

国瑞数码安全系列丛书

(第二版)

杨义先 李志江 钮心忻 曹华平 译



国瑞数码安全系列丛书

智能卡安全与应用

（第二版）

Mike Hendry 著

杨义先 李志江 钮心忻 曹华平 译

人民邮电出版社

图书在版编目 (CIP) 数据

智能卡安全与应用 / (英) 亨德利 (Hendry, M.) 著; 杨义先等译. —北京: 人民邮电出版社, 2002.2

(国瑞数码安全系列丛书)

ISBN 7-115-09738-0

I. 智... II. ①亨... ②杨... III. 智能卡—应用—电子计算机—安全技术 IV. TP309

中国版本图书馆 CIP 数据核字 (2001) 第 088015 号

国瑞数码安全系列丛书

智能卡安全与应用(第二版)

- ◆ 著 Mike Hendry
译 杨义先 李志江 钮心忻 曹华平
责任编辑 陈万寿
- ◆ 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@pptph.com.cn
网址 <http://www.pptph.com.cn>
读者热线 010-67180876
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销
- ◆ 开本: 787 × 1092 1/16
印张: 14.25
字数: 328 2002 年 2 月第 1 版
印数: 1 - 5 000 册 2002 年 2 月北京第 1 次印刷
著作权合同登记 图字: 01 - 2001 - 4498 号
ISBN 7-115-09738-0/TN·1791

定价: 25.00 元

本书如有印装质量问题, 请与本社联系 电话: (010)67129223

内 容 提 要

本书全面地介绍了智能卡在解决普遍存在的计算机安全问题方面的各种方法，并且还对支持这些技术方案所需要的商务体系结构进行了研究。在多应用操作系统、计算机网络和因特网等方面的讨论覆盖了许多最新的进展。

本书提供了许多技术细节，包括最新的保护机制、最新攻击的特征描述、解决唯一性安全问题的巧妙方法等。本书用浅显易懂的方式介绍了智能卡的众多应用。比如，远程支付系统中的用户认证、因特网转帐、移动电话以及卡支付系统中的欺骗与造假、电子售票、易携带性和保密性等。本书解释了智能卡与基于因特网的各种特殊应用之间是如何彼此关联，以及智能卡如何利用密码学、公钥基础设施和生物学来完成现代支付的。

本书层次分明，内容取舍得当，广度与深度之间的关系处理得体，可以作为国内网络安全、信息安全、计算机安全领域相关人员的技术培训教材，还可以作为通信与电子系统、信号与信息处理、密码学等专业的大学生和研究生相关课程的教学参考书。特别地，本书可作为国内众多安全公司的技术人员提高业务水平的实用工具书。

版 权 声 明

本书为阿尔泰克出版社（ARTECH HOUSE,INC.）独家授权的中文译本。本书的专有出版权属人民邮电出版社。未经原版出版者和本书出版者的书面许可，任何单位和个人不得擅自复印、复制、摘录本书的部分或全部内容，也不得以任何形式（包括资料和出版物）进行传播。

版权所有，侵权必究。

© 2001 ARTECH HOUSE,INC.

本书原版版权属 ARTECH HOUSE,INC.

本书原版书名 Smart Card Security and Applications, Second Edition

作者 Mike Hendry

前 言

自从本书第一版出版发行四年来，可以说是什么都没有变，也可以说什么都变了。在智能卡领域，我们没有看见新的应用领域，也没有本质上的创新。四年前，我们考虑了智能卡在交通、电信、数字电视和银行等领域的应用。我们曾讨论了非接触式和接触智能卡。我们也曾描述了能支持多种应用的开放式体系的智能卡结构。我们描述过可以将信息写入一张芯片，且该芯片能在不同类型的硬件上运行的应用。

如果没有本质上的创新，肯定不会有很大的进步。然而，我们所看到的，就是大众化的迅速普及。我想，可以毫不夸张地说：自从本书第一版出版发行以来的四年里，智能卡——卡上计算机时代已经到来。它已变成了一种主流技术。在西欧，很多市民至少拥有一张或两张智能卡。在本书第一版发行时，人们从没有见过一张智能卡。可以说，这的确是一个巨大的进步。

