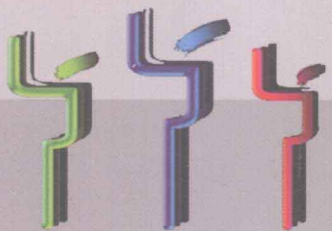
AnQuan

普通高校信息安全系列教材

王 聪 刘 军
王孝国 于振伟 编 著

安全协议原理与验证

ANQUAN XIEYI
YUANLI YU YANZHENG



北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书介绍安全协议及其验证方法，主要内容包括三个部分：1. 基础知识，包括安全协议基本原理介绍、安全性分析以及密码学基础；2. 安全协议原理，包括安全协议概述、经典的密码交换及认证协议、电子商务协议以及应用中的安全协议；3. 安全协议的分析与验证方法，包括 BAN 逻辑、BAN 类逻辑、Kailar 逻辑、CS 逻辑、串空间理论及 CSP 方法等。

本书较为全面、深入地介绍了信息安全体系中的安全协议原理及安全协议的分析验证方法。内容安排由浅入深，重点突出，涵盖了当前安全协议研究领域的主要成果。

本书可作为高等院校信息安全、计算机、通信等专业高年级本科生和研究生教材，也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目(CIP)数据

安全协议原理与验证/王聪等编著. --北京：北京邮电大学出版社，2011.8

ISBN 978-7-5635-2672-7

Ⅰ.①安… Ⅱ.①王… Ⅲ.①计算机网络—安全技术—通信协议 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 125810 号

书　　名：安全协议原理与验证

作　　者：王　聪　刘　军　王孝国　于振伟

责任编辑：满志文

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路 10 号(邮编：100876)

发 行 部：电话：010-62282185　传真：010-62283578

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：北京联兴华印刷厂

开　　本：787 mm×960 mm　1/16

印　　张：20

字　　数：433 千字

版　　次：2011 年 8 月第 1 版　2011 年 8 月第 1 次印刷

ISBN 978-7-5635-2672-7　　定　价：36.00 元

前言

人类正在经历着自工业革命以来最为深刻的信息革命，在这场信息革命中，信息系统作为信息处理及信息传输的重要工具起着举足轻重的作用。然而，信息系统也有其两面性。一方面，它有力地推进了我国的信息化进程，促进了国民经济增长、社会发展和文明进步，增强了经济、科技、军事实力。另一方面信息系统的广泛应用也给国家安全、社会稳定和经济发展带来了许多新的安全威胁。因此，我们在发展信息系统的同时，必须对其安全性加以关注。

随着网络时代的来临，互联网的规模和应用领域不断扩展，在国家信息化建设中，其基础性、全局性的地位和作用日益增强，网络安全问题已经成为影响社会经济发展和国家发展战略的重要因素，是当前世界各国共同关注的焦点。

安全协议是以密码学为基础的协议，它在网络和分布式系统中提供各种各样的安全服务，在网络信息系统安全中占据重要地位。为了减轻由于信息系统遭受攻击所带来的危害，多种安全协议被设计开发出来提供安全保障。

近三十年来，安全协议的研究取得了丰硕的成果，为了满足各种各样的网络应用，提出了大量安全协议，但是后来的研究表明这些安全协议大多数都含有这样或者那样的安全漏洞。所以安全协议的设计与验证一直以来都是信息安全科学中的重难点问题。

本书较为全面、深入地介绍了信息安全体系中的基础密码协议、安全协议原理及安全协议的分析验证方法，按照由浅入深的原则，将全书分为 13 章，内容包括三大部分：1. 基础知识，内容包括安全协议基本原理介绍、安全性分析以及密码学基础；2. 安全协议原理，内容包括安全协议概述、经典的密码交换及认证协议、电子商务协议以及应用中的安全协议；3. 安全协议的分析与验证方法，内容包括 BAN 逻辑、BAN 类逻辑、Kailar 逻辑、CS 逻辑、串空间理论及 CSP 方法等。

