精通

PKI

网络安全认证技术与编程实现

马臣云　王彦　编著

PKI，利用公钥加密技术
解决电子商务信息安全需求的成熟体系

内容充实，技术全面，覆盖了常见的PKI应用开发技术

注重应用，强调实战，填补了PKI类书籍只重理论没有实战的空白

以“步骤＋代码”的方式进行讲解，让初学者快速入门

实例典型、代码丰富，有极大的应用价值

博客专栏支持，解惑答疑，深入交流

人民邮电出版社
POSTS & TELECOM PRESS

CD-ROM

精通

PKI

网络安全认证技术与编程实现

马臣云　王彦　编著

人民邮电出版社

北京

图书在版编目（CIP）数据

精通 PKI 网络安全认证技术与编程实现 / 马臣云，王彦编著. —北京：人民邮电出版社，2008.7
ISBN 978-7-115-17845-9

Ⅰ. P… Ⅱ. ①马…②王… Ⅲ. ①计算机网络—安全技术②电子商务—安全技术 Ⅳ. TP393.08 F713.36

中国版本图书馆 CIP 数据核字（2008）第 035953 号

内 容 提 要

PKI 是解决开放式互联网络信息安全需求的成熟体系。PKI 体系支持身份认证，信息传输、存储的完整性，消息传输、存储的机密性，以及操作的不可否认性。本书从实战出发，介绍了 PKI 应用开发过程和细节。全书共 32 章，分 6 篇，主要内容包括 PKI 基础知识、OpenSSL 开发、CrytoAPI 开发、Java Security 开发、电子商务网站应用、PKI 技术应用等，涉及 C 语言、Java 语言、JSP、ASP/ASP.NET、PHP 等开发语言。为了方便读者深入了解 PKI，本书按照先原理、再讲解、再实战的方式进行，并且全部实例和软件都保存在随书赠送的光盘中。

本书适合 PKI 应用开发人员、企业网络管理人员以及大、中专院校师生阅读。

精通 PKI 网络安全认证技术与编程实现

◆ 编　　著　马臣云　王　彦
责任编辑　屈艳莲

◆ 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@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：29.25
字数：766 千字　　2008 年 7 月第 1 版
印数：1－4 000 册　　2008 年 7 月北京第 1 次印刷

ISBN 978-7-115-17845-9/TP

定价：55.00 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

随着电子商务的发展，网上购物、网上支付等消费方式已经逐渐被大众所接受。但是由于互联网的开放性，网络交易中的身份认证、数据保密、防篡改、防抵赖等安全需求变得越来越迫切。PKI（Public Key Infrastructure，公开密码基础设施）是解决开放式互联网络信息安全需求的成熟体系。

PKI 是以现代密码学为基础的，其理论在国内外已经得到深入的研究。在我国，PKI 方面的应用也正在逐步开展，但是 PKI 开发人才的短缺极大地限制了其发展速度。

目前市场上有一些介绍 PKI 的中外文书籍，但都偏重于理论，或是与艰涩难懂的密码算法一起介绍。而本书直接从实战出发，介绍了 PKI 应用开发过程和细节。

本书介绍了 PKI 应用开发常用的技术，包括 OpenSSL 开发、CrytoAPI 开发、Java Security 开发、电子商务网站应用、PKI 相关技术应用等，涉及 C 语言、Java 语言、Web 开发语言（JSP、ASP/ASP.NET、PHP），每个系列都是按照先原理、再讲解、再实战的方式进行。力求读者学完本书后，可进行项目实践。

本书的特点

1．技术全面，内容充实

本书覆盖了常见的 PKI 应用开发技术，包括 OpenSSL、CrytoAPI、Java Security、电子商务网站（JSP、ASP/ASP.NET、PHP）等。这样无论 Windows 开发还是 Web 开发，无论是 C 开发还是 Java 开发都可以从本书中获得必要的帮助。