我们已经看到，除了来自电信产业的 GSM 标准成为全球性标准外，还有来自金融产业的 EMV 和 CEPS 也成为了全球性标准。在欧洲，银行信用卡协会已经制定出时间进度表，要在 2005 年初，把现在所有的 Visa 卡，Europay/Mastercard 转换为基于芯片的智能卡。随着每年能够处理上千万次交易的 Octopus 系统在香港的成功应用，我们已经看到非接触式卡将成为一种消费品技术。我们已经看到多功能开放式平台产品的价格急剧降至 3 欧元以下，并且这些产品是作为标准产品而销售的……，也许，最为激动人心的事情是，智能卡已不再是欧洲专用了：GSM 已遍布世界各地，在 2000 年，我们开始看到，北美开始大规模地采用智能卡。

下一个四年，我们将会看到智能卡技术应用的进一步普及。

Jon Prideaux

国际 Visa 欧洲分部 Virtual Visa 常务副主席

作者简介

Mike Hendry 是支付系统与电子商务方面的独立顾问，擅长于智能卡和交易的安全。他也是《实用计算机网络安全》和《EDI 实现》这两本书的作者。他从日内瓦国际管理学院获得了工商管理硕士学位（MBA），从英国剑桥大学获得了工程硕士。他精通多种语言，曾为欧洲的零售商、银行和服务提供商做过关于技术和商业策略方面的工作。

Hendry 先生曾参与英国和欧洲的基于芯片的信用卡、借记卡和钱包卡的实现工作。他曾为智能卡发行商和主要的零售商做过关于在商业、操作和技术上的规范，这些智能卡发行商和零售商还很幸运地得到了 **Hendry** 先生技术上长时间的支持。**Hendry** 先生当前的工作领域包括电子商务、移动电话的尖端产品和系统设计，同样包括为信用卡、借记卡进行异地交易的产品和系统的设计。

目 录

第一部分 背 景

第 1 章 引言	2
1.1 卡的发展史	2
1.2 什么是芯片卡	3
1.3 系统和程序	3
1.4 市场问题	4
1.5 本书结构	5
参考文献	6
第 2 章 问题描述	7
2.1 感觉	7
2.2 真实情况	7
2.3 计算风险：可能性与几率	8
2.4 技术交流的障碍	9
参考文献	9
第 3 章 确定需求	10
3.1 安全标准	10
3.1.1 安全服务	10
3.1.2 安全	10
3.1.3 没有送达	11
3.1.4 精确性	11
3.1.5 数据完整性	11
3.1.6 机密性	12
3.1.7 冒充	12
3.1.8 抵赖	12
3.2 量化威胁	13
3.2.1 可能的后果与威胁	13
3.2.2 受威胁的对象	13
3.2.3 错误原因和错误模式	14
3.2.4 事故频率	14
3.2.5 风险管理	15

3.3 标准	16
3.3.1 按规定使用标准	16
3.3.2 安全等级	16
3.3.3 质量保证	17
3.4 规范成文	18
3.4.1 初始系统规范	18
3.4.2 分析和准则	18
3.4.3 安全实体的组成	18
参考文献	18

第二部分 技 术

第4章 卡技术	20
4.1 表面特征	20
4.2 磁 条	21
4.2.1 拷贝和伪造	21
4.2.2 高磁性卡	22
4.2.3 其他类型的磁卡	23
4.3 使用辅助技术提高安全性	23
4.4 光卡	23
4.5 智能卡	24
4.5.1 起源与发展	24
4.5.2 技术构成	25
4.5.3 标准	26
4.6 混合型卡	26
4.7 PCMCIA 卡	27
4.8 其他	27
4.8.1 条形编码	27
4.8.2 无线频率辨认(RFID)	27
第5章 加密	29
5.1 密码学概论和术语	29
5.2 算法	30
5.2.1 对称密钥系统	30
5.2.2 非对称密钥系统	31
5.2.3 认证	32
5.3 密钥	33
5.3.1 秘密密钥	34
5.3.2 公钥和私钥	34

