信息与网络安全丛书

安全电子商务

——为数字签名和加密构造基础设施

(第二版)

Secure Electronic Commerce

沃里克·福特（Warwick Ford）

迈克尔·鲍姆（Michael S.Baum） 著

劳帼龄 等 译

人民邮电出版社 PH PTR Pearson Education 出版集团

图书在版编目（CIP）数据

安全电子商务：为数字签名和加密构造基础设施：第 2 版 /（美）福特（Ford，W.），（美）鲍姆（Baum, M. S.）著；劳帼龄译. —北京：人民邮电出版社，2002.5
ISBN 7-115-10240-6

Ⅰ. 安…　Ⅱ. ①福… ②W… ③鲍… ④劳…　Ⅲ. 电子商务—安全技术　Ⅳ. F713.36

中国版本图书馆 CIP 数据核字（2002）第 019407 号

信息与网络安全丛书

安全电子商务

—— 为数字签名和加密构造基础设施（第二版）

◆ 著　沃里克·福特（Warwick Ford）
　　迈克尔·鲍姆（Michael S .Baum）
　译　劳帼龄　等
　责任编辑　李　际

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
　邮编　100061　电子函件　315@ptpress.com.cn
　网址　http://www. ptpress.com.cn
　读者热线　010-67180876
　北京汉魂图文设计有限公司制作
　北京顺义向阳胶印厂印刷
　新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
　印张：24.25
　字数：574 千字　　2002 年 5 月第 1 版
　印数：1-3 000 册　　2002 年 5 月北京第 1 次印刷

著作权合同登记　图字：01 - 2001 - 4823 号

ISBN 7-115-10240-6/TP • 2839

定价：46.00 元

本书如有印装质量问题，请与本社联系　电话：(010)67129223

译者序

在中国互联网络信息中心所作的历次调查和发布的《中国互联网络调查统计报告》中，安全问题一直是电子商务用户特别关注的主题。安全漏洞的存在，将直接影响电子商务网站的信誉度，而电子商务交易的安全性得不到保证，则必将影响电子商务的顺利发展。确实，电子商务的安全问题已成为推进国际国内电子商务发展的一大瓶颈，正在引起越来越多人士的关注。然而，电子商务的安全问题并不是仅靠技术就能解决的，这是一个涉及范围极广的社会问题，需要各方的协调配合。

因特网的普及促进了网上电子商务的开展，但企业面对潮水般涌入的信息流，该如何分辨交易信息的真假呢？在这里，除了要充分依靠现代信息技术，尤其是信息安全技术手段来进行保护外，还需要沿用法律和管理的手段对交易行为进行约束。

本书从技术与法律控制相结合的角度论述了电子商务的安全问题，立意新颖，结构清晰。第 1 章作为导论首先介绍电子商务的基本概念；第 2 章介绍电子商务得以开展的基础——因特网；第 3 章介绍基本的商务活动与法律原则，对电子商务中所涉及的基本的法律问题作了简单的介绍和铺垫；第 4 章概要介绍信息安全原理及各类信息安全技术；第 5 章立足因特网介绍 Internet 安全问题；第 6 章介绍证书及证书的管理；第 7 章介绍公开密钥基础设施 PKI；第 8 章介绍与电子商务有关的立法活动及相关的法律法规；第 9 章介绍电子商务交易的不可否认机制；第 10 章介绍证书策略 CP 与认证操作说明 CPS 的内容；第 11 章介绍对公开密钥基础设施 PKI 的评估与鉴定。此外，本书还在附录中介绍各类合同的形式，介绍美国的联邦电子签名法、联合国电子商务示范法、欧洲电子签名指南等法律法规，另外还介绍了 ASN.1 表示法、X.509 标准、各类安全标准以及公开密钥加密算法等。

本书用了三个贯穿始终的案例：（1）Vera 制造公司在网上采购 Danielle 机器制造公司生产的车床；（2）Danielle 机器制造公司为生产机器需要钢材原料而与 Sharon 钢铁公司进行 B-B 交易；（3）Nola 通过开设因特网购物中心——Nola 电子市场，向消费者提供网上零售。通过这三个典型的案例，把无论是 B-B 还是 B-C 电子商务中所涉及的各类安全问题的技术解决方法、法律控制与管理手段表达得淋漓尽致。

