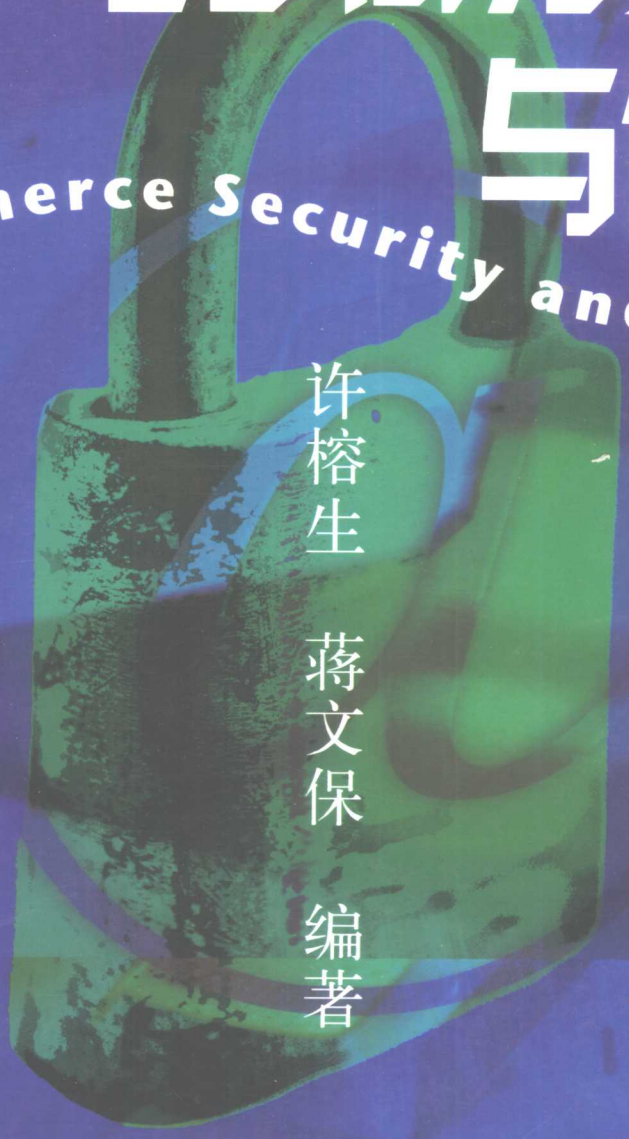
中科院“黑客入侵防范体系”课题组

电子商务安全与保密

E-Commerce Security and Privacy



许榕生 蒋文保 编著

中国电力出版社
www.cepp.com.cn

电子商务安全与保密
中国电力出版社

电子商务安全与保密

许榕生　蒋文保 编著

中国电力出版社
www.cepp.com.cn

内 容 提 要

随着电子商务的迅速发展，基于 Internet 的电子商务所面临的各种安全问题也正逐渐成为业内人士所关注的热点。

本书围绕电子商务活动所涉及的安全问题，全面深入地讲述了各种相关的信息安全技术及网络安全解决方案，主要包括加密技术、认证技术、电子商务安全认证体系、安全电子交易技术、网络安全与黑客防范技术、操作系统安全问题、Internet 服务及其安全性分析。

本书适合从事电子商务及其研究的各界人士、网络安全研究人员及高等院校相关专业的研究生。

图书在版编目（CIP）数据

电子商务安全与保密/许榕生，蒋文保编著.-北京：中国电力出版社，2001

ISBN 7-5083-0526-4

Ⅰ.电… Ⅱ.①许…②蒋… Ⅲ.电子商务—安全技术 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字（2001）第 03757 号

中国电力出版社出版、发行

（北京三里河路 6 号 100044 http://www.cepp.com.cn）

三河实验小学印刷厂印刷

各地新华书店经售

*

2001 年 6 月第一版 2001 年 6 月北京第一次印刷

787 毫米×1092 毫米 16 开本 21.25 印张 481 千字

定价 33.00 元

前　言

在 20 世纪末，由于计算机和网络技术的迅速发展和普及，人们再一次感受到了科学技术发明及其应用给人类社会带来的根本性影响。当人类跨入 21 世纪时，人们预期的信息时代已经不折不扣地展现在世人前面。如今的信息时代是一个以计算机网络为主的信息时代，或者更准确地说，是一个以 Internet 为主的信息时代。Internet 对现代人的影响可以说是无比博大而深远的，它不但正在改变着人们日常的生活、工作、学习和娱乐方式，也必将给整个人类社会的经济、政治和文化带来革命性的影响。

电子商务的迅速发展就是 Internet 对人类社会巨大影响的一个重要表现。虽然电子商务不是 Internet 的专利，因为从广义上说只要借助于电子信息及通信手段进行的商务都可以算是电子商务；但是，基于 Internet 的电子商务才是具有现代意义的电子商务，也只有借助于 Internet，电子商务才能具有旺盛的生命力。随着 Internet 技术的迅猛发展和广泛应用，电子商务作为一种崭新的商业运作模式，在现代经济活动中具有举足轻重的地位。它不仅是现代企业参与竞争、提高经济效益的重要手段，而且也直接关系到每个国家未来的经济竞争力与综合国力。因此，世界上重要国家的政府都非常重视电子商务的发展，我国政府也不例外。无疑，电子商务的发展与推广将使我国加速实现经济的腾飞和社会科技的进步，并将极大地促进社会主义精神文明和物质文明建设。