5.3.3	主密钥和导出密钥	34
5.3.4	用户和设备密钥	35
5.3.5	密钥加密密钥	35
5.3.6	会话密钥	36
5.3.7	算法和密钥长度的选择	37
5.4	密钥管理	38
5.4.1	密钥的产生	38
5.4.2	密钥发送	38
5.4.3	密钥索引	39
5.4.4	认证机构	39
5.5	公共密钥基础设施	40
5.6	计算要求	41
5.7	密码出口控制	41
5.8	小结	42
	参考文献	42
第 6 章	口令和生物测定	44
6.1	个人身份识别类型	44
6.1.1	口令、令牌、生物测定	44
6.1.2	行为特性和生理机能测定	45
6.2	需求	45
6.2.1	识别与核实	45
6.2.2	行为	45
6.2.3	过程	46
6.3	组成部分	46
6.4	口令和 PIN	47
6.5	行为特性测定	47
6.5.1	签名验证	47
6.5.2	击键动态特性	48
6.5.3	语音识别	48
6.6	生理机能测定	49
6.6.1	指纹/拇印	49
6.6.2	掌型测定	50
6.6.3	视网膜扫描	50
6.6.4	虹膜扫描	50
6.6.5	其他	51
6.7	生物测定和卡	51

第 7 章 芯片卡的类型和特征	52
7.1 存储卡	52
7.1.1 无保护型	52
7.1.2 保护型	52
7.1.3 安全逻辑	53
7.2 微处理器卡	53
7.2.1 发展	53
7.2.2 历史	53
7.2.3 状态变换	54
7.2.4 加密	55
7.3 接触型与非接触型	55
7.3.1 接触型卡	55
7.3.2 非接触型卡	55
7.3.3 复合型智能卡	56
7.4 构成因素	57
7.4.1 模块	57
7.4.2 小型卡	58
7.4.3 钥匙型卡	58
7.4.4 USB 设备	59
7.4.5 其他	59
第 8 章 芯片卡安全特性	60
8.1 载体	60
8.2 外部安全特性	60
8.3 芯片	61
8.3.1 微处理器	61
8.3.2 存储器	62
8.3.3 协处理器	63
8.3.4 存储器管理	63
8.3.5 输入/输出	64
8.3.6 芯片的安全特性	64
8.4 接触型	65
8.5 天线	66
8.6 掩模	66
8.7 攻击和反攻击措施	67
8.7.1 内部攻击	68
8.7.2 外部攻击	68
8.8 可靠性因素	69

8.9 样品卡规格说明	70
参考文献	71
第 9 章 多用途操作系统	72
9.1 目标	72
9.2 功能	73
9.3 产品	74
9.3.1 JavaCard	74
9.3.2 Multos	74
9.3.3 Windows for Smart Cards	75
9.3.4 开放式平台	76
9.3.5 安全性	76
参考文献	76
第 10 章 系统组成	77
10.1 读卡机	77
10.1.1 触点	77
10.1.2 卡传送	78
10.1.3 控制电子设备	79
10.1.4 非接触型卡读卡机	80
10.2 终端	81
10.2.1 PINpads	81
10.2.2 PC 读卡机	82
10.2.3 EPOS 或 EFT-POS 终端	84
10.2.4 ATM	85
10.2.5 自动售货机	85
10.2.6 访问控制	85
10.2.7 其他	86
10.2.8 终端保护	86
10.3 网络	86
10.3.1 卡的作用	86
10.3.2 网络安全检测	86
10.3.3 网络安全的规定	87
10.3.4 备份和恢复	87
10.4 主机系统	87
参考文献	88
第 11 章 进程和过程	89
11.1 芯片设计	89

11.2	制造	89
11.3	个性化	92
11.3.1	数据发送	92
11.3.2	固定数据和导出数据	92
11.3.3	测试	92
11.3.4	数据保护	93
11.3.5	静电排除和干扰	93
11.4	发行	93
11.5	装载/证实	93
11.6	使用	94
11.6.1	日志	94
11.6.2	卡和持卡人认证	94
11.6.3	恢复错误	94
11.7	卡丢失、被盗和误用	95
11.7.1	问题	95
11.7.2	检测	95
11.7.3	锁定与解锁	95
11.7.4	重新发行	96
11.8	应用装载与卸载	96
11.9	生命结束	97
11.9.1	期满	97
11.9.2	处理或复原	97
11.9.3	重复利用	97

