華夏英才基金學術文庫

谢晓尧 著

电子商务网络协议的形式化分析理论与应用

科学出版社
www.sciencep.com

華夏英才基金學術文庫

电子商务网络协议的形式化分析理论与应用

谢晓尧 著

科学出版社
北京

内 容 简 介

本书叙述了与信息安全有密切联系的基于网络电子商务协议的形式化分析理论方法与实际应用。具体内容包括：电子商务协议的形式化逻辑分析方法、通用形式化 Petri 网模型分析方法、有穷自动机模型检测分析方法、安全认证和交易的基本协议，以及协议的有色 Petri 网模型及分析的软件工具 CPN Tools 等。同时，本书应用这些分析方法和工具具体分析了相关的认证和支付等协议。

本书适合于高等院校计算机专业、电子商务专业高年级本科生和研究生阅读，也可供科研人员参考。

图书在版编目(CIP)数据

电子商务网络协议的形式化分析理论与应用/谢晓尧著. —北京：科学出版社，2008

（华夏英才基金学术文库）

ISBN 978-7-03-020032-7

Ⅰ. 电… Ⅱ. 谢… Ⅲ. 电子商务-计算机网络-通信协议 Ⅳ. F713.36 TN915.04

中国版本图书馆 CIP 数据核字(2007)第 203282 号

责任编辑：姚庆爽/责任校对：陈玉凤

责任印制：刘士平/封面设计：王 浩

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

源海印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2008 年 1 月第 一 版 开本：B5(720×1000)

2008 年 1 月第一次印刷 印张：10

印数：1—3 000 字数：184 000

定价：30.00 元

（如有印装质量问题，我社负责调换〈明辉〉）

序

21 世纪是信息的时代。信息已成为一种重要的战略资源，信息技术改变着人们的生活和工作方式，社会的信息化程度大大提高，信息产业成为世界第一大产业。信息的获取、处理和安全保障能力成为一个国家综合国力的重要组成部分。

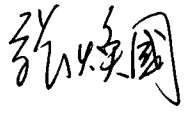
当前，一方面，信息技术与产业欣欣向荣，处于空前繁荣的阶段。可是另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

计算机网络的迅速发展和广泛应用，正引起社会和经济的深刻变革。计算机网络已经成为我们生活和工作中的一个不可分割的组成部分。基于计算机网络的“电子商务”正在兴起。它们的兴起在商务领域引起了一场革命。对此，发展我国的电子商务已成为建设具有中国特色社会主义强国的不可回避的选择。然而，计算机网络的开放性等原因，使得信息安全问题成为影响电子商务发展和应用的主要技术障碍之一。因此，必须研究解决电子商务系统中信息安全问题，发展我国的电子商务事业。

谢晓尧教授长期从事电子商务与信息安全领域的科学研究和教学工作。他潜心研究其中的基础理论，结合科研项目攻克关键技术，并面向应用解决实际问题。长期的教学和科研实践使他具有坚实的理论基础，并积累了丰富的实践经验。他基于自己的研究工作，撰写了《电子商务网络协议的形式化分析理论与应用》。这一著作是他研究成果和心得的结晶。

该书针对目前电子商务协议研究中重视加密技术而忽视协议逻辑设计的问题，采用形式化的分析工具来精确描述和仿真协议的行为，验证协议能否达到预期的目标，从而确保电子商务协议设计的正确性。该书的主要内容包括：电子商务协议的形式化逻辑分析方法、通用形式化 Petri 网模型分析方法、有穷自动机模型检测分析方法、安全认证和交易的基本协议，以及协议的有色 Petri 网模型及分析的软件工具 CPN Tools 等。同时，该书应用这些分析方法和工具，对相关的认证和支付协议进行了具体分析。