本书的两位作者，一位是信息技术专家，一位是法律工作者。由他们联合撰写的这本著

作，从技术与法律相结合的角度全面论述了电子商务的安全问题，通过技术手段与法律控制的结合阐明了安全电子商务的组成及实现安全电子商务的秘诀。在电子商务的安全问题日益引起人们关注的今天，本书值得一切与电子商务安全相关的人员阅读，也适合对电子商务安全感兴趣的人士参考。

本书由劳帼龄主持翻译，参加翻译工作的还有钟伟春（第5章）、张雪凤（第6章）、周新燕（第8、9章）、李文斌（第10、11章）。劳帼龄除了负责第1、2、3、4、7章以及前言、序和附录A～K的翻译外，还负责了对其他译者初稿的修改和全书的统稿工作。由于译者水平所限，书中难免有错误之处，欢迎广大读者批评指正。

劳帼龄

于上海

2002年3月

序

美国参议院 Spence Abraham 先生所作的序

我们正生活在一个激动人心的时代，很显然这是一个由高技术企业所带来的无穷无尽的改进和变革所造就的时代。在这样的时代中，需要对各个组织所使用的系统、安全措施甚至于各种商业模式进行重新的学习和重新的审视。无论是智能卡、还是生物测定装置、加密方法以及创新型的解决方案，都将要经历即将到来的变革。对企业和消费者来说，公开密钥加密技术的使用可能会成为他们的安全箭囊中一支重要的利箭。

近年来，美国国会已经开始意识到了自己对于因特网以及大量相关技术的革命性变革负有不可推卸的重要责任。利用其声望，国会通过消除旧的监管体制、消除对电子商务的法律障碍，为推动和促进技术型企业的持续发展作了很多努力。

最近通过的 S.761 文件，即《电子签名与国际国内商务（电子签名）法》就是意在进一步加强对电子商务的公共接入，提高人们对电子商务安全的信心。国会正在与私人企业、联邦机构以及各州一起为确保电子签名与电子记录能够有一个全国统一的法律基准而努力。全国管理者协会对各州及联邦在这方面的新规则作了一个很好的总结，在其于 9 月 28 日通过的文件中认为“这是管理者必须要知晓的”，他们认为，该联邦法案“是一个使用和保留记录与签名的基本框架”，该法案“认为电子签名和电子记录与手写签名和手写记录一样，具有同样的法律上的有效性、合法性和可执行性，认为法律应该对用来创建这类记录和签名的专门技术与方法保持中立。”

正如《安全电子商务》一书所清晰地论述的，对企业、消费者以及政府来说，必须对其在各类应用中到底选择什么样的安全措施、其安全程度如何进行仔细的判断。对今天的企业来说，在选择信息安全技术时，比以往任何时候都更需要了解这类技术的新旧交替、成本、收益及风险。而要做到这一切，那就必须从本书的第 1 章开始认认真真地阅读。

Spence Abraham

U.S. Senate

密歇根州的 Abraham 参议员是联邦电子签名法案的设计者，该法案肯定了电子商务中电子签名的合法性。Abraham 参议员也是政府消除文书工作法案的倡议者，该法案为在联邦政府机构中使用电子签名打开了

方便之门。

美洲银行 Rhonda MacLean 先生所作的序

与其他任何应用程序相比，1994 年问世的 Web 浏览器给予了因特网革命巨大的帮助。简单、直观、互动，与印刷在纸上的新闻相比，在 Web 上浏览对于社会、经济和政治的影响更大。这种信息的表示方式、传播方式、访问形式以及使用方式上的革命推动美国经济进入了一个史无前例的发展时期。目前，这场以新经济为代名词的革命已经在全世界扎根，其影响还在继续扩大而且没有减轻的迹象，它将进一步推动旧经济模式下的企业采用新的原则和技术来传递其产品与服务。而且，这一信息革命的传播速度超过了以往任何的技术。