本书由王聪统稿及定稿，刘军、王孝国、于振伟参加了部分编写工作。

本书的写作得到了解放军理工大学通信工程学院电子信息工程系孟凡秋主任、王衍波教授的鼓励、支持和帮助。

在本书的写作过程中，中国科学院软件研究所信息安全国家重点实验室的雷新锋博

士提供了大量资料；解放军理工大学通信工程学院电子信息工程系信息技术教研室的杨健、周海刚、黄勇、王志祥等同志给予了很多帮助，作者在此一并表示感谢。

本书可作为高等院校信息安全、计算机、通信等专业高年级本科生和研究生教材，也可供从事相关专业的教学、科研和工程技术人员参考。

由于作者水平有限，书中纰漏在所难免，恳请广大读者批评指正。

作　者

目 录

第一部分 基础知识

第 1 章 引言 …… 3

1.1 安全协议的研究背景、基本概念 …… 3
1.1.1 安全协议的研究背景 …… 3
1.1.2 安全协议的基本概念 …… 4
1.2 安全协议的安全性分析 …… 5
1.2.1 秘密性 …… 5
1.2.2 认证性 …… 5
1.2.3 完整性 …… 5
1.2.4 不可否认性 …… 5
1.2.5 公平性 …… 6
1.2.6 原子性 …… 6
1.2.7 匿名性 …… 6
1.3 安全协议的形式化分析技术概述 …… 6
1.3.1 安全协议形式化分析方法概述 …… 6
1.3.2 基于知识与信念的逻辑推理方法 …… 8
1.3.3 基于代数模型的状态检验方法 …… 9
1.3.4 基于不变集的代数定理证明方法 …… 10
1.4 本书的安排 …… 11

第 2 章 密码学基础 …… 14

2.1 密码学概述 …… 14
2.1.1 密码学的发展过程 …… 14

2.1.2 密码学的基本概念…… 15
2.2 密码体制…… 16
2.3 对称密钥密码体制…… 17
2.3.1 代换密码…… 17
2.3.2 数据加密标准 DES …… 19
2.3.3 高级数据加密标准 AES …… 27
2.4 公钥密码体制…… 32
2.4.1 单向陷门函数…… 33
2.4.2 RSA 密码体制 …… 34
2.4.3 MH 背包体制 …… 35
2.5 数字签名…… 37
2.5.1 数字签名的基本概念…… 37
2.5.2 数字签名方案…… 38
2.5.3 RSA 数字签名 …… 38
2.6 哈希函数…… 39
2.6.1 哈希函数基本概念…… 39
2.6.2 几种常用哈希函数介绍…… 40
2.7 本章小结…… 45
习题 …… 46

第二部分 安全协议原理

第 3 章 安全协议概述 …… 49

3.1 概述…… 49
3.2 安全协议分类…… 50
3.3 安全协议的缺陷…… 52
3.4 安全协议的威胁模型…… 53
3.5 针对安全协议的攻击…… 54
3.5.1 重放攻击…… 55
3.5.2 中间人攻击…… 55
3.5.3 并行会话攻击…… 55
3.5.4 反射攻击…… 56
3.5.5 交错攻击…… 57

3.5.6 归因于类型缺陷的攻击 …… 57
3.5.7 归因于姓名遗漏的攻击 …… 58
3.6 安全协议的设计原则 …… 59
3.7 本章小结 …… 60
习题 …… 60