相信该书的出版能够为计算机和电子商务专业的研究生提供一本合适的教材，为计算机和相关领域的技术人员提供一本好的技术参考书。



武汉大学 教授

2007 年 10 月 28 日

前　言

当今时代已进入互联网络的时代，网络的飞速发展给社会带来了巨大的变革，电子商务以及电子政务的蓬勃发展和应用就是一个典型的例子。但这种应用及网络的开放性也带来了新的信息安全问题。信息安全已成为影响国家安全、社会稳定和经济发展的重要因素。基于信息安全的电子商务协议的设计和应用，就是为了保证网络和信息的安全。协议涉及两方面的内容：一是加密技术的选用，二是协议逻辑的设计。通常加密技术备受重视而协议逻辑设计则被忽略，这就为黑客的攻击留下许多隐患和漏洞。

针对协议逻辑出现的问题，为保证基于信息安全的电子商务协议设计的正确性，就需要用形式化的分析工具来精确描述和仿真协议的行为、协议所要达到的目标以及能否达到其预期的目标。

本书的第 1 章概论说明了信息安全的重要性，给出了信息安全的定义和网络的安全体系结构。

第 2 章介绍了电子商务的定义及电子商务的安全性。具体涉及协议的安全性、设计原则和形式化分析方法分类。

第 3 章论述了目前流行的电子商务协议的形式化逻辑分析方法。阐述了基于信息逻辑的形式化方法用于分析认证协议的安全性的 BAN 逻辑，分析电子商务协议的不可否认性的 Kailar 逻辑以及分析电子商务协议的可追究性和公平性的卿周逻辑等。

第 4 章陈述了电子商务协议的通用形式化 Petri 网模型分析方法，介绍了分析中常用的 Petri 网模型，如 P/T 网、有色网、常量弧有色网等及 Petri 网的基本知识。通过第 4 章的学习，读者即可灵活的应用 Petri 网。

第 5 章介绍了电子商务协议的形式化有穷自动机模型检测分析方法。具体内容包括确定的有穷自动机 DFA 的定义、通道 DFA、协议实体 DFA。

第 6 章分两个部分论述了基于电子商务安全认证的基本协议和交易协议。认证涉及 Needham-Schroeder 认证协议、Kerberos 认证协议、Otway-Rees 认证协议。交易涉及了 IBS 支付协议、CMP1 及 CMP2 非否认协议、Zhou-Gollman 非否认协议、ISO 非否认协议 M2、卿斯汉非否认协议、ISI 支付协议。

第 7 章描述了基于公钥基础设施 PKI 的安全认证协议。在此基础上，第 8 章提出了基于工商电子政务的安全认证协议。根据这个安全认证协议在第 9 章用 Petri 网协议模型技术，构造了单向认证协议和双向认证协议的 Petri 网模型的状

态空间，并进行了仿真分析。通过仿真分析，找到了协议的安全漏洞，完善了认证协议。

第10章利用有穷自动化理论，构造了电子交易中的支付协议的状态模型。通过状态仿真，证明了支付协议满足不可否认性却不满足公平性。为此修改了支付协议并证明了修改过的协议满足公平性。

第11章详细介绍了协议的有色Petri网模型及分析的软件工具CPN Tools。并用该工具具体分析了认证等协议。

本书以计算机专业和电子商务专业的高年级本科生、研究生为主要对象，亦可供计算机科研人员和相关专业的读者参考。

特别说明，高建瓴副教授帮助整理了本书并完成了3.3节、6.2.8～6.2.10小节的内容，卢敏高工撰写了本书第11章。

在本书的写作过程中张焕国教授、李祥教授提出了许多宝贵的意见和建议。相关的书籍和文章给了我有益的启迪。同时在给研究生开设这门课程时与学生的讨论，也对我写作本书很有帮助。青年教师陈彦，研究生谢婷、于徐红、吕波、杨惠仁、张安钰、王蕾、杨义在等为本书的录入和画图做了大量细致的工作。在此，我向他们表示深深的感谢。