各类杂志、电视节目、书籍以及其他媒体已经对新经济作了大量的报道和宣传，其宣传的重点主要在于信息的可用性和前所未有的方便的访问方式是如何改变了人们与企业间的交互方式。因特网上对于信息的表示、传输以及交换方式的开放式标准，极大地推动了涉及几百万用户的新经济应用的诞生。在过去的两三年时间里，人们已经看到，通过因特网可以创造出任何商业理念，也可以重新再造和不断地改进各类商业理念。各种电子化的活动，如用电子化手段开展的银行业务和电子销售活动，已经演化成了电子银行（e-banking）和电子销售（e-sales），甚至像因特网上的拍卖网站 eBay 这样的 e 化新名词。电子商务创新活动正在不断地衍生出新的不同的方式。

不幸的是，新经济所带来的并非全都是奇迹和喜悦。电子化的世界使得创造更多的商业新理念成为可能，但同时它也带来了电子化的犯罪活动。因特网上所使用的为开放的信息交换所设计的协议和服务，其安全性是相对比较弱的，这就为觊觎者提供了可乘之机。为了从胜利者手中分得一部分财富，这些人可以想出各种各样的方法来。媒体上已经公开报道了很多由电子犯罪和黑客式的攻击所造成的电子入侵事件，如有些电子商务零售网站由于安全措施不够严密而丢失了数千个用户的信用卡账号，另外，有一家英国的大银行也由于安全的缘故不经意间让几千个客户的账户信息成为了因特网上垂手可得的公开信息。这些破坏事件动摇了用户的信心，也破坏了用户与企业间的关系。而这些事件同时也说明了本书所介绍的那些信息和概念的重要价值，以及对这些信息和概念进行了解的广泛需求。

新经济的承诺还需要依靠服务的支持，信息与商务的交易需要在一年中的每一天、一天中的每一个小时、在全世界都可以进行。一些知名的电子商务企业曾经遭受称为拒绝服务的恶毒攻击而导致网站瘫痪，由此给企业造成了巨大的业务损失和相当的不便。

调查和民意测验显示，大约有 80%的因特网用户对其个人隐私、信用卡或其他购买信息的安全问题表示担忧，其中大部分用户曾经在尝试用电子手段购买产品和服务过程中遇到过这样那样的麻烦，许多用户还是更信赖人与人的接触，宁愿从那些传统企业购买物品。

身份的被窃和被冒充越来越引起人们的不安。人们必须要知道正在和你做生意的到底是谁，于是认证服务就成为了安全电子商务的基本保证。此外，保护隐私和保障信息的安全可信也是必须的。

为保证因特网革命的成功，需要对正在使用的和已经理解的安全框架进行根本的改进。如果不能在安全问题上取得协调的、根本的改进，那么就无法将因特网和电子商务的全部能量发挥出来。因特网应该成为进行商业和金融交易的可信赖的媒体。为了电子商务的成功，企业需要像本书作者这样的专家的指导，需要了解像本书专家所介绍的那些知识，或许这种需求还超出了对新经济预言的需求。通过运用安全的原则与技术，电子商务就能被客户所接纳。

历史上，金融机构早就意识到了安全与信任是企业的核心竞争力，因此在保证信息与交易的安全方面作了不懈的努力。美洲银行正在以前所未有的方式向自己的客户提供各类银行业务，所采取的方法之一就是要保证银行业务的便利性，确保客户的使用的方便，并确保安全。我们正在致力于解决以前可能很少关注的隐私与安全问题，人们将会在我们的工作中看到本书中所介绍的那些原则与技术。

例如，在国际上，美洲银行正与许多其他的金融机构一起通过一种互相合作的契约式结构——Identrus 来实施像数字证书这样的安全机制。Identrus 通过提供可互操作的公开密钥基础设施来验证数字证书的有效性和数字签名的真实性。这套系统推动了电子商务在涉及成千上百万美元的国际业务领域中安全的、可信的应用 。

要想通过电子商务把新经济的能量淋漓尽致地发挥出来，那就必须解决安全问题。目前我们所面临的问题是：安全专家太少，而构建不安全应用的方法却太多，此外，各类商用产品和未能进行充分的安全配置的产品也太多。我们认为，安全产品应该有像金融服务圆桌会议的 BITS 实验室一样的安全测试实验室的评估和批准，也可以联合行业集团来共享各类与安全脆弱性、安全论点和安全问题有关的信息，如金融服务信息共享与分析中心（FSISAC），就能在其可信赖的成员间共享匿名的信息。

