电子商务应用丛书

电子商务安全与社会环境

芮廷先
钟伟春　编著
郑燕华

上海财经大学出版社

图书在版编目(CIP)数据

电子商务安全与社会环境/芮廷先,钟伟春,郑燕华编著. —上海:上海财经大学出版社,2000.8
(电子商务应用丛书)
ISBN 7-81049-453-8/F·378

Ⅰ.电… Ⅱ.①芮… ②钟… ③郑… Ⅲ.电子商务-安全技术 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2000)第 36051 号

责任编辑 王 芳
封面设计 周卫民

Dianzi Shangwu Anquan Yu Shehui Huanjing
电子商务安全与社会环境

芮廷先 钟伟春 郑燕华 编著

上海财经大学出版社出版发行
(上海市中山北一路 369 号 邮编 200083)
网 址:http://www.sufep.com
电子邮件:webmaster@sufep.com
全国新华书店经销
上海印刷七厂一分厂印刷装订
2000 年 9 月第 1 版 2000 年 9 月第 1 次印刷

787mm×960mm 1/32 7.5 印张 108 千字
印数:0 001—4 000 定价:11.00 元

第一章

电子商务的安全问题

互联网的发展极大地促进了网上电子商务的开展，通过互联网实现的商业销售正以成十倍的速度增长，众多企业把电子商务作为21世纪的业务增长点。面对企业潮水般涌入的信息流，怎样才能分辨交易的真伪、信息的真假？除了沿用传统的法律和道德来约束交易行为外，在信息时代依靠技术来保护自身的手段显得越来越重要。

电子商务的安全现状

2000 年 2 月 7 日、8 日、9 日这三天，美国多家著名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。

黑客 3 天来的袭击，造成的间接和直接损失达 10 亿美元。2 月 7 日，除了免费电子邮件等三个站点未受影响外，雅虎的大部分网络服务陷于瘫痪。雅虎是全球第二大搜索引擎网站，每天被浏览页次达 4.65 亿次，其股市价值达 930 亿美元。8 日上午，先是当天股市的网络销售公司购买网站死机，再是网上电子拍卖网站电子港湾、网上书店及商品销售的亚马逊网站告急。电子港湾的注册用户达1 000万，是每月键阅率达 15 亿次的网上电子拍卖网站，8 日下午 6 时，商品买卖一度被迫停止数小时。当晚，美国有线电视新闻网宣布，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，电子商务网站再度遭殃，电子交易网站在股市开市

前遭到持续 1 小时的攻击；信息技术公司的科技新闻网站 ZDNet 约有 70%的内容被中断 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。

美国联邦计算机案件处理中心主任大卫·加诺说："全美至少有数百台的计算机受到袭击。万幸的是，黑客并未进入网站内部，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袭击，这在因特网历史上还是第一次。"有关专家称，此事将进一步引起人们对网络安全和电子商务风险的关注。

近年来，网络技术和电子商务迅猛发展，人们在网络上进行从购买书籍、日用品到计算机、房产交易以及股票炒作、资金运作等的活动剧增，网络安全问题一直是人们关注的话题。电子商务安全的重要性已不言而喻，安全问题是电子商务推进中的最大路障。营造信誉良好、安全可靠的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赊销，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，但因为业界一直没有提供一个安全保护的完整概念，所以很多人在安全认知上仅限于对防火墙的了解，而防火墙只是安全保护的一个方面，绝不等于全部，这也正是实施了防火墙的网络仍有漏洞的原因所在。

为了使我们对电子商务的安全问题有更感性的认识，我们可以分析一下黑客盗取信用卡的过程。黑客在互联网的新闻组上发布带有后门病毒的程序，并鼓励人们下载到自己的 PC 机上，一旦某台 PC 机下载了此程序，那么他就成为黑客可以侵略的对象。黑客可以浏览被入侵者 PC 机上的全部信息资源，可以实时地掌握被入侵者的桌面使用情况。如果被入侵者此时输入信用卡号，那么黑客就可易如反掌地窃取到这一代码，这是信用卡被盗用的主要原因。即使你不曾在公共信息场所下载软件，你也很有可能成为无辜的受害者，因为黑客程序中的后门病毒具有很强的蔓延性，即一台 PC 机被感染后，病毒可通过此台 PC 机上的地址簿向所有这些地址的 PC 机传播，然后按同样的方法再进一步把态势扩大。这种几何级的增长使病毒的蔓

延速度极快，覆盖范围极广。所以，不经意间或许你的 PC 机就已成为黑客的盘中餐，而一个从事网上交易的网站一旦发生消费者信用卡泄露事件，那么将不会再有人去访问这个站点。因此，要使电子商务能够健康、蓬勃地发展，就必须用全面的电子商务安全解决方案来提供交易的信任保障。

电子商务站点上的安全漏洞会造成网上交易用户的账号、交易密码泄露，恶意攻击者甚至可以使用他人资金进行网上交易。中国互联网中心于 2000 年 2 月 18 日发布的《中国互联网络发展状况统计报告》中关于电子商务的调查表明，安全可靠性是 52.26% 的电子商务用户最关心的问题。安全漏洞的存在，直接影响国内电子商务站点的信誉程度。网上交易安全性若不能得到保证，就必将影响国内电子商务的顺利发展。

