠕虫等感染。

（1）动态网页内容

动态网页内容是指在页面上嵌入一段对用户透明的程序，它可实现一些动态的效果，例如显示动态图像、下载和播放音乐或实现基于 Web 的电子表格程序、客户机中的表单数据提交等交互操作。动态网页内容扩展了 HTML 的功能，使页面更为生动活泼。同时，动态网页内容还将原来要在服务器上完成的某些辅助性处理任务转给在多数情况下处于闲置状态的客户机来完成，均衡了服务器的负载。

动态网页有多种形式，最著名的动态网页形式包括 JavaScript 和 VBScript、Java Applet 和 ActiveX 控件等。这些程序经常被企图破坏客户机的人伪装成无害的内容，一旦触发运行，就会对客户机带来安全威胁。这种隐藏在程序或页面里而掩盖其真实目的的程序统称为“特洛伊木马”。它可窃听计算机上的保密信息，并将这些信息传给它的远程 Web 服务器，从而构成保密性侵害。而且，特洛伊木马还可改变或删除客户机上的信息，构成完整性和不可拒绝性侵害。

（2）相关技术或机制

能够威胁客户机安全的因素，除了动态网页内容，还包括其他一些相关技术或机制。这些技术或机制和动态网页内容相呼应，使得其对客户机的安全威胁势态扩大，使得后果更加严重。

1）cookie。因为互联网是无状态的连接，它不能记忆从一个页面到另一个页面间的响应，所以网站设计时利用 cookie 进行服务器与客户机之间的连续连接（也称公开会话），目的是解决需要记忆关于顾客订单信息、用户名与口令、购物车与结算处理软件的公开会话等问题。Cookie 的使用给有些恶意的动态内容提供了可乘之机，一些页面嵌入的恶意代码也使存放在 cookie 里的信用卡号、用户名和口令等敏感信息容易暴露。

2）邮件通信簿。使用邮件客户端收发邮件的用户通常在电子邮件通信簿上存放联系人的信息，一些计算机病毒可以成功地检测到这些内容，并通过互联网把自己发给这些联系人，其传播难以得到有效的扼制。

3）信息隐蔽。一般情况下，计算机文件中都有冗余的或能为其他信息所替代的无关信息。黑客会利用信息隐蔽技术隐藏他们在网络上的活动，甚至能不被杀毒软件检测出来。信息隐蔽是指隐藏在另一段信息中的信息，它提供将加密的文件隐藏在另一个文件中的保护方式，粗心的观察者看不到其中含有的重要信息。

2. 对通信信道的安全威胁

互联网是将客户机和电子商务服务器连接起来的电子通道。在已了解对客户机的安全威胁后，所要考虑的第二个环节就是将客户机连到服务器上的传输信道，即互联网。

虽然互联网起源于军事网络，但美国国防部高级研究项目中心建造这个网络的主要目的不是为了安全传输，而是为防止一个或多个通信线路被切断之后仍有通信信道可供使用，即提供冗余传输。互联网发展到今天，其不安全状态与最初相比并没有多大改观。在互联网上传输的信息，从起始节点经由若干中间节点到目标节点之间的路径是随机选择的。在同一起始节点和目标节点之间发送信息时，每次所用的路径也都是不同的，所以根本无法控制信息的传输路径，也不知道信息包曾到过哪里，因而无法保证信息传输时所通过的每台计算机都是安全的和无恶意的。如果在信息包传递途中被任意一个中间节点窃取、篡改甚至删除了用

户的信息，那么客户所遭受的损失将是无法弥补的。

（1）搭线窃听

电子商务的一个很大的安全威胁就是敏感信息或个人真实信息被窃。在互联网上，有种叫做“嗅探器”的特殊软件能够记录下通过某个网关或路由器的信息。它类似于在电话线上搭线并录下一段对话。嗅探器可以截获并阅读电子邮件信息，也可记录敏感信息或个人真实信息，或者用来攻击相邻的网络，并且能够做到不留痕迹。

（2）IP 欺骗

所谓 IP 欺骗，就是伪装成合法主机的 IP 地址与目标主机建立连接关系。通过这种欺骗方法可以把某个服务器的访问者引到一个虚假网站，或者假冒合法用户主机名进入目标服务器。

当用户主机与目标服务器之间建立了 TCP（Transmission Control Protocol，传输控制协议）连接后，通过双方信息包的不断交互取得用户主机或服务器的信息。入侵者猜测出信息包的序列号，就能够向用户主机或服务器发出伪造的、看上去是来自合法主机的数据包，构成对完整性的威胁。

此外，用户主机与服务器之间建立网络连接时经常需要某种形式的认证，发生在应用层上的认证是不透明的，如进行 FTP 或 Telnet 连接时需要用户输入密码和账号。IP 地址欺骗可以针对非应用层的、通常是自发的、无需用户参与的认证，从而达到非法入侵的目的。

（3）IP 源端路由选择

IP 数据包在互联网上传输到达最终目的主机之前通常要经过许多路由器。路由器动态决定了 IP 数据包的传输路线。允许源端路由选择就是允许 IP 数据包向经过的路由器声明到达目标主机所希望经过的路由。

入侵者利用 IP 数据包源端路由选择避开那些包含过滤路由器、防火墙以及其他安全检查机制的路由，就可以访问在正常情况下所不能访问的主机。另外，如果目标主机的访问控制机制是认证源主机的 IP 地址，入侵者使用 IP 源端路由选择就可以有效地通过目标主机的认证。

（4）目标扫描

入侵者在确定扫描目标系统后，利用一些扫描程序和安全分析工具，如 IIS（Internet Information Server）漏洞扫描器、SATAN（Security Administrator Tool ForAnalyzing Networks）网络分析工具等，寻求该系统的安全漏洞或弱点，并试图找到安全性最弱的主机作为入侵的对象。如果目标主机的管理员系统配置不当，或者未能及时发现并更新针对产品或系统安全漏洞的补丁程序，安全薄弱的主机就极易被攻破，继而造成对与本机建立了访问链接和信任关系的其他网络计算机被攻破的连锁反应，最终威胁到整个系统。

3. 对服务器的安全威胁

客户机、互联网和服务器的电子商务链上第三个环节是服务器。企业借助各种服务器软件设置自己的 Web 服务器、FTP 服务器、E-Mail 服务器等。对企图破坏或非法获取信息的人来说，服务器有很多弱点可被利用。其中的攻击入口是 Web 服务器及其软件、数据库和数据库服务器以及通用网关接口 CGI（Common Gateway Interface）程序或其他工具程序。