第 4 章 认证与密钥交换协议 …… 61

4.1 无可信第三方的对称密钥协议 …… 62
4.1.1 ISO one-pass 对称密钥单向认证协议 …… 62
4.1.2 ISO two-pass 对称密钥单向认证协议 …… 62
4.1.3 ISO two-pass 对称密钥双向认证协议 …… 62
4.1.4 ISO three-pass 对称密钥双向认证协议 …… 62
4.1.5 Andrew 安全 RPC 协议 …… 63
4.2 具有可信第三方的对称密钥协议 …… 63
4.2.1 NSSK 协议 …… 63
4.2.2 Otway-Rees 协议 …… 64
4.2.3 Yahalom 协议 …… 65
4.2.4 大嘴青蛙协议 …… 65
4.2.5 Denning-Sacco 协议 …… 66
4.2.6 Woo-Lam 协议 …… 66
4.3 无可信第三方的公开密钥协议 …… 67
4.3.1 ISO one-pass 公开密钥单向认证协议 …… 67
4.3.2 ISO two-pass 公开密钥单向认证协议 …… 67
4.3.3 ISO two-pass 公开密钥双向认证协议 …… 68
4.3.4 ISO three-pass 公开密钥双向认证协议 …… 68
4.3.5 ISO two-pass 公开密钥并行双向认证协议 …… 68
4.3.6 Diffie-Hellman 协议 …… 68
4.4 具有可信第三方的公开密钥协议 …… 69
4.4.1 NSPK 协议 …… 69
4.4.2 SPLICE/AS 协议 …… 70
4.4.3 Denning Sacco 密钥分配协议 …… 71
4.5 针对认证与密钥交换协议的攻击 …… 71
4.5.1 针对无可信第三方的对称密钥协议的攻击 …… 71
4.5.2 针对具有可信第三方的对称密钥协议的攻击 …… 72
4.5.3 针对无可信第三方的公开密钥协议的攻击 …… 76

4.5.4 针对具有可信第三方的公开密钥协议的攻击 …… 77
4.6 本章小结 …… 79
习题 …… 79

第5章 电子商务协议 …… 80

5.1 电子商务协议概述 …… 80
5.1.1 电子商务协议研究背景 …… 80
5.1.2 电子商务协议的安全属性 …… 81
5.2 非否认协议 …… 82
5.2.1 非否认协议的基本概念 …… 82
5.2.2 Markowitch 和 Roggeman 协议 …… 83
5.2.3 Zhou-Gollmann 协议 …… 84
5.2.4 Online TTP 非否认协议——CMP1 协议 …… 86
5.3 电子现金协议 …… 87
5.3.1 电子现金协议中的密码技术 …… 87
5.3.2 Digicash 电子现金协议 …… 91
5.3.3 Brands 电子现金协议 …… 92
5.4 电子支付协议 …… 94
5.4.1 First Virtual 协议 …… 94
5.4.2 NetBill 协议 …… 95
5.4.3 ISI 协议 …… 96
5.4.4 iKP 协议 …… 97
5.4.5 IBS 协议 …… 100
5.4.6 SSL 协议 …… 101
5.4.7 SET 协议 …… 101
5.5 安全电子邮件协议 …… 102
5.6 本章小结 …… 103
习题 …… 104

第6章 实际使用中的安全协议 …… 105

6.1 Kerberos 协议 …… 105
6.1.1 概述 …… 105
6.1.2 术语 …… 106
6.1.3 运行环境 …… 106
6.1.4 消息交互 …… 107

6.1.5 跨域认证 …… 110
6.1.6 安全性分析 …… 111
6.2 SSL 协议 …… 112
6.2.1 概述 …… 112
6.2.2 特点 …… 113
6.2.3 结构 …… 114
6.2.4 原理 …… 115
6.2.5 安全性分析 …… 118
6.3 IPSec 协议 …… 119
6.3.1 概述 …… 119
6.3.2 结构 …… 120
6.3.3 认证头协议 …… 121
6.3.4 封装安全载荷协议 …… 122
6.3.5 AH 协议及 ESP 协议的工作模式 …… 124
6.3.6 Internet 密钥交换协议 …… 125
6.3.7 安全性分析 …… 128
6.4 Set 协议 …… 130
6.4.1 概述 …… 130
6.4.2 SET 支付模型 …… 131
6.4.3 交易流程 …… 132
6.4.4 证书管理 …… 137
6.4.5 安全性分析 …… 140
6.5 本章小结 …… 142
习题 …… 143

第三部分 安全协议的分析、验证方法

第 7 章 BAN 逻辑 …… 147

7.1 BAN 逻辑的基本框架 …… 147
7.1.1 BAN 逻辑的语法、语义 …… 148
7.1.2 BAN 逻辑的推理规则 …… 149
7.2 应用 BAN 逻辑分析协议的方法 …… 151
7.2.1 理想化过程 …… 151

7.2.2 认证协议的基本假设 …… 151
7.2.3 协议解释 …… 152
7.2.4 形式化协议目标 …… 152
7.2.5 BAN 逻辑协议分析步骤 …… 153
7.3 BAN 逻辑的应用实例 …… 153
7.3.1 应用 BAN 逻辑分析 Otway-Rees 协议 …… 153
7.3.2 应用 BAN 逻辑分析 NS 对称密钥协议 …… 157
7.3.3 应用 BAN 逻辑分析 NS 公开密钥协议 …… 160
7.4 BAN 逻辑的缺陷 …… 164
7.4.1 BAN 逻辑的缺陷 …… 164
7.4.2 BAN 逻辑的改进方向 …… 167
7.5 本章小结 …… 167
习题 …… 167