Internet 之所以能发展成为今天的全球性网络，主要依赖于它的开放性。但是，这种开放式的信息交换方法使其网络安全具有很大的脆弱性。因此，基于 Internet 开展的电子商务虽然前景十分诱人，但其安全问题也变得越来越突出。毫无疑问，与一般性的信息交流活动相比，商务活动对 Internet 提出了更高的安全需求。如何建立一个安全、便捷的电子商务应用环境，保证整个商务过程中信息的安全性，使基于 Internet 的电子交易方式与传统交易方式一样安全可靠，已经成为人们十分关心的热门话题。据权威机构调查表明，目前国内企业发展电子商务的最大顾虑是安全问题。因此，信息的安全性是当前发展电子商务最迫切需要研究和解决的问题。不过，我们要提醒读者的是，虽然目前安全问题是一个敏感而突出的问题，但它并不注定就是电子商务发展的致命点。随着信息技术的进一步发展，业界人士在 Internet 安全方面所进行的种种努力，已经逐渐改善了现代电子商务的安全环境。我们有理由相信，通过大家的努力，基于 Internet 的电子商务所面临的各种安全问题，必然都将会得到比较圆满的解决。

本书围绕电子商务活动所涉及的安全问题，全面深入地讲述了各种相关的信息安全技术及网络安全解决方案，主要包括加密技术、认证技术、电子商务安全认证体系、安全电子交易技术、网络安全与黑客防范技术、操作系统安全问题、Internet 服务及其安全性分析。

本书第 1 章是关于电子商务安全问题的总体概述，目的是为了读者对本书所讨论的电子商务安全保密技术有一个总体概要的认识。

第 2 章介绍加密技术。加密技术是电子商务采取的基本安全技术手段。采用加密技术可以满足信息保密性的安全需求，避免敏感信息泄露的安全威胁。可以说。加密技术是认证技术及其他许多安全技术的基础，也是信息安全的核心技术。

第 3 章专门讨论认证技术。认证技术是信息安全理论与技术的一个重要方面，也是电子商务安全的主要实现技术。采用认证技术可以直接满足身份认证、信息完整性、不可否认和不可修改等多项网上交易的安全需求，较好地避免了网上交易面临的假冒、篡改、抵赖、伪造等种种威胁。

第 4、5 章中，讲述了当前电子商务实践中所采用的一整套安全解决方案，主要包括电子商务安全认证体系和安全电子交易技术，可以说，这是电子商务安全的主体内容。其中，第 4 章所讨论的电子商务安全认证体系，实际上就是一套融合了各种先进的加密技术和认证技术的安全体系，它主要定义和建立身份及报文认证和授权规则，然后分发、交换这些规则，并在网络之间解释和管理这些规则。因为电子交易是电子商务活动中的核心内容，所以第 5 章介绍的安全电子交易技术是电子商务安全技术中极其重要的内容。如何在开放的公用网上构筑安全的交易模式，一直是业界研究的热点和大家关注的话题。毫无疑问，也只有建立在各种加密技术和认证技术的基础上，才有可能构筑一个安全的电子交易模式。

本书从第 6 章开始讲述的内容，涉及到的是一般的、普遍性的网络安全话题，它们是基于 Internet 电子商务安全的基础。其中，第 6 章所讨论的网络黑客话题已成为当今全社会的热门话题。目前黑客攻击已成为网络安全所面临的最大威胁，同时黑客防范技术也是网络安全的主要内容。在这一章中，我们较为详细地介绍了黑客技术，即黑客入侵常使用的一些技术。因为为了有效地防范黑客恶意的入侵行为，就必需首先掌握黑客技术，也只有很好地掌握了黑客技术，才有可能在与恶意黑客的战斗中做到“知彼知己，百战不殆”。当然，本章的重点仍放在反黑客技术的论述中，主要包括网络安全评估技术、防火墙技术、入侵检测技术等内容。

如果从技术角度更细更深地探究许多网络安全问题，我们就会发现它们很多都可归源为计算机操作系统层次上的安全问题。实际上，计算机操作系统的安全是网络安全的基础，因而也是电子商务安全的一个重要组成部分。所以，第 7 章专门讨论了常用操作系统的一些安全问题。

在本书的最后一章（第 8 章）中，我们简要地分析了 Internet 提供的各种服务及其安全性。Internet 可提供的服务是多种多样的，但这一章只涉及目前最常用的一些服务，包括电子邮件（E_mail）服务、远程登录（Telnet）服务、文件传输（Ftp）服务和 Web 服务。值得注意的是，网络服务一般都是通过各种各样的协议形式完成的，而网络协议的安全性则很难得到绝对保证，网络协议的漏洞也是当今 Internet 面临的一个严重安全问题。实际上，安全协议一直是网络安全领域的重要研究内容。