第三部分 应 用

第 12 章	电话与广播应用	100
12.1	固定电话	100
12.1.1	公用电话需求	100
12.1.2	电话卡标准	100
12.1.3	发行	101
12.1.4	电话卡的发展	102
12.2	移动电话	103
12.2.1	用户身份识别模块 (SIM)	103
12.2.2	SIM 工具箱	103
12.2.3	无线应用协议	104
12.2.4	全球移动电话服务	105
12.2.5	预付	105
12.2.6	双插槽电话	106

12.3 电缆和卫星电视	107
12.3.1 需求	107
12.3.2 缺点和解决方法	107
12.3.3 向数字化转变	108
参考文献	109
第 13 章 计算机网络和电子商务	110
13.1 网络安全	110
13.1.1 计算机系统访问	110
13.1.2 数据和程序的保密性	111
13.2 因特网浏览和电子邮件	111
13.2.1 互联网协议	111
13.2.2 安全套接层	112
13.2.3 公钥基础设施	112
13.2.4 入侵	112
13.2.5 电子邮件	113
13.3 电子商务	113
13.3.1 企业对企业的电子商务	113
13.3.2 企业对客户的电子商务	114
13.3.3 支付的形式	115
13.3.4 数字签名	116
参考文献	116
第 14 章 金融应用	117
14.1 银行卡	117
14.1.1 功能	117
14.1.2 攻击	119
14.2 信用卡/付款卡	119
14.2.1 需求	119
14.2.2 标准	121
14.2.3 过程	123
14.3 电子钱包	124
14.3.1 需求	124
14.3.2 类型	125
14.3.3 安全机制	126
14.3.4 CEPS	127
14.3.5 状况	127
14.4 在线交易	128
14.4.1 在线银行业务	128

14.4.2 交易授权	129
14.4.3 安全电子交易	130
14.5 福利支付	131
14.6 忠实	132
14.7 新传输渠道	132
参考文献	133
第 15 章 健康	134
15.1 保险	134
15.2 医疗记录	135
15.2.1 可选方法	135
15.2.2 问题	135
15.2.3 操作和指导方案	136
15.3 处方	137
15.4 病人监测	137
参考文献	138
第 16 章 交通运输	139
16.1 本地公共交通	139
16.1.1 组织	139
16.1.2 卡的类型	140
16.1.3 安全性和互操作性	141
16.2 出租车	142
16.3 火车	142
16.4 航空旅行	142
16.4.1 要求	142
16.4.2 电子检票	142
16.4.3 飞行娱乐	143
16.5 道路征税	143
16.6 停车	144
参考文献	145
第 17 章 个人身份认证	146
17.1 认证卡要求	146
17.2 发行	146
17.2.1 安全级别	146
17.2.2 在线和脱机系统	146
17.2.3 卡发行商职责	147
17.3 访问控制	147

17.3.1 替代技术	147
17.3.2 特征	147
17.3.3 特殊情况	148
17.4 大中医院校	148
17.5 政府卡	148
17.6 “白卡”	149
参考文献	150
第 18 章 多用途卡的商业结构	151
18.1 功能和应用	151
18.2 下载	152
18.3 混合卡的类型	153
18.4 卡和应用控制	154
18.5 发行商的责任	154
18.6 消费者的问题	155
18.7 现存智能卡系统的交换性和兼容性	155
第 19 章 安全设计	156
19.1 目标	156
19.1.1 减少回报	156
19.1.2 增加努力	157
19.2 标准	157
19.3 模型	158
19.3.1 存储	158
19.3.2 发送	159
19.3.3 使用	159
19.4 分析	160
19.4.1 初始状态分析	160
19.4.2 攻击的来源	161
19.4.3 定量分析	161
19.4.4 风险分析核对表	162
19.4.5 重复	162
第 20 章 展望	163
20.1 市场预测	163
20.2 卡	164
20.2.1 芯片	164
20.2.2 密码协处理器	165
20.2.3 掩模	165

20.2.4 接触/非接触型165

20.3 应用下载166

20.4 卡和终端标准166

20.4.1 卡166

20.4.2 终端166

20.5 芯片卡及其主流167

20.6 结论168

附录 A 标准169

附录 B 术语表174

附录 C 参考书目（智能卡安全参考书）180

索引183