本书得到华夏英才基金资助，科学出版社为本书的出版给予了大力支持，在此一并表示衷心的感谢。

本书是作者近六年研究工作的总结，疏漏在所难免，敬请读者批评指正。我们的E-mail地址是xyx@gznu.edu.cn。

谢晓尧

2007年9月

于贵州师范大学

目　录

序
前言
第 1 章　概论 …… 1
1.1　信息安全的基本定义 …… 1
1.2　网络的安全问题 …… 1
1.3　网络安全体系结构 …… 3
第 2 章　电子商务协议的形式化分析理论基础 …… 7
2.1　电子商务的定义 …… 7
2.2　电子商务协议的安全性 …… 7
2.2.1　电子商务协议的安全性 …… 7
2.2.2　电子商务协议的设计原则 …… 9
2.2.3　电子商务协议的安全分析 …… 11
2.2.4　电子商务协议形式化分析方法分类 …… 11
第 3 章　电子商务协议的形式化逻辑分析方法 …… 15
3.1　BAN 逻辑 …… 15
3.1.1　BAN 逻辑公式 …… 15
3.1.2　BAN 逻辑的推理规则 …… 16
3.1.3　BAN 逻辑的评价 …… 16
3.2　Kailar 逻辑 …… 17
3.2.1　Kailar 逻辑公式 …… 17
3.2.2　Kailar 逻辑的推理规则 …… 18
3.3　NDL 逻辑 …… 19
3.3.1　NDL 逻辑的语法 …… 19
3.3.2　NDL 逻辑的推理规则 …… 20
3.4　卿周逻辑 …… 21
3.4.1　卿周逻辑的语法 …… 21
3.4.2　卿周逻辑的推理规则 …… 22
第 4 章　电子商务协议的通用形式化 Petri 网模型分析方法 …… 24
4.1　Petri 网概述 …… 24
4.2　Petri 网的定义 …… 24

4.3 Petri 网的应用实例 …… 25
4.4 Petri 网的特性 …… 26
4.4.1 保守网 …… 26
4.4.2 有界网 …… 27
4.4.3 活动性 …… 29
4.4.4 并发与冲突 …… 29
4.5 Petri 网的扩充 …… 29
4.5.1 输入函数和输出函数的扩充 …… 29
4.5.2 触发条件的扩充 …… 30
4.5.3 旗标和库所的扩充（着色 Petri 网） …… 30
4.6 Petri 网的替换与合成 …… 30
4.7 常用的 Petri 网模型 …… 31
4.7.1 库所/变迁网（P/T 网）的形式化定义 …… 31
4.7.2 有色网的形式化定义 …… 32
4.7.3 常量弧有色网的形式化定义 …… 32
4.8 Petri 网的分析 …… 33
4.8.1 常量弧网 …… 33
4.8.2 库所/变迁网（P/T 网） …… 37
4.8.3 有色网 …… 39
第 5 章 电子商务协议的形式化有穷自动机模型检测分析方法 …… 42
5.1 有穷自动机的定义 …… 42
5.2 传输通道类别 …… 43
5.3 通道 DFA …… 44
5.4 协议实体 DFA …… 46
5.5 DFA 的简化 …… 47
5.6 DFA 的合成 …… 48
第 6 章 基于电子商务安全认证和交易的基本协议 …… 52
6.1 安全认证的基本协议 …… 52
6.1.1 Needham-Schroeder 认证协议 …… 52
6.1.2 Kerberos 认证协议 …… 53
6.1.3 Otwag-Rees 认证协议 …… 55
6.2 电子交易的基本协议 …… 56
6.2.1 网上交易协议遵循的原则 …… 56
6.2.2 IBS 支付协议 …… 57
6.2.3 CMP1 及 CMP2 非否认协议 …… 58