随着信息时代的到来，计算机网络对我们工作和生活必将愈来愈重要。同时，网络黑客现象也越来越成为人们关注的焦点。如今，无论是个人、企业、还是政府机构，只要进入计算机网络，都会感受到黑客带来的网络安全威胁。大至国家机密，小到个人隐私，还有商业秘密，都随时可能被黑客发现并作非法之用。目前，黑客防范技术受到了各国政府

和网络业界的高度重视。为了寻找一整套有效防范黑客攻击的手段和方法， 中国科学院高能物理研究所在许榕生研究员的带领下，承担了中国科学院知识创新工程项目子项目——“黑客防范体系”。虽然目前该项目还处于初期的研发阶段，但相信本书的编写是一种有益的尝试，并有利于今后的研究开发工作。

本书主要由许榕生、蒋文保编写，并由蒋文保策划，许榕生统稿。第 6 章和第 8 章的内容主要由杨泽明编写。钱桂琼在资料收集和录入方面做了许多工作。另外，在本书的编写过程中，中国科学院高能物理研究所“黑客入侵防范体系”课题组，以及计算中心的许多同事都给予了大力的支持，作者在此表示衷心的感谢。

在本书编写过程中，参考了很多网上的资料，包括《计算机世界》、《网络世界》等国内多种 IT 报刊的在线版，相关厂家和服务机构的各种网站，以及国内外一些黑客及其组织建立的形形色色的站点，在此谨向有关的作者表示感谢。

在本书的出版过程中，责任编辑王惠娟给予了我们大力的支持，并提出了许多良好的建议，她认真负责的工作态度令人敬佩。我们在此向她表示诚挚的感谢。

由于时间仓促，加上电子商务安全技术是一个较新的研究领域，因此本书错误之处在所难免，欢迎广大读者批评指正。

编者

2000 年 10 月

目　录

第 1 章　电子商务安全概述

随着信息技术日新月异的发展，人类正在进入以网络为主的信息时代，基于 Internet 开展的电子商务已逐渐成为人们进行商务活动的新模式。越来越多的人通过 Internet 进行商务活动，电子商务的发展前景十分诱人，但随之而来的是其安全问题也变得越来越突出。如何建立一个安全、便捷的电子商务应用环境，保证整个商务过程中信息的安全性，使基于 Internet 的电子交易方式与传统交易方式一样安全可靠，已经成为大家十分关心的热门话题。据权威机构调查表明，目前国内企业发展电子商务的最大顾虑是安全问题。因此，信息的安全性是当前发展电子商务最迫切需要研究和解决的问题。

Internet 之所以能发展成为今天的全球性网络，主要是依赖于它的开放性。但是，这种开放式的信息交换方法使其网络安全具有很大的脆弱性。不过，随着信息技术的进一步发展，人们在 Internet 安全上所进行的努力已经逐渐改变了这种情况。我们有理由相信，通过大家的努力，基于 Internet 的电子商务所面临的各种安全问题，必然都将会得到圆满的解决。

本章首先从分析电子商务面临的各种安全性威胁出发，讨论了基于 Internet 进行的电子商务活动提出的安全需求。在此基础上，我们将概要地介绍目前业界用于电子商务的一些基本安全保密技术，目的是为了让读者对本书所讨论的电子商务安全保密技术先有一个总体概要的认识。

1.1　电子商务的安全需求

一、电子交易的安全需求

电子商务安全问题的核心和关键是电子交易的安全性，因此，下面我们首先讨论在 Internet 上进行商务交易过程中的安全问题。由于 Internet 本身的开放性以及目前网络技术发展的局限性，使网上交易面临着种种安全性威胁，也由此提出了相应的安全控制要求。

（1）身份的可认证性

在传统的交易中，交易双方往往是面对面进行活动的，这样很容易确认对方的身份。即使开始不熟悉、不能确信对方，也可以通过对方的签名、印章、证书等一系列有形的身份凭证来鉴别他的身份。另外，在传统的交易中如果是采用电话进行通信，也可以通过声音信号来识别对方身份。然而，在进行网上交易时，情况就大不一样了，因为网上交易的双方可能素昧平生，相隔千里，并且在整个交易过程中都可能不见一面。因此，如果不采取任何新的保护措施，就要比传统的商务更容易引起假冒、诈骗等违法活动。例如，在进行网上购物时，对于客户来说，如何确信计算机屏幕上显示的页面就是大家所说的那个有