2．强调实战，示例代码丰富

本书在讲解知识点时，都附带了实例。每个章节在介绍函数后都会利用实例让读者深入了解该系列函数的功能和用法。同时，章节最后又包括了该部分项目级的综合应用。例如，讲解 OpenSSL 开发时，在 OpenSSL 加密和解密、消息摘要、签名验证等章节中都有相应的实例，最后又以 OpenSSL 的综合应用，即“文件保险箱”、“安全通信软件”、“安全报文系统”为例深入讲解，让读者了解项目级的 OpenSSL 开发情况。

3．配有光盘，实例的源代码实际开发价值巨大

本书中涉及的全部实例都保存在附属光盘中，不少实例都是作者平时的项目积累，故源码的实际开发价值很大，稍微做些产品化即可完成实际项目需要。

4．提供完善的售后服务

为了方便读者学习，作者在博客上创建一个专有版面：http://5233studio.bokee.com/catalog_60759.html。读者可以将自己遇到的问题发布在该版面上，我们将帮助大家解决这些问题。

本书的内容

第 1 篇（第 1 章）主要介绍 PKI 的基础知识。

第 1 章：介绍了什么是数字证书、为什么要使用数字证书、加密技术、数字签名技术。同时还介绍了常见的 PKI 术语。

第 2 篇（第 2 章～第 11 章）主要介绍了 OpenSSL 开发。

第 2 章：OpenSSL 入门介绍，包括 OpenSSL 概述、如何下载和编译 OpenSSL、如何搭建 OpenSSL 开发环境。

第 3 章：介绍了 OpenSSL 加密和解密，首先介绍了加解密的概念，然后详细介绍了相关函数的用法，并给出一个实例应用。

第 4 章：介绍了 OpenSSL 消息摘要，首先介绍了消息摘要的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第 5 章：介绍了 OpenSSL 签名和验证，首先介绍了签名和验证的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第 6 章：介绍了 OpenSSL Base64 编解和解码，首先介绍了 Base64 编解码的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第 7 章：介绍了 OpenSSL 证书操作，首先介绍了证书的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第 8 章：介绍了 OpenSSL SSL/TLS 编程，首先介绍了 SSL/TLS 的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第 9 章：介绍了一个 OpenSSL 开发实例——文件保险箱，首先介绍了实例的功能，然后分析了实现流程，最后给出了功能实现的详细步骤。

第 10 章：介绍了一个 OpenSSL 开发实例——安全通信软件（SSL/TLS 通信），首先介绍了实例的功能，详细分析了实现流程，最后给出了功能实现的详细步骤。

第 11 章：介绍了一个 OpenSSL 开发实例——安全报文系统，首先介绍了实例的功能，然后分析了实现流程，最后给出了功能实现的详细步骤。

第 3 篇（第 12 章～第 19 章）主要介绍了 CryptoAPI 开发。

第 12 章：CryptoAPI 入门介绍，包括 CryptoAPI 组成、CryptoAPI 的优缺点和如何搭建开发环境。

第 13 章：介绍了 CryptoAPI 的密码服务提供者 CSP 函数，首先介绍了密码服务提供者的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第 14 章：介绍了 CryptoAPI 的密钥的产生和交换函数，首先介绍了密钥的产生和交换函数

的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第 15 章：介绍了 CryptoAPI 的数据的加密和解密函数，首先介绍了数据的加密和解密函数的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第 16 章：介绍了 CryptoAPI 的数据的哈希和数字签名函数，首先介绍了哈希和数字签名函数的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第 17 章：介绍了 CryptoAPI 的证书和证书库函数，首先介绍了证书和证书库函数的概念，然后介绍了相关函数的用法，并给出一个实例应用。