电子商务的安全问题是一个涉及范围极广的社会问题，我们希望有越来越多的企业和个人加入到关心电子商务的行列中来，一起为开创崭新的商务时代出力献策！

电子商务的安全控制内容

电子商务的安全问题早已成为大家关心的焦点。人们从面对面的交易和作业，变成网上互不见面的操作，没有国界、没有时间限制，可以利用互联网的资源和工具进行访问、攻击甚至破坏。如何保证商务秘密不被泄露或盗用、数据库的保密性、防止商业欺诈、网络交易系统的安全运行，以及如何判定交易人的身份及用户的信用、电子签名的识别与防伪、如何保证商家安全收款等都是不容忽视的关键所在。概括起来，电子商务面临的安全威胁主要有：

1. 信息在网络的传输过程中被截获

攻击者可能通过互联网、公共电话网、搭线或在电磁波辐射范围内安装截收装置等方式，截获传输的机密信息，或通过对信息流量和流向、通信频度和长度等参数的分析，获取有用信息，如消费者的银行账号、密码等。

2. 传输的文件可能被篡改

攻击者可能从三个方面破坏信息的

完整性：

(1)篡改，即改变信息流的次序，更改信息的内容，如购买商品的出货地址；

(2)删除，即删除某个消息或消息的某些部分；

(3)插入，即在消息中插入一些信息，让收方读不懂或接受错误的信息。

3. 伪造电子邮件

(1)虚开网站和商店，给用户发电子邮件，收订货单；

(2)伪造大量用户，发电子邮件，穷尽商家资源，使合法用户不能正常访问网络资源，使有严格时间要求的服务不能及时得到响应；

(3)伪造用户，发大量的电子邮件，窃取商家的商品信息和用户信用等信息。

4. 假冒他人身份

(1)冒充他人身份，如冒充领导发布命令、调阅密件；

(2)冒充他人消费、栽赃；

(3)冒充主机欺骗合法主机及合法用户；

(4)冒充网络控制程序，套取或修改使用权限、通行字、密钥等信息；

(5)接管合法用户，欺骗系统，占用合法用户的资源。

5. 不承认已经做过的交易(即抵赖)

(1)发信者事后否认曾经发送过某条信息或内容；

(2)收信者事后否认曾经收到过某条消息或内容；

(3)购买者做了订货单不承认；

(4)商家卖出的商品因价格差而不承认原有的交易。

据报道，美国每年因信息与网络安全问题所造成的经济损失达75亿美元，企业电脑安全受到侵犯的比例从1996年的42%上升到1997年的78%。可以说，在电子商务的所有问题中，安全问题已成为危害最大、最急需解决的问题。

实际上，由于电子商务是基于因特网而发展的，因此，网络安全也必然成为电子商务安全的一部分内容。但就电子商务本身的特点而言，从计算机用户的角度来讲，它在安全性方面还有着不同的要求，尤其对于网上的电子支付来讲，如何在网上保证交易的公正性和安全性，保证交易方身份的真实性，保证传递信息的完整性以及

交易的不可抵赖性，成为推广电子商务过程中人们最为关心的问题。因此，在 Internet 上发送和接收信息时要证明：除了发送方和接收方外，不得被其他人知悉；信息在传输过程中不被篡改；发送方能确信接收方不是假冒的；发送方不能否认自己的发送行为。

一般来说，电子商务的安全控制有如下内容：

1. 信息的保密性

在网上进行电子商务的询价、成交、签约，涉及许多商业秘密和公众隐私。如果信用卡的账号和用户名被人知悉，就可能被盗用；如果订货和付款的信息被竞争对手获悉，就可能丧失商机。1998 年初，有人利用能在新闻组中查找到的普通技术手段，轻易地从多个商业站点窃取了80 000多个信用卡账号和密码。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。电子商务是建立在一个较为开放的网络环境上的(尤其 Internet 是更为开放的网络)，维护商业机密是电子商务全面推广应用的重要保障。因此，必须预防非法的

信息存取和信息在传输过程中被非法窃取。所以，在电子商务中传播的信息一般均应加密，以确保传送的信息除了发送方和接收方外，不被其他人知悉。

2. 数据的完整性

电子商务简化了贸易过程，减少了人为的干预，同时也带来了维护贸易各方商业信息的完整性、统一性的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的差异。此外，数据传输过程中信息的丢失、信息重复或信息传送的次序差异也会导致贸易各方信息的不同。贸易各方信息的完整性将影响到贸易各方的交易和经营策略，保持贸易各方信息的完整性是电子商务应用的基础。因此，应当预防对信息的随意生成、修改和删除，同时要防止数据传送过程中信息的丢失和重复，并保证信息传送次序的统一，即电子商务应能确保信息在传输过程中不被篡改。