名的网上商店，而不是居心不良的黑客冒充的呢？同样，对于商家来说，怎样才能相信正在选购商品的客户不是一个骗子，而是一个当发生意外事件时能够承担责任的客户呢？

因此，电子交易的首要安全需求就是要保证身份的可认证性。这就意味着，在双方进行交易前，首先要能确认对方的身份,要求交易双方的身份不能被假冒或伪装。

（2）信息的保密性

在传统的贸易中，一般都是通过面对面的信息交换，或者通过邮寄封装的信件或可靠的通信渠道发送商业报文，达到保守商业机密的目的。而电子商务是建立在一个开放的网络环境上，当交易双方通过 Internet 交换信息时，因为 Internet 是一个开放的公用互联网络，如果不采取适当的保密措施，那么其他人就有可能知道他们的通信内容；另外，存储在网络上的文件信息如果不加密的话，也有可能被黑客窃取。上述种种情况都有可能造成敏感商业信息的泄露，导致商业上的巨大损失。例如，如果客户的信用卡的账号和用户名被人知悉，就可能被盗用；如果企业的订货和付款的信息被竞争对手获悉，就可能丧失商机。

因此，电子商务另一个重要的安全需求就是信息的保密性。这意味着，一定要对敏感信息进行加密，即使别人截获或窃取了数据，也无法识别信息的真实内容，这样就可以使商业机密信息难以被泄露。

（3）信息的完整性

上面所讨论的信息保密性，是针对网络面临的被动攻击一类威胁而提出的安全需求，但它不能避免针对网络所采用的主动攻击一类的威胁。所谓被动攻击，就是不修改任何交易信息，但通过截获、窃取、观察、监听、分析数据流和数据流模式获得有价值的情报。而主动攻击就是篡改交易信息，破坏信息的完整性和有效性，以达到非法的目的。例如，在电子贸易中，乙给甲发了如下一份报文：“请给丁汇一百元钱。乙”。报文在转发过程中经过了丙之手，丙就把“丁”改为“丙”。这样甲收到后就成了“请给丙汇一百元钱。乙”，结果是丙而不是丁得到了这一百元钱。当乙得知丁未收到钱时就去问甲，甲出示有乙签名的报文，乙发现报文被篡改了。

因此，保证信息的完整性也是电子商务活动中的一个重要的安全需求。这意味着，交易各方能够验证收到的信息是否完整,即信息是否被人篡改过，或者在数据传输过程中是否出现信息丢失、信息重复等差错。

（4）不可抵赖性

由于商情千变万化，交易合同一旦达成就不能抵赖。在传统的贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章，确定合同、契约、单据的可靠性并预防抵赖行为的发生，这也就是人们常说的“白纸黑字”。但在无纸化的电子交易中，就不可能再通过传统的手写签名和印章来预防抵赖行为的发生。因此，必须采用新的技术，防止电子商务中的抵赖行为，否则就会引起商业纠纷，使电子商务无法顺利进行。例如，在电子商务活动中订购冰箱时，如果订货时冰箱价格较低，但收到订单后，冰箱价格上涨了，假如供应商能否认收到订单的事实，则采购商就会蒙受损失；同样，如果收到订单后，冰箱价格下跌了，假如订货方能否认先前发出订货单的事实，则供应商就会蒙受

损失。

因此，保证交易过程中的不可抵赖性也是电子商务安全需求中的一个重要方面。这意味着，在电子交易通信过程的各个环节中都必须是不可否认的，即交易一旦达成，发送方不能否认他发送的信息，接收方则不能否认他所收到的信息。

（5）不可伪造性

在商务活动中，交易的文件是不可被修改的，如上例所举的订购冰箱一案，如果供应商在收到订单后，发现冰箱价格大幅上涨了，假如能改动文件内容，将订购数 100 台改为 10 台，则可大幅受益，那么采购商就会因此而蒙受巨大损失。在传统的贸易中，可以通过合同字迹的技术鉴定等措施来防止交易过程中出现的伪造行为，但在电子交易中，由于没有书面的合同，因而无法采用字迹的技术鉴定等传统手段来裁决是否发生了伪造行为。

因此，保证交易过程中的不可伪造性也是电子商务安全需求中的一个方面。这意味着，电子交易文件也要能做到不可修改，以保障交易的严肃和公正。

二、计算机网络系统的安全问题

在公用互联网 Internet 上进行电子商务活动时，除了在交易过程中会面临上述一些特殊的安全性问题外，毫无疑问，还会涉及到一般计算机网络系统普遍面临的一些安全问题。威胁计算机网络安全的因素很多，有些因素可能是有意的，有些因素可能是无意的；有些因素可能是人为的，有些因素可能是非人为的。归结起来，针对网络安全的主要问题有如下几种。

（1）物理实体的安全问题

物理实体的安全问题主要包括以下几种。

1）设备的机能失常。任何一种设备都不是十全十美、万无一失的，或多或少都存在着这样或那样的缺陷。有时会出现一些比较简单的故障，而有些则是灾难性的。有些简单故障，特别是周期性故障，往往比那些大的故障更难于查找与修复。有些故障是当它们已经破坏了系统数据或其他设备时才被发现，而这时往往为时已晚，后果也是非常严重的。

2）电源故障。由于各种意外的原因，网络设备的供电电源可能会突然中断或者产生较大的波动，这可能会突然中断计算机系统的工作。如果这时正在进行某些数据操作，这些数据很可能会出错或丢失。另外，突然断电对系统硬件设备也会产生不良后果。