6.2.4 Zhou-Gollman 非否认协议 …… 58
6.2.5 ISO 非否认协议 M2 …… 59
6.2.6 卿斯汉非否认协议 …… 59
6.2.7 ISI 支付协议 …… 60
6.2.8 SSL（安全套接层协议） …… 61
6.2.9 SET 协议 …… 62
6.2.10 PGP（Pretty Good Privacy）协议 …… 63
第 7 章 基于公钥基础设施 PKI 的安全认证协议 …… 64
7.1 PKI 安全体系结构 …… 64
7.2 安全认证体系结构标准 X.509 …… 65
7.2.1 X.509 的简单认证程序 …… 66
7.2.2 X.509 的强认证程序 …… 67
7.2.3 X.509 的证书内容 …… 67
7.3 安全认证的目录存取协议 LDAP …… 69
第 8 章 基于工商管理的安全认证协议 …… 71
8.1 认证协议的用户需求 …… 71
8.2 安全认证协议的功能和机制 …… 72
8.3 安全认证协议的协议元素 …… 74
8.4 认证协议的形式化规定 …… 76
8.5 单向认证协议 …… 76
8.6 双向认证协议 …… 77
第 9 章 安全认证协议的 Petri 网模型 …… 79
9.1 单向认证协议的 Petri 网模型 …… 79
9.1.1 构建 A 主体 Petri 网模型 A …… 79
9.1.2 构建 S 主体 Petri 网模型 S …… 80
9.1.3 构建 B 主体 Petri 网模型 B …… 81
9.1.4 A、B、S Petri 网模型的合并 …… 81
9.2 双向认证协议的 Petri 网模型 …… 82
9.3 安全认证协议模型的仿真分析 …… 86
9.3.1 认证协议的要素 …… 86
9.3.2 安全认证协议的描述语言 …… 88
9.3.3 单向安全认证协议的具体仿真及实现 …… 93
9.3.4 双向认证协议的具体仿真及实现 …… 98
第 10 章 支付协议的有穷自动机模型 …… 102
10.1 支付协议 …… 102

10.2 工商支付协议的形式化描述 …… 102
10.3 支付协议的有穷自动机模型 …… 103
10.4 支付协议满足不可否认性的仿真分析 …… 105
10.5 支付协议满足公平性的仿真分析 …… 107
第 11 章 协议的有色 Petri 网模型及分析 …… 112
11.1 CP _ Net 简介 …… 112
11.2 CPN Tools 简介 …… 112
11.2.1 CPN Tools 安装 …… 113
11.2.2 CPN Tools 界面 …… 113
11.2.3 CPN Tools 文件格式 …… 113
11.2.4 CPN 网络的载入、创建与保存 …… 114
11.3 CPN ML 语言 …… 114
11.3.1 标识符 …… 114
11.3.2 颜色集 …… 115
11.3.3 变量 …… 118
11.3.4 函数 …… 119
11.3.5 常量 …… 120
11.4 CPN 网的有关操作 …… 121
11.4.1 网络编辑 …… 121
11.4.2 添加/编辑声明 …… 121
11.4.3 添加/编辑标注 …… 122
11.4.4 文本编辑 …… 123
11.4.5 布局编辑 …… 123
11.4.6 有色 Petri 网的分析 …… 123
11.5 协议的 Petri 网模型 …… 127
11.5.1 Needham-Schroedor 公钥认证协议 …… 127
11.5.2 Needham-Schroedor 公钥认证协议的 Petri 网模型 …… 128
11.6 基于 Petri 网模型的安全协议分析方法 …… 130
11.6.1 基于 Petri 网的安全协议分析方法和步骤 …… 130
11.6.2 NS 协议的分析 …… 132
11.7 用 CPN tools 工具来分析协议 …… 137
11.7.1 用 CPN tools 工具分析协议的方法和步骤 …… 138
11.7.2 用 CPN tools 工具来分析 Needham-Schroedor 公钥认证协议 …… 138
参考文献 …… 145

