经济管理学术新视角丛书

ELECTRONIC COMMERCE INFORMATION SECURITY TECHNOLOGY AND ITS APPLICATION

电子商务信息安全技术及其应用

陈　莉◎著

经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

经济管理学术新视角丛书

本专著由“河南省高校科技创新人才支持计划”
（HASTIT）资助出版

ELECTRONIC COMMERCE INFORMATION SECURITY TECHNOLOGY AND ITS APPLICATION

电子商务信息安全技术及其应用

陈　莉◎著

经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

图书在版编目（CIP）数据

电子商务信息安全技术及其应用/陈莉著. —北京：经济管理出版社，2015.10
ISBN 978-7-5096-4024-1

Ⅰ. ①电… Ⅱ. ①陈… Ⅲ. ①电子商务—信息安全—安全技术 Ⅳ. ①F713.36

中国版本图书馆 CIP 数据核字（2015）第 255639 号

组稿编辑：杨 雪
责任编辑：张巧梅
责任印制：司东翔
责任校对：张 青

出版发行：经济管理出版社
（北京市海淀区北蜂窝 8 号中雅大厦 A 座 11 层 100038）
网 址：www. E-mp. com. cn
电 话：（010）51915602
印 刷：北京九州迅驰传媒文化有限公司
经 销：新华书店
开 本：710mm×1000mm/16
印 张：15
字 数：252 千字
版 次：2015 年 10 月第 1 版 2015 年 10 月第 1 次印刷
书 号：ISBN 978-7-5096-4024-1
定 价：49.00 元

目 录

第1章　电子商务安全概述

1.1　电子商务的基本概念

电子商务有广义和狭义的两种解释。根据《联合国国际贸易委员会电子商务示范法》，广义的电子商务是指利用数据信息进行的商业活动，而数据信息是指由电子的、光学的或其他类似方式所产生、传输并存储的信息。狭义的电子商务是指基于互联网这个平台实现商业交易电子化的行为。

欧洲议会关于电子商务的定义是：电子商务是通过电子方式进行的商务活动。它通过电子方式处理和传递数据，包括文本、声音和图像。它涉及许多方面的活动，包括货物电子贸易和服务、在线数据传递、电子资金划拨、电子证券交易、电子货运单证、商业拍卖、合作设计和工程、在线资料获得。它包括了产品（如消费品、专门设备）和服务（如信息服务、金融和法律服务）、传统活动（如健身、体育）和新型活动（如虚拟购物、虚拟训练）。

中国上海市电子商务安全证书管理中心对电子商务给的定义是：电子商务是指采用数字化电子方式进行商务数据交换和开展商务亚务活动。电子商务（Ec）主要包括利用电子数据交换（EDC）、电子邮件（E-mail）、电子资金转账（EFT）及 Internet 的主要技术在个人间、企业间和国家间进行无纸化的业务信息的交换。

电子商务涵盖的范围很广，其模式通常分为以下八种：

（1）企业对企业（Business-to-Business，即 B2B）模式，企业与企业之间通过互联网进行产品、服务及信息的交换。通俗的说法是指进行电子商务交易的供

需双方都是商家（或企业、公司），他们使用 Internet 的技术或各种商务网络平台（如拓商网），完成商务交易的过程。这些过程包括：发布供求信息，订货及确认订货，支付过程，票据的签发、传送和接收，确定配送方案并监控配送过程等。

（2）企业对消费者（Business-to-Consumer，即 B2C）模式，企业通过互联网为消费者提供一个新型的购物环境——网上商店，消费者通过网络在网上购物、在网上支付。由于这种模式节省了客户和企业的时间和空间，大大提高了交易效率，尤其是工作忙碌的上班族，这种模式可以为其节省宝贵的时间。同时，B2C 的电子商务模式也越来越被大众接受。

（3）个人对消费者（Consumer-to-Consumer，即 C2C）模式，个人与个人之间的电子商务。比如一个消费者有一台电脑，通过网络进行交易，把它出售给另外一个消费者，此种交易类型就称为 C2C 电子商务。

