

<<OpenSSL与网络信息安全>>

图书基本信息

书名：<<OpenSSL与网络信息安全>>

13位ISBN编号：9787811230062

10位ISBN编号：7811230062

出版时间：2007-4

出版时间：清华大学

作者：王志海

页数：245

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<OpenSSL与网络信息安全>>

内容概要

本书结合OpenSSL的结构和应用指令，对密码算法、公钥基础设施、数字证书和密码应用协议等内容进行较全面的具体阐述。本书试图通过对OpenSSL的具体介绍，一方面让读者能够熟悉和掌握OpenSSL这个强大的工具库，另一方面更希望读者能够在实践中深入理解密码学理论、思想及其相关应用的质。

本书共分12章。第1章对密码学理论、密码学相关应用和本书的情况作了一个概要的说明；第2-3章主要介绍密码学的基本概念、密码技术的基本实现、对称加密算法、公开密钥算法和单向散列函数算法等密码学知识；第4-6章介绍OpenSSL的结构、编译和安装方法及其使用的基本概念；第7-12章是本书的重点，详细介绍了OpenSSL的应用程序（指令）的使用方法和各项参数的意义。

本书可以作为密码技术设计研发人员的参考书籍，在校的本科学生、研究生入门级的密码学和信息安全技术方向的参考书籍，还可以作为信息安全培训和密码技术培训教材。

<<OpenSSL与网络信息安全>>

书籍目录

第1章 概述	1.1 信息安全	1.1.1 信息安全概念	1.1.2 信息安全内容	1.2 密码学	1.2.1 密码学功能	1.2.2 密码学内容	1.2.3 密码学应用	1.3 公钥基础设施	1.3.1 公钥基础设施的必要性	1.3.2 数字证书	1.3.3 公钥基础设施的组件	1.4 安全协议	1.4.1 网络模型和安全协议类型	1.4.2 SSL协议	1.5 OpenSSL	1.5.1 OpenSSL简史	1.5.2 OpenSSL的组成	1.5.3 OpenSSL的优缺点	1.6 本书概要	1.7 推荐资料																
第2章 密码学基本概念	2.1 密码学功能	2.1.1 信息加密	2.1.2 鉴别	2.1.3 完整性	2.1.4 抗抵赖	2.2 密码数学	2.2.1 素数	2.2.2 模运算	2.2.3 数学定理	2.2.4 异或运算	2.2.5 随机数	2.2.6 大数	2.3 密码算法	2.3.1 算法基础	2.3.2 对称加密算法	2.3.3 非对称加密算法	2.3.4 算法安全性	2.4 密码通信协议组件	2.4.1 基于密码学的安全通信	2.4.2 单向散列函数	2.4.3 数字签名	2.5 密钥交换协议	2.5.1 基于对称加密算法的密钥交换协议	2.5.2 基于公开密钥算法的密钥交换协议	2.5.3 高级密钥交换协议	2.5.4 不需要密钥交换协议的安全通信	2.6 鉴别协议	2.6.1 基于口令的鉴别协议	2.6.2 基于公开密钥算法的鉴别协议	2.6.3 基于对称加密算法的鉴别协议	2.6.4 信息鉴别	2.7 实际应用的混合协议	2.7.1 Yahalom协议	2.7.2 Kerberos协议	2.7.3 Neuman-Stubblebine协议	2.7.4 分布式鉴别安全协议
2.8 本章小结	第3章 密码实现技术	3.1 密钥管理技术	3.1.1 密钥生成	3.1.2 密钥分发	3.1.3 密钥验证	3.1.4 密钥使用	3.1.5 密钥存储	3.1.6 密钥销毁	3.1.7 公钥管理	3.2 分组加密模式	3.2.1 电子密码本模式	3.2.2 加密分组链接模式	3.2.3 加密反馈模式	3.2.4 输出反馈模式	3.2.5 三重分组加密模式	3.2.6 其他分组加密模式	3.2.7 数据填充方法	3.3 序列加密模式	3.3.1 自同步序列加密模式	3.3.2 同步序列加密模式	3.4 加密模式选择	3.5 加密算法应用	3.5.1 传输数据加密	3.5.2 存储数据加密	3.5.3 公开密钥算法和对称密钥算法	3.5.4 硬件加密和软件加密	3.6 本章小结	第4章 OpenSSL概述	第5章 OpenSSL编译和安装	第6章 OpenSSL基本概念	第7章 对称加密算法指令	第8章 非对称加密算法指令	第9章 信息摘要和数字签名指令	第10章 证书和CA指令	第11章 OpenSSL的标准转换指令	第12章 OpenSSL的SSL相关指令

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>