第 8 章 BAN 类逻辑 …… 168

8.1 GNY 逻辑 …… 168
8.1.1 GNY 逻辑的计算模型 …… 169
8.1.2 GNY 逻辑的语法、语义 …… 169
8.1.3 GNY 逻辑的推理规则 …… 170
8.1.4 GNY 逻辑应用实例 …… 174
8.2 AT 逻辑 …… 177
8.2.1 AT 逻辑的语法 …… 179
8.2.2 AT 逻辑的推理规则 …… 180
8.2.3 AT 逻辑的计算模型 …… 181
8.2.4 AT 逻辑的语义 …… 182
8.3 SVO 逻辑 …… 185
8.3.1 SVO 逻辑的语法 …… 185
8.3.2 SVO 逻辑的推理规则 …… 186
8.3.3 计算模型 …… 187
8.3.4 SVO 逻辑的语义 …… 188
8.3.5 SVO 逻辑的应用实例 …… 190
8.4 本章小结 …… 196
习题 …… 197

第 9 章 Kailar 逻辑 …… 198

9.1 电子商务协议的安全性分析 …… 198
9.1.1 匿名性 …… 199
9.1.2 原子性 …… 199
9.1.3 不可否认性 …… 199
9.1.4 可追究性 …… 200
9.1.5 公平性 …… 200
9.2 Kailar 逻辑的基本构件 …… 201
9.3 Kailar 逻辑的推理规则 …… 202
9.3.1 一般推理规则 …… 202
9.3.2 可追究性推理规则 …… 203
9.4 Kailar 逻辑的应用举例 …… 203
9.4.1 IBS 协议 …… 203
9.4.2 CMP1 协议 …… 206
9.4.3 ISI 协议 …… 208
9.5 Kailar 逻辑的缺陷 …… 210
9.6 本章小结 …… 212
习题 …… 212

第 10 章 时间相关安全协议分析 …… 213

10.1 Timed-Release 密码协议 …… 213
10.2 CS 逻辑的逻辑构件 …… 215
10.3 CS 逻辑的推理规则 …… 216
10.4 CS 逻辑的公理 …… 216
10.5 CS 逻辑的应用分析 …… 217
10.6 CS 逻辑的改进 …… 220
10.6.1 修改密文公理 …… 221
10.6.2 修改消息接收公理 …… 222
10.6.3 时间密钥 …… 222
10.7 改进的 CS 逻辑的应用分析 …… 223
10.7.1 时间标注 …… 224
10.7.2 协议目标 …… 224
10.7.3 初始假设 …… 225
10.7.4 协议分析 …… 225

10.8 本章小结…… 228
习题…… 228

第 11 章 串空间模型理论及协议分析方法 …… 229

11.1 串空间模型理论基础…… 230
11.1.1 基本概念…… 230
11.1.2 丛和结点的因果依赖关系…… 232
11.1.3 攻击者描述…… 233
11.1.4 协议正确性概念…… 237
11.2 基于极小元理论的串空间方法…… 237
11.2.1 NSL 串空间 …… 237
11.2.2 NSL 响应者的一致性 …… 238
11.2.3 响应者的秘密性…… 241
11.2.4 NSL 发起者的秘密性 …… 242
11.2.5 NSL 发起者的一致性 …… 242
11.3 理想与诚实理论…… 243
11.3.1 理想…… 243
11.3.2 诚实…… 244
11.4 基于理想与诚实理论的串空间方法…… 246
11.4.1 Otway-Rees 协议的串空间模型 …… 246
11.4.2 机密性…… 247
11.4.3 认证性…… 248
11.5 认证测试理论…… 250
11.5.1 基本概念…… 251
11.5.2 攻击者密钥和安全密钥…… 251
11.5.3 认证测试…… 252
11.6 基于认证测试理论的串空间方法…… 254
11.6.1 Otway-Rees 协议的串空间模型 …… 254
11.6.2 Otway-Rees 协议认证 …… 254
11.7 串空间理论分析方法的比较…… 256
11.8 本章小结…… 256
习题…… 257