第1章 概 论

当人类进入20世纪，科学技术进步的速度就不断加快。从人类发明电话，到电话用户达到5000万，历史足足走了七十四年。20世纪90年代Internet的出现到网上用户达到5000万，时间仅仅花了短短的五年。进入21世纪的今天，Internet用户继续以每年60%的速率增加，网络通信量更是以每年80%的速率递增。Internet已经成为我们生活和工作的一个组成部分。因此可以说，当今时代已进入互联网络的时代，网络的飞速发展给社会带来了巨大的变革，但其开放性也带来了新的信息安全问题。信息安全已成为影响国家安全、社会稳定和经济发展的重要因素。

1.1 信息安全的基本定义

由于信息是重要的战略资源，计算机系统集中管理着国家和企业的政治、军事、金融、商务等重要信息，因此计算机系统已成为不法分子的重要攻击目标。又由于计算机系统本身的脆弱性和网络的开放性，使得信息安全成为世人关注的社会问题，并因此成为信息学科的热点研究领域。

从一般意义来说，信息安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

这个定义明确了信息安全从多个侧面来衡量，即数据的保密性（secrecy）、数据的真实性（authenticity）、数据的完整性（integrity），以及与信息使用者有关的安全概念：认证（authentication）、可追究性（requiring accountability）和公平性（fairness）。保密性是指数据只能被授权用户读取；真实性是指数据真实无伪；完整性是指数据正确无误、完整不缺；认证是指对称谓者（人或事）是否真实有效的确认；可追究性是指用户无法否认其执行的操作，迫使用户对自己的行为负责；公平性则是针对使用信息进行交易的双方用户在交易时必须公平。

1.2 网络的安全问题

随着网络和网上业务的发展，信息安全的内容也跟着发生变化和扩展。网络由封闭的计算机网络发展为开放的互联网络，业务由简单的数据通信发展为网上

交易。网络信息安全大致经历了三个发展过程：数据安全、系统安全、交易安全。

数据安全是计算机网络时代的基本安全要求，主要包括与数据安全相关联的技术手段，包括传输数据和存储数据安全，最基础的安全构件是机密性、完整性和访问控制。数据的机密性和完整性可以由算法技术保证，而访问控制则与授权机制结合才能起作用。

系统安全是开放的互联网络时代的最基本安全要求，主要包括与信息系统运行相关的技术手段，含边界和计算环境安全。最基础的安全构件是保护、探测和响应。所用基本技术是防火墙、VPN 加密隧道、IDS 入侵检测、防病毒等。

交易安全是网络交易时代的最基本安全要求，为交易（transaction）提供鉴别性、负责性和审计性。鉴别性和负责性证明和审计服务。最基础的安全构件是鉴别性、负责性和审计性。鉴别性和负责性是通过主体的信任逻辑（trustlogic）和客体的相信逻辑（belieflogic）来证明；负责性则提供行为（action）负责性证明和内容（contents）负责性证明；审计性对整个交易提供全程监控，并提供回执证明。交易安全靠认证系统来保证。认证系统是以交易安全为目的的。它的发展大大拓宽了信息安全的内容。

互联网的高速发展及其开放性，导致网络的抗攻击能力愈来愈脆弱。这些攻击，主要是来自两个方面：外部的和内部的。根据 symantec 公司的统计，来自 Internet 上的攻击行为和内部安全威胁呈上升趋势，危害性严重（图 1.1）。