3）由于电磁泄漏引起的信息失密。计算机和其他一些网络设备大多数都是电子设备，当它工作时会产生电磁泄漏。一台计算机就像一部电台，带有信息的电磁波向外辐射，尤其视频显示装置辐射的信息量最强，用先进的电子设备在一公里之外的地方就能接收下来。另外，电子通信线路同样也有辐射。这样，非法之徒就可以利用先进的接收设备窃取网络机密信息。

4）搭线窃听。这是非法者常用的一种手段，将导线搭到无人值守的网络传输线路上进行监听，通过解调和正确的协议分析可以完全掌握通信的全部内容。

（2）自然灾害的威胁

计算机网络设备大多是一种易碎品，不能受重压或强烈的震动，更不能受强力冲击。所以，各种自然灾害，如地震、风暴、泥石流、建筑物破坏等，对计算机网络系统构成了严重的威胁。另外，计算机设备对环境的要求也很高，如温度、湿度、各种污染物的浓度，等等，所以要特别注意像火灾、水灾、空气污染等对计算机网络系统所构成的威胁。

（3）黑客的恶意攻击

今年初，全世界传媒都在关注美国著名网站被袭事件。在这次事件中，包括雅虎、亚马逊书店、eBay、ZDNet、有线电视新闻网 CNN 在内的美国主要网站接连遭到黑客的攻击。这些网站被迫中断服务数小时，据估算，造成的损失达到 12 亿美元以上。这次袭击事件不仅使著名商业网站蒙羞，更使公众对网络安全的信心受到重创。

所谓黑客，现在一般泛指计算机信息系统的非法入侵者。黑客的出现可以说是当今信息社会，尤其是在 Internet 互联全球的过程中，网络用户有目共睹、不容忽视的一个独特现象。黑客们在世界各地四处出击，寻找机会袭击网络几乎到了无孔不入的地步。黑客攻击目前已成为计算机网络所面临的最大威胁。如今，无论是个人、企业、还是政府机构，只要进入计算机网络，都会感受到黑客带来的网络安全威胁。大至国家机密，小到个人隐私，还有商业秘密，都随时可能被黑客发现并公布。

根据美国军方的一份报告透露：1998 年试图侵入五角大楼计算机网络系统的尝试达 25 万次之多，其中 60%的尝试成功达到了目的。五角大楼计算机网络中的数据涉及到诸如部队调动、武器采购和维护等事关国家安全的非常敏感的信息。由此可见，黑客袭击的潜在危险是何等的巨大。1998 年，由于黑客的入侵，世界范围内的主要银行和大公司损失了大约 8 亿美元，其中美国约占 4 亿美元。近几年，美国政府的计算机系统平均每年遭到非法侵入的次数至少有 30 万次，其中犯罪行为引起的损失估计可达 15 亿美元。

黑客的攻击手段和方法多种多样，一般可以粗略的分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。

（4）软件的漏洞和“后门”

随着现代软件系统的越来越复杂，对于一个软件，特别是较大的系统或应用软件来讲，要想进行全面彻底的测试已经变得越来越不可能了。虽然在设计与开发一个大型软件的过程中可以进行某些测试，但总是会多多少少留下某些缺陷和漏洞，这些缺陷可能长时间也发现不了，而只有当被利用或某种条件得到满足时，才会显现出来。目前最常用的一些大型的软件系统，例如 Windows 98、Windows 2000 和一些 UNIX 系统软件，以及 MS Internet Explorer 和 Netscape Communicator 等大型应用软件，都不断被用户发现有这样或那样的安全漏洞。另外，软件的“后门”都是软件公司的设计和编程人员为了自便而设置的，一般不为外人所知，但一旦“后门”洞开，其造成的后果将不堪设想。

（5）网络协议的安全漏洞

网络服务一般都是通过各种各样的协议完成的，因此网络协议的安全性是网络安全的

一个重要方面。如果网络通信协议存在安全上的缺陷，那么敌手就有可能不必攻破密码体制即可获得所需要的信息或服务。值得注意的是，网络协议的安全性是很难得到绝对保证的。目前协议安全性的保证通常有两种方法：一种是用形式化方法来证明一个协议是安全的；另一种是设计者用经验来分析协议的安全性。形式化证明的方法是人们所希望的，但一般的协议安全性也是不可判定的，所以对复杂的通信协议的安全性，现在主要采用找漏洞分析的方法。无疑，这种方法有很大的局限性。实践证明，目前 Internet 提供的一些常用服务所使用的协议，例如，Telnet、FTP 和 HTTP 协议，在安全方面都存在一定的缺陷。当今许多黑客攻击都是利用了这些协议的安全漏洞才得逞的。实际上，网络协议的漏洞是当今 Internet 面临的一个严重安全问题。