（4）企业对政府（Business-to-Government，即 B2G）模式，企业与政府管理部门之间的电子商务，如政府采购、海关报税的平台、国税局和地税局报税的平台等。

（5）线上对线下（Online-to-Offline，即 O2O）模式，将线下商务的机会与互联网结合在一起，让互联网成为线下交易的前台。这样线下服务就可以在线上揽客，消费者可以在线上筛选服务，还有成交可以在线结算，很快达到规模。O2O 的优势在于把网上和网下的优势完美结合，让消费者在享受线上优惠价格的同时，又可以享受线下贴心的服务。

（6）商业机构对家庭（Business-to-Family，即 B2F）模式，是相对于 B2C 模式的一种升级模式，但是它们针对的顾客群体不同。B2F 的营销模式一般以目录+网络销售为主，主要借助于快讯商品广告（Direct Mail，DM）和 Internet 开展销售活动。通过商业机构的 DM 和互联网为消费者提供一个新型的购物环境。

（7）供给方对需求方（Provide-to-Demand，即 P2D）模式，是一种全新的、涵盖范围更广泛的电子商务模式，强调的是供应方和需求方的多重身份，即在特定的电子商务平台中，每个参与个体的供应面和需求面都能得到充分满足，充分体现特定环境下的供给端报酬递增和需求端报酬递增的现象。

（8）门店在线（Online-to-Partner，即 O2P）模式。通过构建各方参与者（厂商—经销商—门店—消费者）多赢的格局，以形成具有核心竞争力的互联网生态

圈，成为相关标准定义者与游戏规则的制定者。其中包括以下三大 P（Platform、Place、People ）作为实现手段：

一是 O2Platform（平台），通过针对区域合作伙伴及门店的应用需求而定制的平台，包括前端平板、后台管理系统、短信平台、400 电话、移动 APP、云服务等。

二是 O2Place（本地化），通过移动互联网的技术手段，构建具有本地化、社交型的线上线下互动的电商平台，帮助道易行区域合作伙伴，推进渠道向社区化、乡镇网点全覆盖，多品牌多品种类型运作，形成富有竞争力的立体化的渠道网络。

三是 O2People（消费者），通过互联网化的产品展示方式与平板综合应用以及渠道全网点的布局优势，结合短信及全国统一 400 电话的手段，推进门店形象、销售及售后服务的标准化，提升消费者满意度，形成长期的竞争优势。

1.2　电子商务面临的安全威胁

随着电子商务在互联网上的日益盛行，网络和电子商务的广泛应用给人们的工作和生活带来了极大的方便。电子商务交易方式使商家能够以高效率、低成本的方式处理业务，同时也给消费者带来了方便、快捷的消费方式。与此同时，电子商务应用中的安全问题也日益严重，没有完整的信息安全保障体系和机制，网上交易将存在极大风险，商业机密信息一旦被攻击者窃取，后果将不堪设想。

在传统交易过程中，由于商家和客户是面对面的，比较容易保证交易过程的安全性。但在电子商务交易过程中，商家和客户是通过网络完成交易的，交易涉及的订单信息、账户信息等各种敏感信息通过公共网络传输，因此，电子商务的交易主体面临着不同的威胁。

1.2.1　商家（商品或服务的提供者）面临的威胁

（1）电子商务系统的安全性受到破坏：入侵者假冒合法客户改变客户数据

(如改变商品的送达地址)、解除客户订单或生成虚假订单。

(2) 竞争者获取商业信息：恶意竞争者以他人名义订购商品，从而了解有关商品的递送状况和商品的库存情况等商业信息。

(3) 客户的资料被竞争者获取，为其所用。

(4) 被他人假冒而损害公司的信誉。这种安全威胁主要包括以下三种方式：①建立与商家服务器名字相同的另一个 WWW 服务器来假冒商家。②制造虚假订单。③假冒成电子商务的参与方，以获得其他人的机密信息。