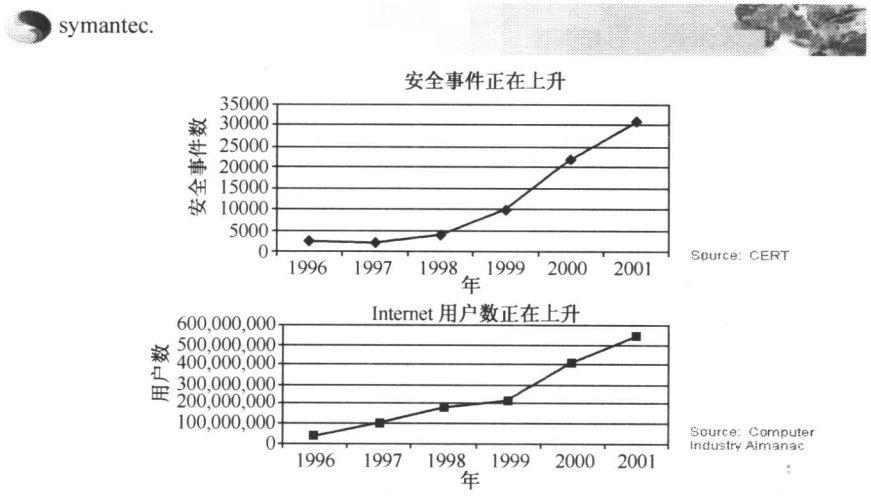


图 1.1 Internet 上的安全事件和用户数呈上升趋势

这些威胁对各机构信息资产的保密性、完整性和真实性构成直接损害，而且这些安全事件的频率和复杂性正在增加（图 1.2）。

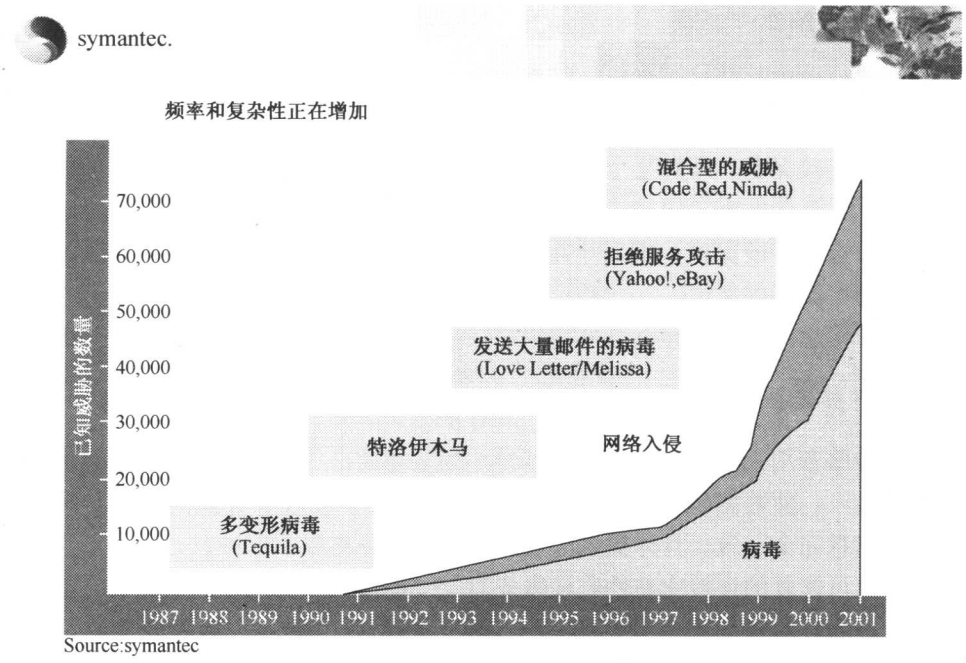


图 1.2 安全事件的频率和复杂性正在增加

1.3 网络安全体系结构

信息安全及网络安全技术是一门新兴科学，它涉及众多领域，许多方面还不成熟。为了适应网络技术的发展，ISO 的计算机专业委员会（ISO/IEC/JTC1/SC21）根据 OSI/RM 制定了一个网络安全体系结构（ISO7498-2N）。针对网络系统受到的威胁，ISO7498-2N 提出了六类安全服务。

1. 对等实体鉴别服务

这种服务是在两个开放系统同等层中的实体建立连接和数据传送期间，为提供对连接实体身份的鉴别而规定的一种服务。这种服务防止假冒实体或重放以前的连接，也即防止伪造连接初始化这种类型的攻击。这种鉴别服务可以是双向的也可以是单向的。