（6）计算机病毒的攻击

信息技术的飞速发展虽然极大地推动了计算机和网络的普及，但同时也大大地促进了计算机病毒的发展，给人们日常生活和工作带来了许多不便，甚至造成巨大的损失。据 ICSA（International Computer Security Association，国际计算机安全协会）1999 年对各大企业进行的抽样调查结果显示，病毒感染、发作率在近年有增无减，1999 年计算机受病毒感染的概率是 80‰，而 1998 年同期的概率是 32‰。据统计，现在的病毒有数万种之多，而且还在以每月产生数百种的速度急剧地增长。因此，保护有价值的数据不受病毒破坏，已经成为一项非常重要而又非常艰巨的工作。

什么是病毒？计算机病毒(Computer Virus)在《中华人民共和国计算机信息系统安全保护条例》中被明确定义为："指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码"。

目前全球出现的数万种病毒按照基本类型划分，可归为 6 种类型：引导型病毒、可执行文件病毒、宏病毒和混合病毒、特洛伊木马型病毒、INTERNET 语言病毒。关于各种病毒的论述，读者可以参看其他文献，这里不多作介绍。

计算机病毒作为一种具有破坏性的程序，往往想尽一切手段将自身隐藏起来，保护自己；但是病毒最根本的目的还是达到其破坏目的，在某些特定条件被满足的前提下，病毒就会发作，这也就是病毒的破坏性。病毒的破坏性有些只是显示一些图片、放一段音乐或和你开个玩笑，这类病毒就是良性病毒；而有些病毒则含有明确的目的性，象破坏数据、删除文件、格式化磁盘等，这类病毒就是恶性病毒。计算机病毒的破坏行为体现了病毒的杀伤能力，病毒破坏行为的激烈程度取决于病毒作者的主观愿望和他所具有的技术能量。根据有关的病毒资料，可以把病毒的破坏目标和攻击部位归纳如下：

1）攻击系统数据区。攻击部位包括：硬盘主引导扇区、Boot 扇区、FAT 表、文件目录。一般来说，攻击系统数据区的病毒是恶性病毒，受损的数据不易恢复。

2）攻击文件。病毒对文件的攻击方式很多，可列举如下：删除、改名、替换内容、丢失部分程序代码、内容颠倒、写入时间空白、变碎片、假冒文件、丢失文件簇、丢失数据文件。

3）攻击内存。内存是计算机的重要资源，也是病毒的攻击目标。病毒额外地占用和消

耗系统的内存资源，可以导致一些大程序受阻。病毒攻击内存的方式如下：占用大量内存、改变内存总量、禁止分配内存、蚕食内存。

4）干扰系统运行。病毒会干扰系统的正常运行，以此做为自己的破坏行为。此类行为也是花样繁多，可以列举下述诸方式：不执行命令、干扰内部命令的执行、虚假报警、打不开文件、内部栈溢出、占用特殊数据区、换现行盘、时钟倒转、重启动、死机、强制游戏、扰乱串并行口。

5）速度下降。病毒被激活时，其内部的时间延迟程序启动。在时钟中纳入了时间的循环计数，迫使计算机空转，计算机速度明显下降。

6）攻击磁盘。攻击磁盘数据、不写盘、写操作变读操作、写盘时丢字节。

7）扰乱屏幕显示。病毒扰乱屏幕显示的方式很多，可列举如下：字符跌落、环绕、倒置、显示前一屏、光标下跌、滚屏、抖动、乱写、吃字符。

8）键盘。病毒干扰键盘操作，已发现有下述几种方式：响铃、封锁键盘、换字、抹掉缓存区字符、重复、输入紊乱。

9）喇叭。许多病毒运行时，会使计算机的喇叭发出响声。有的病毒作者让病毒演奏旋律优美的世界名曲，在高雅的曲调中去杀戮人们的信息财富。有的病毒作者通过喇叭发出种种声音。已发现的有以下方式：演奏曲子、警笛声、炸弹噪声、鸣叫、咔咔声、嘀嗒声

10）攻击 CMOS。在机器的 CMOS 区中，保存着系统的重要数据。例如，系统时钟、磁盘类型、内存容量等，并具有校验和。有的病毒被激活时，能够对 CMOS 区进行写入动作，破坏系统 CMOS 中的数据。

11）干扰打印机。假报警、间断性打印、更换字符。

1.2 电子商务基本安全保密技术

针对前面介绍的电子商务所面临的安全性威胁，以及由此提出的安全需求，迄今为止，国内外学术界和相关厂商已提出了很多相应的解决方案，并且基本上满足了人们在 Internet 上开展安全的电子商务活动的愿望。在许许多多的解决方案中，涉及到的安全保密技术主要有加密技术、认证技术、CA 安全认证体系、安全电子交易协议、虚拟专用网技术、反病毒技术、黑客防范及其他相关的网络安全技术。下面分别简要加以介绍。

一、加密技术

加密技术是电子商务采取的主要安全技术手段。采用加密技术可以满足信息保密性的安全需求，避免敏感信息泄露的威胁。通常信息加密的途径是通过密码技术实现的，密码技术是保护信息的保密性、完整性、可用性的有力手段，它可以在一种潜在不安全的环境中保证通信及存储数据的安全，密码技术还可以有效地用于报文认证、数字签名等，以防止种种电子欺骗。可以说，加密技术是认证技术及其他许多安全技术的基础，也是信息安全的核心技术。