(5) 客户提交订单后不付款。

(6) 虚假订单。

1.2.2 客户（商品或服务的购买者）面临的威胁

(1) 冒名虚假订单：冒名者以其他客户的名义来订购商品，而且有可能收到商品，而被冒名的客户却被要求付款或返还商品。

(2) 商家信用的威胁：客户付款后，收不到商品。

(3) 客户信息机密性丧失：客户可能将秘密的个人数据或自己的身份数据(如 PIN，电子商务安全协议的分析口令等) 发送给冒名为商家的机构。同时，这些信息在传递的过程中也有可能受到窃听的威胁。

(4) 拒绝服务：攻击者可能向商家的服务器发送大量的虚假订单来挤占它的资源，从而使合法的客户得不到正常的服务。

(5) 电子货币丢失：电子货币可能遭到物理破坏或者被偷窃。这样会给客户带来不可挽回的损失。

根据上述分析可知，电子商务系统遭受攻击的手段可以大致归纳为以下几种：

(1) 伪造 (攻击系统的真实性)：将伪造的虚假消息输入系统，假冒合法人员进入银行专用网络、重放截获的合法消息以实现非法目的、否认消息的接收和发送等。

(2) 窃听 (攻击系统的机密性)：通过搭线与电磁泄漏等手段窃听通信，或对银行专用网络中的业务流量进行分析，获取有用情报。

(3) 篡改 (攻击系统的完整性)：篡改系统中的数据内容，修改消息次序、时间 (延时和重放) 等。

（4）中断（攻击系统的可用性）：破坏系统中的硬件、线路、文件系统等，使系统不能正常工作。

通过上述分析可以得知，电子商务交易主体面临的威胁包括安全和信任关系两个方面。电子商务安全协议是保障电子商务安全、顺利开展的关键技术，电子商务中的交易主体通过安全的、可信赖的电子商务协议建立起相互之间的信任关系，从而完成资金交割与商品交易。然而，电子商务安全协议自身的缺陷和安全漏洞可能导致交易信息遭到恶意修改、伪造等攻击，从而使交易主体的利益受到严重损失。因此，正确掌握电子商务安全协议的安全需求具有重要意义。

1.3　电子商务安全协议

电子商务安全协议是保障电子商务安全、顺利开展的关键技术。电子商务中的交易主体之间通过安全的、可信赖的电子商务协议建立相互的信任关系，从而完成资金交割与商品交易。然而，电子商务安全协议自身的缺陷和安全漏洞，可能导致交易信息遭到恶意修改、伪造等诸多攻击问题，如协议异常中断、不诚实交易方否认自己的行为，以及无法追究不诚实交易方的责任等，都将使诚实交易主体的利益受到严重损失。因此，电子商务安全协议应该具有更全面的安全属性，即不仅要满足一般安全协议具有的认证性、密钥保密性、密钥新鲜性、密钥专有性和完整性等安全属性，而且还要满足原子性、公平性、非否认性、匿名性、可追究性、时限性、不可滥用性等安全属性。

由于电子商务安全协议需要满足更多的安全属性，而且其运行环境复杂、并发性较高，所以设计与分析电子商务安全协议更为复杂。即使是精心设计的协议往往也存在安全漏洞，而且使用非形式的方法也难以发现这些漏洞。因此，要设计一个安全的电子商务安全协议，必须以满足上述安全属性为基本准则，也必须要分析验证其正确性，以及是否满足上述安全属性。

1.4 电子商务安全协议研究现状

电子商务安全协议是电子商务应用的关键技术，是保证电子商务活动正常开展的基础。然而，要设计一个正确的、符合安全目标的、没有冗余的电子商务安全协议非常困难。原因在于：①协议运行环境的复杂性。实际上，当安全协议运行在一个十分复杂的公开环境中，攻击者无处不在，针对不同应用存在不同安全攻击，因此，使用形式化方法完整地刻画出安全协议的运行环境，是一项艰巨的任务。②协议运行的“高并发性”。一个电子商务协议可能同时运行多个实例或与其他电子商务协议同时运行，甚至与其他非电子商务并发执行。另外，分析并发环境下协议安全性能否得到保障也是一件困难的事情。③协议安全属性形式化描述和分析的复杂性。由于协议需要满足多种安全属性，而且有些安全属性之间相互制约，因此，使用形式化方法客观准确地描述协议的各种安全属性，以及使用形式化方法严格验证各种安全属性都是非常复杂的任务。④协议安全漏洞和缺陷的隐蔽性。实践表明，即使是精心设计的协议往往也存在安全漏洞，使用非形式的方法难以发现这些漏洞。使用形式化分析方法严格分析协议安全属性是一件复杂而艰巨的任务。⑤协议安全需求的复杂性。随着电子商务的发展，安全需求不断提高，协议安全属性的分析和验证不断面临新的更大的挑战。