3. 非伪装性

网上交易的双方很可能素昧平生、相隔千里。要使交易成功，首先要能确认对方的身份。商家要考虑客户端不能是骗

子，而客户也会担心网上的商店是不是一个玩弄欺诈的黑店。因此，能方便而可靠地确认对方身份，即发送方能确信接收方不是假冒的，是交易的前提。

4. 不可否认性

由于商情的千变万化，交易一旦达成是不能被否认的，否则必然会损害另一方的利益。例如订购黄金，订货时金价较低，但收到订单后，金价上涨了，如收单方能滞认收到订单的实际时间，甚至否认收到订单的事实，则订货方就会蒙受损失。因此，电子交易通信过程的各个环节都必须是不可否认的，要在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。

5. 不可修改性

交易的文件是不可被修改的，如上例所举的订购黄金。供货单位在收到订单后，发现金价大幅上涨了，如其能改动文件内容，将订购数 1 吨改为 1 克，则可大幅受益，那么订货单位可能就会因此而蒙受损失。因此，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。

6. 审查能力

根据信息的保密性和数据的完整性的要求，应对数据审查的结果进行记录，以备交易双方产生纠纷时交由第三方处理。

电子商务的安全技术

长期以来，人们把信息安全理解为对信息的机密性、完整性和可获性的保护，这固然是对的，但这种观念是在 20 多年前的主机时代形成的。80 年代是微机和局域网时代，计算机已从专用机房内解放到分散的办公桌乃至家庭。由于它的用户/网络结构比较简单，所以既要依靠保护措施，又要制定人人必须遵守的规定。因此，这个时代的信息安全是面向规约的。90 年代进入了互联网时代，每个用户都可以连接、使用乃至控制散布在世界上各个角落的上网计算机，因此，Internet 的信息安全内容更多，更为强调面向连接、面向用户，人、网、环境相结合，形成了一个复杂的系统，通过网上的协同和交流，人的智能和计算机快速运行的能力汇集和融合起来，创造了新的生产力，丰富着电子商务、网上购

物等大量应用，满足着人们的交往、学习、医疗、消费、娱乐、安全感、安全环境等各种社会需要。

可以这样说，面向数据的安全概念是前述的保密性、完整性和可获性，而面向使用者的安全概念则是鉴别、授权、访问控制、抗否认性和可服务性以及基于内容的个人隐私、知识产权等的保护。这两者结合就是电子商务安全体系结构中的安全服务，而这些安全问题又要依靠密码、数字签名、身份验证技术、防火墙、安全审计、灾难恢复、防病毒、防黑客入侵等安全机制（措施）加以解决。其中，密码技术和管理是电子商务安全的核心，安全标准和系统评估是电子商务安全的基础。

电子商务系统的安全体系包括以下三个层次：

1. 密码机制，即基本加密算法，其中包括对称密钥加密、非对称密钥加密等。

2. 以密码机制为基础的 CA 体系以及数字信封、数字签名、数字时间戳等基本安全技术。

3. 以密码机制、基本安全技术、CA 体系为基础的各种安全应用协议，如 SET、

SSL、S/MIME 等。

以上各部分构成了电子商务的安全体系，在此安全体系之上可以建立电子商务的支付体系和各种业务应用系统。另外，防火墙技术属于一种被动的保护措施，也是参与电子商务应用的企业所常用的一种技术手段。

这里将介绍为了确保网上交易的安全性及满足相应的安全控制要求，在电子商务的应用过程中主要采用的几种安全电子交易的方法和手段。

一、密码机制

采用密码技术对信息加密是最常用的安全交易手段，是电子商务安全的基础。加密的主要目的是防止信息的非授权泄露。加密可用于传输信息和存储信息。从谱分析的角度看，加密把声音变成噪声、把图像变成雪花、把计算机数据变成一堆无规律杂乱无章的字符，攻击者即使得到经过加密的信息即密文，也无法辨认原文。因此，加密可以有效地对抗截收、非法访问数据库窃取信息等的威胁。加密一般是利用信息变换规则把可懂的信息变成不可懂

的信息，其中的变换规则称为密码算法，可懂的信息称为明文，不可懂的信息称为密文。密码算法是一些数学公式、法则或程序，算法中的可变参数是密钥。密钥不同，明文与密文的对应关系就不同。密码算法总是设计成相对稳定的，从这个意义上讲，可以把密码算法视为常量，而密钥则是变量。

现代密码学的一个基本原则是，一切秘密寓于密钥之中。在设计加密系统时，总是假设密码算法是公开的，真正需要保密的是密钥。因此，在分发密钥时，必须要采用安全方式。衡量一个加密技术的可靠性，主要取决于解密过程的数学问题难度，而不是对加密算法的保密；可靠的加密系统应当不怕公开它的加密算法。此外，可靠性还与密钥的长度有关。

在电子商务中获得广泛应用的加密技术，主要有秘密密钥和公开密钥两种。

1. 秘密密钥系统

秘密密钥系统属于对称型加密系统，其特点是数据的加密方和接收方使用同一个密钥，即文件的加密和解密用的是同一个秘密密钥。由于秘密密钥为了保密起见