第 18 章：介绍了一个 CryptoAPI 开发实例——文件保险箱，首先介绍了实例的功能，然后分析了实现流程，最后给出了功能实现的详细步骤。

第 19 章：介绍了一个 CryptoAPI 开发实例——安全报文系统，首先介绍了实例的功能，然后分析了实现流程，最后给出了功能实现的详细步骤。

第 4 篇（第 20 章～第 26 章主要介绍了 Java Security 开发。

第 20 章：Java Security 开发入门介绍，包括 Java Security 设计原理和体系结构、主要概念、主要类和接口以及如何搭建开发环境。

第 21 章：介绍了 Java 消息摘要，首先介绍了 MessageDigest 类，然后详细介绍了类内函数的用法，并给出一个实例应用。

第 22 章：介绍了 Java 加密和解密，首先介绍了 KeyGenerator 和 Cipher 类，然后详细介绍了类内函数的用法，并给出一个实例应用。

第 23 章：介绍了 Java 数字签名和验证，首先介绍了 KeyPairGenerator 和 Signature 类，然后详细介绍了类内函数的用法，并给出一个实例应用。

第 24 章：介绍了 keytool 和证书类，首先介绍了 keytool 工具的使用方法以及参数的意义，然后介绍了 X509Certificate 类、X509CRL 类的函数，最后给出一个实例应用。

第 25 章：介绍了一个 Java 开发实例——文件保险箱，首先介绍了实例的功能，然后分析了实现流程，最后给出了功能实现的详细步骤。

第 26 章：介绍了一个 Java 开发实例——安全报文系统，首先介绍了实例的功能，然后分析了实现流程，最后给出了功能实现的详细步骤。

第 5 篇（第 27 章～第 29 章）主要介绍了 PKI 电子商务网站的应用。

第 27 章：介绍 ASP/ASP.NET 电子商务网站应用，包括 IIS 配置 SSL 服务器证书的方法、基于数字证书的用户身份认证、基于 CAPICOM 的数字签名应用、基于自开发控件的数字签名应用以及一个安全登录的实例。

第 28 章：介绍 JSP 电子商务网站应用，包括配置 JSP Web 服务器的 SSL 证书的方法、基于数字证书的用户身份认证、数字签名处理以及安全登录和订单签名两个实例。

第 29 章：介绍 PHP 电子商务网站应用，包括配置 Apache 的 SSL 证书的方法、基于数字证书的用户身份认证、数字签名处理以及安全登录和订单签名两个实例。

第 6 篇（第 30 章～第 32 章）主要介绍了 PKI 技术其他方面的应用。

第 30 章：介绍如何颁发和获取数字证书，包括利用 OpenSSL 颁发数字证书、利用 Windows 证书服务颁发数字证书、通过 CA 机构获取数字证书。

第 31 章：介绍安全电子邮件应用，分别介绍了 FoxMail 和 OutLook 的安全电子邮件的配置方法以及发送和阅读安全电子邮件的方法。

第 32 章：介绍代码签名应用，首先介绍了代码签名的概念，然后分别介绍了 Windows 应用

程序代码签名、Java 代码签名、移动代码签名的操作方法。

适合的读者

- PKI 应用开发人员；
- C 程序员；
- JAVA 程序员；
- JSP Web 开发程序员；
- ASP Web 开发程序员；
- ASP.Net Web 开发程序员；
- PHP Web 开发程序员；
- 普通软件开发人员；
- 企业网络管理维护人员；
- 大、中专院校的师生；
- 社会培训学生。

关于作者

本书由马臣云组织编写，同时参与编写、资料整理和代码编写的有何世晓、何颖、卢顺科、吴恒奎、宋智广、宋燕、宋翔、寇苏朋、尚兴隆、张立全、戎剑、李东博、李丹、李春萌、杨涵、杨选举、梁其学、梁艺娟、苏鹏、陈劢、鞠明君、黄志等，在此一并表示感谢。由于本书编写仓促，疏漏之处在所难免，望读者批评指正。

编　者

2008 年 5 月

目　录

第 1 篇　PKI 技术概述

第 2 篇　OpenSSL 开发

第 3 篇 CrytoAPI 开发

第 4 篇 Java Security 开发

第 5 篇 PKI 电子商务网站应用

第 6 篇 其他 PKI 技术应用