本书将对你了解电子商务所必须的运作环境有极大的帮助。此外，本书所介绍的信息还将帮助你为企业选择正确的安全方向，以满足你的企业对安全的特定需求。在本书的字里行间对电子商务与信息安全的基本元素作了有相当说服力的介绍，希望你能够好好地使用这本综合性的指导书，能经常翻翻它。

祝各位好运！

Rhonda MacLean
Senior Vice President—Division Manager,
Information Protection
Bank of America

通用汽车公司 Mark Hogan 先生所作的序

通用汽车，作为一家有着 80 多年历史的世界上最大的制造型企业，其所受到的因特网革命的影响恐怕没有一家企业能与之相比。今天，因特网正在改变着我们企业的一切。通常，一辆汽车需要由近 5000 个零部件才能组成为一件完美的产品。与过去生产库存和经销商处的产品库存那长长的传递途径相比，我们今天正在缩短这两者，而更重要的是，因特网正在

改变我们的制造模式。过去要处理 5000 个零部件的工厂，今天只需要处理其中的一部分就可以了。我们工厂的规模变得更小，而质量与效率却提高了。同样，经销商的规模也变得更小，而效率却更高，今天我们把更多的时间花在通过 Web 与我们的客户进行个别接触上。

我们看到在市场中正在出现的为客户度身定制的模式。Michael Dell 在计算机销售中所开创的那套模式不久将被用在我们的汽车销售上，也就是说，根据客户在网上所下的订单来进行生产。客户可以在他所希望的时间、地点，以他所希望的价格得到他所希望的汽车。更进一步的是，因特网为我们所提供的可以进行反复设计的机会，意味着我们可以进行实时的交互设计，从而更精确地满足我们的目标客户的需求。

公司在去年新成立了 E-GM，作为一个庞大的机构主要负责对 GM 的大部分在线业务进行监督。我们的 BuyPower 网站以及与其他网站的联盟，包括与美国在线的联盟，在将客户吸引到我们的网上展示室方面取得了巨大的成功，在 12 个月的运行期间，其销售额是传统经销方式的 3 倍。

无论如何，从扭转或者至少了阻止国外竞争者对美国汽车制造市场的侵蚀的角度来说，电子商务是我们未来的关键所在。我们已经主动在企业的供应商和经销商这两方面想了很多办法，基于因特网的 B-B 电子商务为我们极大地削减成本和提高生产效率提供了机会。

然而，在电子商务成为主流之前，我们还面临着一大障碍，即我们要让那些新技术的用户们满意地理解和运用新的商业风险模式，而这些模式又必须是新技术所能支持的。从这一点来说，本书恰好满足了这一关键的需求。在本书中，我们可以令人振奋地发现，它对那些电子商务的风险管理问题作了完整的和明晰的解释，其中既有对于安全技术问题的综合介绍，又有对于最新的立法和法律法规问题的分析，而这些问题都会对企业的风险管理决策造成非常大的影响。

Mark Hogan, Group Vice President, E-GM
General Motors Corporation

微软公司 Hank Vigil 先生所作的序

对于那些正在寻找电子商务优点的人们来说，因特网代表了一种惊人的承诺。但不幸的是，相对于因特网出现之前所有的交易方式而言，因特网有一个致命的弱点，那就是其完全的公开性。如果不使用专门的安全技术和相应的支撑结构，任何人只要有足够的毅力就有可能读取到交易内容，也就有可能编造和修改交易内容。如果我们不能应对安全问题的挑战，那就有可能严重地影响因特网商用潜力的挖掘，这主要是因为用户会因此而缺乏信心，同时一次次地应对安全攻击也耗费了巨额的费用。

微软公司的因特网安全目标主要由 4 个方面组成：（1）提供最强壮的技术以满足客户在因特网上交互时对安全的需求；（2）与标准化组织一起努力确保采用最佳的技术来满足客户的需求并确保互操作性；（3）将安全标准添加到微软的技术中，并将其用到我们的操作系统和万维网浏览器及服务器中；（4）在我们现有的应用产品中增加安全方面的内容。

