

<<网络安全编程与实践>>

图书基本信息

书名：<<网络安全编程与实践>>

13位ISBN编号：9787118057553

10位ISBN编号：711805755X

出版时间：2008-8

出版时间：国防工业出版社

作者：陈卓，阮鸥，沈剑 编著

页数：308

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>

<<网络安全编程与实践>>

内容概要

本书首先介绍了网络安全基础概念，然后重点介绍网络安全编程中常用的两种重要的开发包CryptoAPI、OpenSSL的编程方法和技巧。

本书在基本概念、基本方法讲解后紧跟实例，力求操作步骤清晰易懂，一步一步引导读者掌握网络安全编程方法。

本书理论与实践相结合，实践性强是本书的主要特点，文字通俗易懂，可作为信息安全专业或其他相关专业的教学或参考用书，也可作为从事网络安全研究、软件开发以及网络安全编程爱好者的参考书。

<<网络安全编程与实践>>

书籍目录

第一篇 第1章 概述	1.1 引言	1.1.1 计算机网络面临的主要威胁	1.1.2 计算机网络安全的基本需求	1.1.3 主要的网络安全技术	1.2 网络安全编程简介	1.2.1 借助开发工具实现网络安全编程	1.2.2 几种常见网络安全开发包	1.2.3 如何使用网络安全开发包	本章小结	复习思考题	第2章 网络安全基础	2.1 密码学基本概念	2.1.1 密码学的历史与发展	2.1.2 密码体制的构成	2.1.3 密码体制的分类	2.2 对称密码体制	2.2.1 DES	2.2.2 其他几种对称分组算法	2.2.3 分组算法的工作模式	2.2.4 序列算法	2.2.5 对称密码的局限性	2.3 公钥密码体制	2.3.1 公钥密码体制基本概念	2.3.2 RSA算法	2.3.3 Diffie—Hellman交换	2.3.4 对称密码体制与公钥密码体制的比较	2.4 密钥管理	2.4.1 密钥的种类与层次式结构	2.4.2 密钥的生成与分发	2.5 消息的鉴别与数字签名	2.5.1 哈希函数	2.5.2 消息鉴别的原理	2.5.3 数字签名	2.6 证书与PKI	2.6.1 数字证书	2.6.2 CA认证中心	2.6.3 公共密钥基础设施PKI	2.7 网络安全协议	2.7.1 网络安全协议概述	2.7.2 SSL简介	本章小结	复习思考题	第二篇 第3章 CryptoAPI概述	3.1 CryptoAPI简介	3.1.1 微软加密服务体系	3.1.2 CryptoAPI体系架构	3.1.3 CryptoAPI基本功能	3.2 CryptoAPI编程	3.2.1 Crypto API编译环境设置	3.2.2 例子程序	本章小结	复习思考题	第4章 CryptoAPI安全服务的编程实现	4.1 CryptoAPI编程基础	4.1.1 CryptoAPI密钥管理	4.1.2 CryptoAPI编码与解码	4.2 CryptoAPI数据加解密	4.2.1 加解密操作流程	4.2.2 文件加密	4.2.3 文件解密	4.2.4 数字信封打包及拆解	4.3 CryptoAPI数字签名	4.3.1 CryptoAPI数字签名流程	4.3.2 哈希与数字签名	4.3.3 利用数字证书进行签名与验证	4.3.4 数字签名与消息加密	4.4 CryptoAPI证书与证书库	4.4.1 CryptoAPI证书与证书库概述	4.4.2 应用工具makecert介绍	4.4.3 CryptoAPI证书库管理	4.4.4 CryptoAPI书管理	本章小结	复习思考题	第三篇 第5章 OpenSSL概述与基本指令	5.1 OpenSSL概述	5.1.1 OpenSSL基本结构和功能	5.1.2 OpenSSL的编译安装	5.1.3 在VC++6.0下使用OpenSSL库的环境设置	5.2 OpenSSL基本指令介绍	5.2.1 对称加密算法指令enc	5.2.2 非对称加密指令	5.2.3 信息摘要和数字签名指令	5.2.4 证书和CA指令	5.3 OpenSSL基本指令的应用	5.3.1 创建CA	5.3.2 计算文件摘要	5.3.3 加密算法运算速度表	本章小结	复习思考题	第6章 OpenSSLEVP编程	6.1 对称算法以及Base64编码编程	6.1.1 主要数据结构和函数说明	6.1.2 程序举例	6.2 公钥算法编程	6.2.1 相关函数说明	6.2.2 程序举例	6.3 哈希摘要算法编程	6.3.1 相关函数说明	6.3.2 程序举例	6.4 消息鉴别码MAC算法编程	6.4.1 函数说明	6.4.2 程序举例	6.5 摘要签名和验证算法编程	6.5.1 相关函数说明	6.5.2 程序举例	本章小结	复习思考题	第7章 OpenSSL应用与高级编程	7.1 SSL / TLS编程	7.1.1 一个基本的服务器	7.1.2 一个基本的客户端	7.1.3 服务器和客户端证书的生成	7.1.4 有SSL“握手”的服务器	7.1.5 有SSL“握手”的客户端	7.2 双向认证的SSL连接	7.2.1 双向认证的SSL服务器	7.2.2 双向认证的SSL客户端	7.3 PKI编程	7.3.1 PKI编程概述	7.3.2 X-509标准的编程实现	7.3.3 PKCS#7标准的编程实现	7.3.4 PKCS#12标准的编程实现	7.4 OpenSSL高级编程	7.4.1 BIO库	7.4.2 OpenSSL的Engine机制	本章小结	复习思考题	参考文献
------------	--------	--------------------	--------------------	-----------------	--------------	----------------------	-------------------	-------------------	------	-------	------------	-------------	-----------------	---------------	---------------	------------	-----------	------------------	-----------------	------------	----------------	------------	------------------	-------------	------------------------	------------------------	----------	-------------------	----------------	----------------	------------	---------------	------------	------------	------------	--------------	-------------------	------------	----------------	-------------	------	-------	---------------------	-----------------	----------------	---------------------	---------------------	-----------------	------------------------	------------	------	-------	------------------------	-------------------	---------------------	----------------------	--------------------	---------------	------------	------------	-----------------	-------------------	-----------------------	---------------	---------------------	-----------------	---------------------	-------------------------	----------------------	----------------------	--------------------	------	-------	------------------------	---------------	----------------------	--------------------	--------------------------------	-------------------	-------------------	---------------	-------------------	---------------	--------------------	------------	--------------	-----------------	------	-------	------------------	----------------------	-------------------	------------	------------	--------------	------------	--------------	--------------	------------	------------------	------------	------------	-----------------	--------------	------------	------	-------	--------------------	-----------------	----------------	----------------	--------------------	--------------------	--------------------	----------------	-------------------	-------------------	-----------	---------------	--------------------	---------------------	----------------------	-----------------	------------	------------------------	------	-------	------