第 12 章 安全协议的 CSP 分析方法 …… 258

12.1 CSP 基本概念 …… 258

12.1.1 事件…… 258
12.1.2 进程…… 259
12.1.3 迹…… 261
12.1.4 并发…… 264
12.1.5 选择…… 265
12.1.6 穿插…… 266
12.1.7 CSP 建模举例 …… 266
12.2 安全属性 …… 268
12.2.1 秘密性…… 269
12.2.2 认证性…… 269
12.3 CSP 网络模型 …… 270
12.3.1 网络模型…… 270
12.3.2 消息空间…… 271
12.3.3 攻击者描述…… 272
12.3.4 协议参与者…… 274
12.4 CSP 方法的应用分析 …… 274
12.4.1 消息空间…… 274
12.4.2 协议建模…… 274
12.4.3 协议分析…… 275
12.5 本章小结…… 278
习题…… 278

第 13 章 其他安全协议分析验证方法 …… 279

13.1 Dolev-Yao 模型 …… 279
13.1.1 协议模型…… 280
13.1.2 协议安全的定义…… 280
13.1.3 举例…… 281
13.2 Paulson 归纳法 …… 282
13.2.1 归纳定义操作…… 282
13.2.2 事件和攻击者…… 283
13.2.3 协议建模…… 283
13.2.4 标准规则…… 284
13.2.5 归纳法…… 285
13.2.6 证明秘密性定理…… 285
13.3 Schneider 秩函数 …… 286

13.3.1 基本概念…… 286
13.3.2 实例分析…… 288
13.4 基于 Petri 网的安全协议分析方法 …… 291
13.4.1 基本概念…… 291
13.4.2 协议建模…… 293
13.4.3 带攻击者的协议建模…… 294
13.4.4 攻击者模型…… 295
13.4.5 安全属性分析…… 298
13.5 本章小结…… 300
习题…… 300

参考文献…… 301

第一部分　基础知识

第1章 引 言

人类正在经历着自工业革命以来最为深刻的信息革命，在这场信息革命中，软件系统作为现代条件下信息处理及信息传输的重要手段起着举足轻重的作用。然而，软件系统也有其两面性：一方面，它有力地推动了我国的信息化进程，促进了我国国民经济的增长，推动着我国社会发展和文明进步，增强了我国经济、科技、军事实力；另一方面，软件系统的广泛应用也给国家安全、社会稳定和经济发展带来了许多新的安全威胁。因此，我们在发展软件系统的同时，必须对其安全性加以关注。

为了减轻由于系统遭受攻击所带来的危害，多种安全协议被设计开发出来提供安全保障。安全协议是以密码学为基础的协议，它在网络和分布式系统中提供各种各样的安全服务，在信息系统安全中占据重要地位。与其他各种类型的协议一样，“安全协议”由参与协议的主体，以及主体之间交换信息的事件组成。安全协议是构建安全网络环境的基石，它的正确性对于网络安全极其关键。然而由于安全协议的执行具有高度不确定性，以致有些安全协议往往不如它们的设计者所期望的那样安全，存在很多缺陷和漏洞，这些缺陷和漏洞可能来源于三个方面：①协议中采用的密码算法；②算法和协议中采用的密码技术；③协议自身的结构。因此，在互联网飞速发展的今天，软件安全机制，特别是安全协议的分析、研究就显得特别的重要。

1.1 安全协议的研究背景、基本概念

1.1.1 安全协议的研究背景

ISO对信息安全的定义为：“为数据处理系统建立和采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭受破坏、更改、泄露。”该定义把信息安全的具体的内容分成以下部分：①运行系统的安全。涉及了计算机的硬件设备的安全、操作系统的安全以及数据库的安全等。②系统信息的安全。涉及了信息的传