特别值得一提的是，微软已经为电子商务和在线通信开发了一个跨平台的安全框架，称为微软因特网安全框架。这个开放的、可互操作的框架支持因特网的安全标准和一些新的技术，其中许多技术都在这本书中作了介绍，包括万维网上的认证与加密、公钥证书服务、数字钱包以及用于信用卡交易的“安全电子交易”（SET）协议。

在因特网上会遇到各种各样的安全问题。例如，今天的用户会面临的最严重的风险之一可能是：并不知道自己下载了会对自己计算机上的内容进行篡改或进行恶意攻击的软件。为帮助人们降低这类风险，微软公司已经开发了一个 Authenticode 系统，该系统可以提高 Web 用户在因特网上下载软件时对其真实性的信心。借助 Authenticode，用户可以知道该软件是谁发布的以及该软件自发布以来是否被篡改过。因此，用户就可以更可靠地作出是否接受该下载软件的决定。

安全问题的解决将能让我们把因特网商店这样的概念变为现实。因特网商店必须建立在集成的、强有力的工业化解决方案基础上，它涉及到商品价值链的所有组成部分，包括以一种协调一致的、方便的、灵活的、可扩展的、可靠的方法来进行商店管理、订单采购、财务交易、分销及交货。在线商店的建立和经营必须非常方便，能够让经销商把精力放在商品上。微软的商店产品家族就能满足这一市场需要，这类产品是以微软因特网安全框架来作为其安全基础的。

虽然将一些相应的安全措施合并到软件产品中对实现安全的电子商务是必须的，但仅靠这些还远远不够。要实现安全的电子商务还需要其他必备的因素，包括：（1）基本的信息安全技术，如加密和数字签名技术；（2）安全体系、安全协议、安全手段方面的一致的标准；（3）安全基础设施服务提供商，如认证机构；（4）能够被接受的商业实践和司法实践；（5）立法、法规与法律指导。其中的每一个因素都是独立的，而且都不是那么简单的。

如果有人能将这些因素组合起来并考虑其相互作用，则结果可能是惊人的复杂，这就是本书的重要性所在。《安全电子商务》一书为电子商务的进步所作出的贡献是独一无二的，其价值是无法估量的。Warwick Ford 和 Michael Baum 两位作者以非常易读的笔触为我们介绍了该领域各个方面的基本内容。

基于因特网的电子商务的出现是一个令人振奋的现象，微软为自己能成为其中的一部分而自豪。但是，只有当对使用、提供和管理这些服务与产品所涉及的安全问题有了充分的了解之后，才能将大规模的快速普及的因特网电子商务的潜力全部发挥出来。本书为我们对这些问题的了解作出了重要的贡献，各位请好好地读一下这本书吧，好好地学习和享受这本书为我们带来的知识吧。

Hank Vigil
VP, Consumer Strategy and Partnerships
Microsoft Corporation

Hank Vigil 先生的序是于 1997 年为本书第一版所写

前 言

电子商务的出现，作为企业重组的推进器和企业重组的重要组成部分，伴随着我们走进了 21 世纪。电子商务给那些拥抱接纳它的人们带来了巨大的回报，同时，它也给那些未能谨慎地使用它的人们带来了相当大的风险。虽然人们大量地责怪新技术，认为是这些新技术的复杂性以及新技术的普及过快而导致了这些新的风险，但新技术又在管理和减轻风险中扮演了重要的角色。在这些新技术中尤以数字签名和公开密钥加密技术为代表。然而，实现安全的电子商务所需要的不仅仅是实现由这些核心技术所构成的应用，它还需要依靠技术、企业以及法律基础设施的互相依赖，只有实现了它们之间的相互依赖，才能使得那些核心技术在一个广阔的范围内得以很好地使用。在本书中，我们的目的就是要向大家介绍安全电子商务的组成以及实现电子商务安全的秘诀，我们将把重点放在安全电子商务的作用、其实际运用以及这些基础设施的使用上。

为什么本书是由一位工程师和一位律师联合撰写的呢？答案在于，要想实现安全的电子商务必须将技术上的安全措施与法律上的控制巧妙地结合在一起。如果只是单方面地从技术或是从法律的角度来进行研究，那是无法理解其中最关键的问题的。所以必须将技术专家和法律专家的意见综合起来，才能对电子商务安全问题进行有效的论述。