综上所述，电子商务安全协议设计与分析任务复杂，极具挑战性。目前，形式化分析方法是分析电子商务安全协议非常有效的方法，形式化分析不仅能发现协议存在的安全漏洞和缺陷，而且其分析结果还可以用于指导电子商务安全协议的设计，并弥补现有协议中的潜在问题。因此，对电子商务安全协议及其形式化分析方法研究具有重要的理论意义和现实应用价值。

电子商务安全协议形式化分析从 20 世纪 90 年代起发展极为迅速，目前已成为安全协议理论与技术研究领域的重要分支，也随着电子商务的蓬勃发展，成为科技研究前沿问题。

在对电子商务安全协议的安全属性研究方面，电子商务中交易实体身份的认证性、交易数据的机密性、完整性等安全属性已得到了较广泛研究。随着电子商

务的不断发展，电子商务协议的非否认性、可追究性、公平性、原子性、时限性等安全属性也得到了学者们的广泛关注。非否认性是电子商务协议中重要的属性，并且与公平性相关联。最初的非否认协议没有考虑协议的公平性，但研究人员发现非否认协议必须实现公平性，否则协议可能无法保证非否认性。如国际标准化组织 ISO 建议的几种非否认实现机制均不能提供公平性，也不适合应用于电子商务环境中。目前，电子商务安全协议通常采用可信第三方保证交易的公平性和非否认性，根据可信第三方 TTP（Trusted Third Party）介入的程度，非否认协议可分为中介第三方（Inline TTP）协议、在线第三方（Online TTP）协议和离线第三方（Offline TTP）协议。在 Inline TTP 协议中，TTP 参与协议执行的每一步，帮助传递消息或者非否认证据，缺点是容易造成通信和计算瓶颈；在 Online TTP 协议中，TTP 参与协议的执行，但不介入每次消息的传递；在 Offline TTP 协议中，不需要第三方的介入，只有当交易双方产生争议时，第三方才会介入。Zhou 提出了公平的非否认协议，该协议实现了公平非否认性，减少了通过 TTP 的通信量。Franklin 等人提出的半可信第三方协议，在保证公平性的前提下，降低了对 Online TTP 可信度的要求。杜红珍等提出的 Offline TTP 公平非否认协议，进一步降低了对 TTP 可信度的要求。目前，这方面的研究体现在两个方面：一个是降低 TTP 的数据通信量，另一个是降低对 TTP 可信度的要求。在原子性研究方面，Tygar 提出电子交易要满足原子性，并给出了原子性定义。Camp 等提出了一种能够满足匿名性和原子性的电子交易协议，但没有实现公平匿名性。针对此问题，刘文远等提出了一种满足原子性和公平匿名性的电子交易协议。在可追究性的研究方面，Kailar 学者最早针对电子商务安全协议提出可追究性属性，满足可追究性的前提是协议必须满足非否认性。Medvinsky 等提出的匿名电子现金支付协议被证明不满足商家的非否认性目标，进而也被证明不满足可追究性。Deng 等提出的可认证邮件传递协议 CMP1，后来被证明在通信信道不可靠的情况下，不满足其预期非否认目标，故而被证明不满足可追究性。

1978 年，Needham 和 Schroeder 首次提出了安全协议形式化分析的思想。1983 年，Dolev 和 Yao 给出了著名的 Dolev-Yao 模型，该模型以完善的密码学原语为前提，赋予攻击者截获、插入、篡改、伪造、假冒等攻击能力。目前，大多数协议形式化分析方法都是基于 Dolev-Yao 模型提出的。形式化分析的方法主要有：基于逻辑推理的形式化分析技术、基于模型检测的形式化分析技术、基于定