密码技术包括密码设计、密码分析、密钥管理、验证技术等内容。密码设计的基本思想是伪装信息，使局外人不能理解信息的真正含义，而局内人却能够理解伪装信息的本来含义。其中，密码设计的中心内容就是数据加密和解密的方法。所谓“加密”，简单地说，就是使用数学的方法将原始信息（明文）重新组织与变换成只有授权用户才能解读的密码形式（密文），而“解密”就是将密文重新恢复成明文。密码的出现可以追溯到远古时代，密码学也和其他学科一样随着社会的发展而发展，先后经历了手工阶段、机械阶段、电子阶段，而现在则进入了计算机和网络时代。目前，密码学已发展成一门系统的技术科学，是集数学、计算机科学、电子与通信等诸多学科于一身的交叉学科。根据不同的标准，密码体制的分类方法很多，其中常用的主要有对称密码体制（也叫作单钥密码体制、秘密密钥密码体制、对称密钥密码体制）、非对称密码体制（也叫作双钥密码体制、公开密钥密码体制、非对称密钥密码体制）等。

在对称密码体制中，加密密钥与解密密钥是相同的。早期使用的加密算法大多是对称密码体制,所以对称密码体制通常也称作传统密码体制，或常规密码体制。在这种密码体制下，有加密（或解密）的能力就意味着必然也有解密（或加密）的能力。对称密码体制的优点是具有很高的保密强度，可以达到经受国家级破译力量的分析和攻击，但它的密钥必须通过安全可靠的途径传递。由于密钥管理成为影响系统安全的关键性因素，使它难以满足系统的开放性要求。

为了解决对称密码体制的密钥分配问题，以及满足对数字签名的需求，20 世纪 70 年代产生了非对称密码体制。在这种密码体制下，人们把加密过程和解密过程设计成不同的途径，当算法公开时，在计算上不可能由加密密钥求得解密密钥，因而加密密钥可以公开，而只需秘密保存解密密钥即可。在非对称密码体制中，最具代表性的算法当数 RSA，它从 1978 年公布至今，一直是加密算法中的主要算法之一。尽管该算法吸引了无数研究者，但在数学上还未找到最佳破译方法。其他的非对称密码体制，有些虽很著名，但已被破译，如背包体制；有些还处于研究和发展阶段，如椭圆曲线体制；有些密码体制在算法上与 RSA 有相似之处，破译的途径之一是大素数的分解，如 Rabin、ElGamal 体制等。

关于加密技术，我们将在第二章中详细讨论，这里不再多介绍。

二、认证技术

认证技术是信息安全理论与技术的一个重要方面，也是电子商务安全的主要实现技术。采用认证技术可以直接满足身份认证、信息完整性、不可否认和不可修改等多项网上交易的安全需求，较好地避免了网上交易面临的假冒、篡改、抵赖、伪造等种种威胁。

认证技术主要涉及身份认证和报文认证两个方面的内容。身份认证用于鉴别用户身份，报文认证用于保证通信双方的不可抵赖性和信息的完整性。在某些情况下，信息认证显得比信息保密更为重要。例如，在很多情况下用户并不要求购物信息保密，而只需要确认网上商店不是假冒的（这就需要身份认证），确保自己与网上商店交换的信息未被第三方修改或伪造，并且网上商家不能赖帐（这就需要报文认证）；商家也是如此。从概念上讲，

信息的保密与信息的认证是有区别的。加密保护只能防止被动攻击，而认证保护可以防止主动攻击。被动攻击的主要方法是截收信息；主动攻击的最大特点是对信息进行有意的修改，使其失去原来的意义。主动攻击比被动攻击更复杂，手段也比较多。它比被动攻击的危害更大，后果也特别严重。

身份认证是信息认证技术中十分重要的内容，它一般又涉及到两个方面的内容：一个是识别；一个是验证。所谓识别就是指要明确用户是谁？这就要求对每个合法的用户都要有识别能力。为了保证识别的有效性，就需要保证任意两个不同的用户都具有相同的识别符。所谓验证就是指在用户声称自己的身份后，认证方还要对它所声称的身份进行验证，以防假冒。一般来说，用户身份认证可通过三种基本方式或其组合方式来实现：①用户所知道的某种秘密信息，例如，用户知道自己的口令；②用户持有的某种秘密信息(硬件)，用户必须持有合法的随身携带的物理介质，例如，智能卡中存储用户的个人化参数，访问系统资源时必须要有智能卡；③用户所具有的某些生物学特征，如指纹、声音、DNA 图案、视网膜扫描，等等。

报文认证用于保证通信双方的不可抵赖性和信息的完整性，它是指通信双方之间建立通信联系后，每个通信者对收到的信息进行验证，以保证所收到的信息是真实的过程。验证的内容包括：①证实报文是由意定的发方产生的；②证实报文的内容没有被修改过（即证实报文的完整性）；③确认报文的序号和时间是正确的。