本书将阅读对象定位为一个比较广泛的群体，包括企业专业人员、信息技术人员以及法律工作者——即一切与电子商务的安全有关的人员，而且对读者来说，不需要具有技术和法律方面的扎实背景。为了让本书对企业工作者、消费者、银行工作者、产品开发人员、服务提供商、律师、决策人员以及学生都能具有参考价值，我们尽可能地包括了各个方面的介绍材料，并且在介绍一些比较复杂的问题之前，首先向读者介绍有关方面的启蒙知识。

自本书的第一版出版以来，在安全电子商务领域已经有了巨大的进展。虽然核心的技术并没有什么根本的改变，但在软件工具、封装技术、标准化、全球性的立法以及在将我们在第一版中所介绍的技术运用到实际电子商务中的经验方面，已经有了长足的进步。例如在标准化领域，我们已经看到了像 S/MIME 安全消息传递规范 Ipsec 虚拟专用网规范以及用于公开密钥基础设施的 IETF PKIX 规范的建立，以及它们的广泛应用。此外我们也看到了在各国和各州的数字签名法以及美国联邦电子签名法案中所体现出来的一些著名的立法行动。另外在

安全电子商务的基础设施的组件的评价鉴定如认证机构方面，也有了巨大的进展。这些进步通常是伴随着电子商务应用规模的不断扩大，尤其是伴随着 B-B 因特网商务的迅速涌现而发生的。因而，在本书的这一版中，我们将把重点放在那些已被证明在今天的市场空间中是非常重要的，以及为确保电子商务应用的成功需要对其进行严格分析的那些领域上。

我们写作本书的思路是将其介绍给全世界的读者。虽然读者将会发现，尤其在具体的实践和法律问题方面，我们主要是以美国为蓝本来介绍的。通常，我们认为全球所面临的问题其实与美国所面临的问题基本上是一样的，所以我们期望我们对美国所面临的问题以及在解决这些问题方面的进展情况的介绍，能够对其他国家的应用具有重要的意义。如果我们在这方面有什么欠缺的话，我们向我们的国际同行们表示歉意。

我们必须要感谢 VeriSign 公司，也就是我们两位作者所供职的公司，没有 VeriSign 就不会有这本书。公司给予了我们精神上的巨大支持，同时又通情达理地谅解了我们从许多日常工作中分出心来写这本书。不过，作者在本书中所发表的看法未必代表 VeriSign 公司的看法，也不一定代表任何其他实体的看法。

我们还要感谢其他好多人的帮助。首先我们必须要感谢的是 Eric Pearson，他在法律资料的评估和审阅方面帮了我们的大忙。

还有很多人在本书手稿的整理和法律相关资料审阅中作了很多重要的工作，他们是：

Joseph Alhadeff
Rich Ankney
Lee Barrett
David Billiter
Barclay Blair
Jim Brandt
Pat Cain
Terry Ford
Twyla Furger
John Gregory
Peter Gregory
Rich Guida
Phillip Hallam-Baker
Paul Heath
Mack Hicks
Jeremy Hilton
Cris Hollier
Russ Housley
Kaye Caldwell
Eric Caprioli
Kevin Coleman
Bruce Crabtree
Walter Effross
Gillian Elcock
David Fillingham
Sam Phillips
Stephanie Plasse
Tim Polk
Michael Power
Ron Rivest
Ron Ross
Greg Rowley
Mark Russell
Bruce Schneier
Stratton Sclavos
Mark Silvern

Jeff Kalwerisky
Hoyt Kesterson
Marcus Leech
Judah Levine
David W. Maher
Rebecca Matthias
Charles Merrill
Michael Myers
Steve Orlowski
Renaud Sorieul
Gary Stoneburner
Riad Tallim
Robert Tample
Paul Van Oorschot
Ian Waters
Peter Williams
Stephen Wu

我们还要感谢 X.509 的编辑 Sharon Boeyen，她为我们审阅了 X.509 的相关资料，此外还要感谢 West Publishing 公司，它为我们提供了很多在线的研究资料。

Warwick Ford 于美国马萨诸塞州坎布里奇市
Michael S.Baum 于美国加利福尼亚州洛斯阿尔托斯市

目 录