理证明的形式化分析技术和借助图论的串空间（Strand Space）方法。

在基于逻辑推理的形式化分析技术方面，由于 BAN 逻辑成功发现了 Kerberos 等著名协议已知的和未知的漏洞，极大地激发了密码研究者对安全协议形式化分析的兴趣，并由此产生了多类安全协议形式化分析方法。典型的电子商务安全协议逻辑分析方法包括 SVO 逻辑、Kailar 逻辑、非单调动态逻辑 NDL 以及时序逻辑等。其中，SVO 逻辑可用于分析电子商务安全协议的认证性，J. Zhou、Li Botao 等将 SVO 逻辑运用于非否认性的分析。王茜等对 SVO 逻辑进行改进，增加对电子商务协议非否认性和原子性的分析能力；Li Botao 等对 SVO 逻辑进行改进，增加了对非否认性和时限性的分析能力。周典萃等提出了一种分析电子商务安全协议的新工具；王彩芬等将 Kailar 逻辑和 LPC（Logic Process Calculus）方法相结合，提出了一种逻辑分析方法，此方法能够分析电子商务安全协议的可追究性和公平性。卿斯汉在 Kailar 逻辑改进的基础上，提出了一种新的电子商务安全协议形式化分析方法（简称为卿—逻辑）。Mauricio Papa 等将逻辑与 Spi（Spi Calculus Process）演算整合在一起，提出分析电子商务安全协议的形式方法，该方法具有 Dolev-Yao 的许多特性，如用黑盒子的形式表示密码算法，入侵者具有建立、修改、删除信息的能力等。Mauricio Papa 等提出的方法可以分析协议中参与者的知识和行为，但该方法只能说明参与者拥有的知识，不能说明知识或信息的来源，因此无法分析协议的可追究性。陈庆锋等使用 NDL 逻辑对 SET 协议进行了分析。由于传统时序逻辑方法把协议看成封闭式并发系统进行研究，不适合复杂的电子商务安全协议的描述与分析。Kremer 提出一种新的基于博弈的 ATL（Alternating-time Temporal Logic）逻辑分析方法，形式化分析了几个典型的公平电子商务安全协议的公平性等属性。Levente Buttyan 等、文静华等使用基于博弈理论的方法描述和分析了公平交换协议。

在基于状态检测技术的模型检测方法中，具有代表性的是 CSP（通信顺序进程）。1996 年，Lowe 首先应用 CSP 模型和 CSP 模型校验工具 FDR 对 NSPK 协议进行了形式化分析，发现了一个近 17 年来未知的攻击。之后，Roscoe 提出 CSP 与 FDR 结合是形式化分析安全协议的一条新途径，可用于分析不可靠环境下电子商务安全协议的确认发送原子性、原子性及可追究性。另外，Standford 大学的 Mitchel 等使用 Murφ 分析了一些复杂协议，如 Ketheros 协议、SSL 协议等。S. Xu 等、C. John Mitchell 等使用 Murφ 证明了合同签署协议和公平交换协议；

Schneider 使用 CSP 分析非否认协议；Heintze 等人使用 FDR 模式检测分析了 Netbill 和 Digicash 协议；C.Meadows 使用 NRL 分析器分析了 SET 协议；Dominique Bolignano 用模型检测工具 SMV 分析了 Digicash 协议和 Netbill 协议的原子性。在定理证明方面，Bolignano 使用定理证明技术 Coq 分析了 C-SET 协议。