2. 访问控制

访问控制服务可以防止未经授权的用户非法使用系统资源。这种服务不仅提供给单个用户，也可以提供给一个封闭的用户组中的所有用户。

3. 数据保密

数据保密服务的目的是保护网络中各系统之间交换的数据，防止因数据被截获而造成的泄密。这种服务包括以下内容。

（1）连接保密，即对某个连接上所有数据提供保密。

（2）无连接保密，即对一个无连接的数据报的所有用户提供保密。

（3）选择字段保密，即对一个协议数据单元（PDU）中的用户数据的一些经选择的字段提供保密。

（4）信息流安全，即对有可能从观察信息流就能推导出的信息提供保护。

4. 数据完整性

这种服务用来防止非法实体（用户）的主动攻击（如对正在交换的数据进行修改、插入，使数据延时以及丢失数据等），以保证接收方收到的信息与发送方发送的信息完全一致。具体提供的数据完整性服务有以下五种。

（1）可恢复的连接完整性：该服务对一个连接上所有用户的数据的完整性提供保障，而且对任何服务数据单元（SDU）的修改、插入、删除或重放都使之复原。

（2）无恢复的连接完整性：该服务除了不具备恢复功能外，其余同（1）。

（3）选择字段的连接完整性：该服务提供在连接上传送的选择字段的完整性，能确定所选字段是否被修改、插入、删除或重放。

（4）无连接完整性：该服务提供单个无连接 SDU 的完整性，能确定收到的 SDU 是否已被修改。

（5）选择字段无连接完整性：该服务提供单个无连接 SDU 中各个选择字段的完整性，能确定选择字段是否被修改。

5. 数据源认证

这是 N 层向第 $N+1$ 层提供的服务，它用来确保数据是由合法实体发出的，它为 $N+1$ 层提供对数据源的对等实体进行认证，以防假冒。

6. 不可否认

这个服务用来防止发送方发送数据后否认自己发送过数据，或接收方收到数据后否认自己收到过数据。该服务由以下两种服务组成。

（1）不可否认发送：这种服务向数据接收者提供数据源的证据，从而可防止发送者否认发送过这个数据。

（2）不可否认接收：这种服务向数据发送者提供数据已交付接收者的证据，

因而接收者事后不能否认曾收到此数据。

上面这两种服务实际是一种数字签名服务。

为了实现上述各种服务，ISO7498-2N 建议采用以下八种安全机制。

1）加密机制

加密是提供数据保护的最常用的方法。按密钥类型分，加密算法可分为对称密钥加密算法和非对称密钥（又叫做公开密钥）加密算法两种；按密码体制分，可分为序列密码和分组密码算法两种。用加密的方法与其他技术相结合，可以提供数据的保密性和完整性。除了对话层不提供加密保护外，加密可在其他各层上进行。与加密机制伴随而来有密钥管理机制。

2）数字签名机制

数字签名是解决网络通信中特有的安全问题的有效方法。当通信双方发生下列情况时，就会产生安全问题。

（1）否认：发送者事后不承认自己已发送过某份文件。

（2）伪造：接收者伪造一份文件，声称它发自发送者。

（3）冒充：网上的某个用户冒充另一个用户接收或发送信息。

（4）篡改：接收者对收到的信息进行部分篡改。

以上安全问题与社会生活中的类似问题相近。在社会生活中，用手写签名的办法有效地解决了这类问题，而在网络中则采用数字签名机制解决这类问题。

3）访问控制机制

访问控制规则是事先确定的规则决定主体对客体的访问是否合法。当一个主体试图非法访问一个未经授权的客体时，该机制将拒绝这一企图，并附带向审计跟踪系统报告这一事件。审计跟踪系统将产生报警信号或形成部分追踪审计信息。网络上的访问控制机制类似于单个计算机系统上的访问控制机制。