<<网络安全编程与实践>>

章节摘录

第一篇第1章概述1.1引言1.1.1计算机网络面临的主要威胁当你遨游在Internet浩瀚无际的信息海洋时，就会发现计算机只有同网络相连，才是名副其实的计算机，从一定意义上讲，“网络就是计算机”，“计算机就是网络”，两者密不可分。

随着计算机网络的飞速发展，这一关于计算机的现代理念已经越来越得到人们的认可。

因此，要给计算机网络安全下定义，首先要了解计算机安全的概念。

国际标准化组织（ISO）将计算机安全定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。

”综合上述计算机安全的定义以及计算机和网络的密切关系，可以给计算机网络安全作如下定义：“保护计算机网络系统中的硬件、软件及其数据不受偶然或者恶意原因而遭到破坏、更改、泄露，保障系统连续可靠地正常运行，网络服务不中断。

”计算机网络如此容易受到侵害，由于主要存在两个方面的问题：一方面，资源共享是计算机网络的重要特点，这对于无数的计算机用户无疑是天大的好事，否则，网络也不会受到人们的如此青睐。

但也正是因为共享，却被一些别有用心者钻了空子，使得网络信息及网络设备的安全容易受到种种不同程度的威胁；另一方面，从网络协议结构设计看，如今使用最广泛的网络协议是TCP / IP协议，它最初的主要设计目标是互联、互通、共享，而不是安全。

实践证明，该协议中已被发现有许多安全漏洞和隐患，这是因为研制者在设计初并没有过多考虑网络的安全性能。

因此，计算机技术包括网络技术，虽然已经从过去的研究阶段进入了商品实用阶段，但是它的技术基础却是不安全的，有其脆弱的一面，这是不可否认的客观事实。

<<网络安全编程与实践>>

编辑推荐

《网络安全编程与实践》是关于介绍“网络安全编程与实践”的教学用书，书中首先介绍了网络安全基础概念，然后重点介绍网络安全编程中常用的两种重要的开发包CryptoAPI、OpenSSL的编程方法和技巧。

<<网络安全编程与实践>>

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>