1998 年，Thayer，Herzog 和 Guttma 提出了一种分析密码协议安全性的新方法，称为串空间（Strand Space）方法。它利用图论方法来建立协议中因果关系的模型，但本质上仍是基于代数的分析方法。该模型用串表示参与协议的主体可以执行的事件序列，通过次序关系来刻画协议主体间直观的因果关系，将协议的描述和目标安全属性转化为图结构，借助次序关系理论来研究安全协议的认证和保密属性。串空间模型比较简单，结果表达精确，在不使用自动推理的情况下也能得到可理解且可信赖的证明，同时可有效地避免状态空间爆炸问题。串空间理论的代数证明具有四大优点：①数据项的假设有清晰的语义；②明确、一般性地规定入侵者的行为能力；③能同时分析秘密性和认证性；④详细洞察了协议正确的原因。因此，研究人员经常将这种方法作为安全协议形式化分析的有效的理论基础，并且利用它对所提出的方法进行语义分析，例如，Syverson 为 SVO 逻辑引入串空间语义。

移动电子商务是电子商务重要应用领域之一，在移动环境下，交易主体的高效身份认证和密钥协商问题引起研究人员的广泛关注。Y. Frankel 等、S. Mohan 等、H. Zhang 提出了一些解决方案，但是，这些方案也存在一些问题。例如，认证方案不能在第一时间实现对交易主体的认证，可能会引发拒绝服务攻击等。此外，这些方案普遍引入了公钥基础设施 PKI，用于实现签名与验证、加密与解密，在一定程度上影响了认证效率。

数字商品的微支付交易是电子商务应用中的一种重要类型，如数字商品的按页支付、付费图片下载以及视频点播中的即付即看等。目前，研究人员已提出一些基于 Hash 链的微支付方案，姬东耀等提出的 NMP 方案对 PayWord 方案进行了改进，增加了交易双方的相互认证、数字商品的保密传输、出错处理等功能，增强了交易公平性。但是 NMP 方案没有考虑恶意透支、时限性等问题，而且其效率和安全性也受到 Hash 链机制自身不足的制约。

研究发现，目前在电子商务安全协议设计中存在以下问题：大多数电子商务安全协议安全目标单一，即协议设计通常只考虑满足部分安全属性，甚至有些协

议还不能达到其预期的安全目标。微支付协议设计一般存在不能有效兼顾效率和安全性的问题。电子商务移动认证协议设计，没有充分考虑移动实体资源受限情况，不能在“第一时间”认证交易实体，易遭受拒绝服务攻击等。研究发现，电子商务安全协议逻辑分析方法存在下列问题：虽然以简单、实用著称的逻辑分析方法，在电子商务安全协议分析方面已取得了丰硕的成果，但是，多数典型的逻辑分析方法只能对协议的某一种安全属性进行分析。其改进方法也只能针对协议相关的安全属性。而且，有些逻辑自身还缺乏形式化语义分析。本书围绕上述问题，深入研究典型的电子商务安全协议及其逻辑分析方法，并提出了有效的解决方案。

第 2 章　电子商务安全基础设施

公钥基础设施 PKI 是目前部署电子商务安全，保障信息安全最有效和得到广泛认可的技术。本章介绍公钥基础设施 PKI 的概念、体系结构、安全服务、标准以及实施 PKI 的方法和意义。

2.1　PKI 综述

PKI 是“Public Key Infrastructure”的缩写，意为“公钥基础设施”。简单地说，PKI 技术就是利用公钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制，在这一体制中，加密密钥与解密密钥各不相同，发送信息的人利用接收者的公钥发送加密信息，接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性，又能保证信息具有的不可抵赖性。目前，公钥体制广泛地用于 CA 认证、数字签名和密钥交换等领域。

PKI 是基于公开密钥理论和技术建立起来的安全体系，是提供信息安全服务的具有普适性的安全基础设施。该体系在统一的安全认证标准和规范基础上提供在线身份认证，是 CA 认证、数字证书、数字签名以及相关安全应用组件模块的集合。作为一种技术体系，PKI 可以作为支持认证、完整性、机密性和不可否认性的技术基础，从技术上解决网上身份认证、信息完整性和抗抵赖等安全问题，为网络应用提供可靠的安全保障。但 PKI 绝不仅仅涉及技术层面的问题，还涉及电子政务、电子商务以及国家信息化的整体发展战略等多层面问题。PKI 作为国家信息化的基础设施，是相关技术、应用、组织、规范和法律法规的总和，是一个宏观体系，其本身就体现了强大的国家实力。PKI 的核心是要解决信息网络空