4）数据完整性机制

数据完整性包括两种形式：一种是数据单元的完整性，一种是数据单元序列的完整性。数据单元完整性包括两个过程，一个过程发生在发送实体，另一个过程发生在接收实体。保证数据完整性的一般方法是：发送实体在一个数据单元上加一个标记，这个标记是数据本身的函数，如一个分组校验（类似于 CRC 校验），或密码校验函数，它本身是经过加密的。接收实体产生一个对应标记，并将所产生的标记与接收的标记相比较，以确定在传输过程中数据是否被修改过。

数据单元序列的完整性是要求数据编号的连续性和时间标记的正确性（不是过时的），以防止假冒、丢失、重发、插入或修改数据。

5）交换认证机制

交换认证是以交换信息的方式来确认实体身份的机制。用于交换认证的技术有：

（1）口令：由发方实体提供，收方实体检测。

（2）密码技术：将交换的数据加密，只有合法用户才能解密，得出有意义的明文。在许多情况下，这种技术与下列技术一起使用：

① 时间标记和同步时钟；

② 双方或三方“握手”；

③ 数据签名和公证机构。

（3）利用实体的特征或所有权。这时常采用的技术是指纹识别和身份卡等。

6）业务流量填充机制

这种机制主要是对抗非法者在线路上监听数据并对其进行流量和流向分析。采用的方法一般由保密装置在无信息传输时，连续发生伪随机序列，使得非法者不知哪些是有用信息，哪些是无用信息。

7）路由控制机制

在一个大型网络中，从源节点到目的节点可能有多条线路可以到达，有些线路可能是安全的，而另一些线路是不安全的。路由控制机制可使信息发送者选择特殊的路由，以保证数据安全。

8）公证机制

在一个大型网络中，有许多节点或端节点。在使用这个网络时，并不是所有用户都是诚实的、可信的，同时也可能由于系统故障等原因使信息丢失、迟到等，这很可能会引起责任问题。为了解决这个问题，就需要有一个各方都信任的实体——公证机构，如同一个国家设立的公证机构一样，提供公证服务，仲裁出现的问题。

一旦引入公证机制，通信双方进行数据通信时必须经过这个机构来交换，以确保公证机构能得到必要的信息，供以后仲裁。

第 2 章　电子商务协议的形式化分析理论基础

2.1　电子商务的定义

电子商务，也称电子贸易（electronic commerce，EC），是指所有利用 Internet、Intranet、Extranet 来解决商业交易问题，降低产供销成本，开拓新的市场，创造新的商机，通过采用新的网络技术手段来增加企业利润的所有商业活动。它是在 Internet 开放的网络环境下，基于浏览器服务器应用方式，实现消费者的网上购物，商户之间的网上交易和在线电子支付的一种新型的商业运营模式。

Internet 上的电子商务可以分为三个方面：信息服务、交易和支付。主要内容包括：电子商情广告、电子选购和交易、电子交易凭证的交换、电子支付与结算以及售后的网上服务等。主要交易类型有企业与个人的交易（B to C 方式）和企业之间的交易（B to B 方式）两种。参与电子商务的实体有四类：顾客（个人消费者或企业集团）、商户（包括销售商、制造商、储运商）、银行（包括发卡行、收单行）和认证中心。

与传统的商业系统相比，电子商务具有交易花费成本低、资金更安全、资金结算速度快、节省人力物力、方便等特点。

2.2　电子商务协议的安全性

目前，已设计出的电子商务协议有许多，但有些刚一发表便被发现有缺陷和漏洞，会受到攻击。造成这种现象的原因有很多，但最主要的还是因为协议的设计者对安全需求定义研究得不够彻底，并且对设计出来的协议也没有进行足够的安全性分析。

2.2.1　电子商务协议的安全性

1. 有效性（availability）

EC 以电子形式取代了纸张，那么如何保证这种电子形式的贸易信息的有效性则是开展 EC 的前提。EC 作为贸易的一种形式，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。因此，要对网络故障、操作错误、应用