目前，在电子商务中广泛使用的认证方法和手段主要有数字签名、数字摘要、数字证书、CA 安全认证体系，以及其他一些身份认证技术和报文认证技术。我们将在第三章和第四章中详细讨论电子商务活动中涉及到的认证技术。下面只简要加以说明。

（1）数字签名

在人们的工作和生活中,许多事务的处理都需要当事者签名,如政府文件、商业合同等。签名起到认证、审核的作用。在传统的以书面文件为基础的事务处理中，认证通常采用书面签名的形式,如手签、印章、指印等。在以计算机文件为基础的事务处理中则采用电子形式的签名,即数字签名。数字签名技术以加密技术为基础,其核心是采用加密技术的加、解密算法体制来实现对报文的数字签名。数字签名能够实现以下功能：

1）收方能够证实发方的真实身份;

2）发方事后不能否认所发送过的报文;

3）收方或非法者不能伪造、篡改报文。

目前已有大量的数字签名算法，比如 RSA 数字签名算法、ElGamal 数字签名算法、 Fiat－Shamir 数字签名算法、Guillou－Quisquarter 数字签名算法、Schnorr 数字签名算法、美国的数字签名标准 / 算法（DSS / DSA）、椭圆曲线数字签名算法，以及另外一些不可否认的签名算法、群数字签名算法、盲数字签名算法、具有报文恢复的数字签名算法等。

（2）数字摘要技术

数字摘要技术就是单向哈希（HASH）函数技术，它除了可用于前面所讨论的数字签名应用之外，还可用于信息的完整性检验，各种协议的设计以及计算机科学等。所谓单向

哈希函数就是把任意长的输入串 x 变化成固定长的输出串 y 的一种函数,并满足:

1）已知哈希函数的输出，求解它的输入是困难的，即已知 y=Hash(x),求 x 是困难的;

2）已知 x,计算 Hash(x)是容易的;

3）已知 y1=Hash(x1),构造 x2 使 Hash(x2)=y1 是困难的;

4）y=Hash(x),y 的每一比特都与 x 的每一比特相关，并有高度敏感性。即每改变 x 的一比特，都将对 y 产生明显影响。

构造单向哈希函数的方法多种多样，目前主要有以下几种:

1）利用某些数学难题，比如因子分解问题、离散对数问题等，设计哈希函数。已设计出的算法有 Davies-Price 平方哈希算法、Jueneman 哈希算法、Damgard 平方哈希算法、Damgad 背包哈希算法、Schnorr 的 FFT 哈希算法等。这些算法中有的已不安全。

2）利用一些对称密码体制，比如 DES 等，设计哈希函数。这种哈希函数的安全性与所使用的基础密码算法有关。这类哈希算法有 Rabin 哈希算法、Winternitz 哈希算法、Quisquater-Girault 哈希算法、Merkle 哈希算法、N-哈希算法等。

3）直接设计哈希函数。这类算法不基于任何假设和密码体制，受到了人们的广泛关注和青睐，是当今比较流行的一种设计方法。美国的安全哈希算法（SHA）就属于这类算法，另外还有 MD4、MD5、MD2、RIPE-MD、HAVAL 等算法。

（3）数字证书

数字证书（digital certificate, digital ID）又称为数字凭证，即用电子手段来证实一个用户的身份和对网络资源的访问权限。数字证书是一种数字标识，也可以说是网络上的安全护照，它提供的是网络上的身份证明。数字证书拥有者可以将其证书提供给其他人、Web 站点及网络资源，以证实他的合法身份，并且与对方建立加密的、可信的通信。比如用户可以通过浏览器使用证书与 Web 服务器建立 SSL 会话，使浏览器与服务器之间相互验证身份；另外用户也可以使用数字证书发送加密和签名的电子邮件。

目前数字证书格式一般采用 X.509 国际标准。一个标准的 X.509 数字证书包含以下一些内容：证书的版本信息、证书的序列号、证书所使用的签名算法、证书的发行机构名称、证书的有效期、证书所有人的名称、证书所有人的公开密钥、证书发行者对证书的签名。

我们可以使用数字证书，通过运用对称和非对称密码体制等密码技术建立起一套严密的认证系统，从而保证：信息除发送方和接收方外不被其他人窃取；信息在传输过程中不被篡改；发送方能够通过数字证书来确认接收方的身份；发送方对于自己的信息不能抵赖。这样，在网上的电子交易中，如果双方出示了各自的数字凭证，并用它来进行交易操作，就可以不用担心受骗上当了。

（4）CA 安全认证中心

为了全面解决在 Internet 上开展电子商务的安全问题，建立一套完善的电子商务安全认证体系是非常必要的。电子商务安全认证体系是一套融合了各种先进的加密技术和认证技术的安全体系，它主要定义和建立身份认证和授权规则，然后分发、交换这些规则，并在网络之间解释和管理这些规则。