国瑞数码安全系列丛书

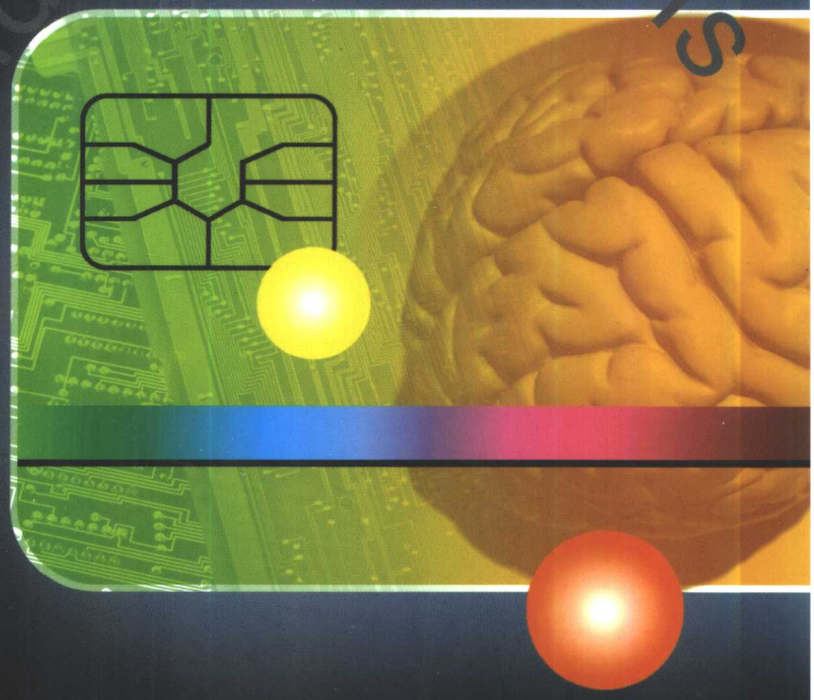
智能卡安全与应用

（第二版）

Mike Hendry 著

杨义先 李志江 钮心忻 曹华平 译

Smart Card Security and Applications



人民邮电出版社
www.pptph.com.cn

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

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

第二部分 技 术

第三部分 应 用