第一图书网, tushu007.com

<<网络安全>>

图书基本信息

书名：<<网络安全>>

13位ISBN编号：9787030319234

10位ISBN编号：7030319230

出版时间：2011-7

出版时间：科学出版社

作者：胡建伟

页数：276

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

内容概要

网络安全和密码学是当今通信与计算机领域的热门课题。
本书系统地介绍了网络安全问题。
胡建伟编著的这本《网络安全》共14章，内容包括网络安全综述、对称密码学、单向散列函数、公钥密码系统、因特网与
TCP/IP安全、VPN和IPSec、SSL和TLS、身份认证及其应用、访问控制与系统审计、防火墙技术、入侵检测系统、安全编程、恶意代码安全和无线局域网安全。
本书内容新颖、丰富，各章节都提供了参考资料和思考题，以供进一步学习研究。

《网络安全》可作为信息对抗、通信、电子或计算机相关专业的教材，也可作为相关领域的研究人员和专业技术人员的参考书。

第一图书网, tushu007.com

书籍目录

丛书序
前言
第1章 网络安全综述
1.1 安全概念和术语
1.2 网络安全威胁
1.2.1 脆弱性、威胁和风险
1.2.2 网络威胁的类型
1.3 网络攻击
1.3.1 网络攻击的定义
1.3.2 攻击的一般过程
1.3.3 攻击的主要方式
1.4 X.800安全体系结构
1.4.1 安全攻击、安全机制和安全服务
1.4.2 安全服务
1.4.3 安全机制
1.4.4 服务和机制之间的关系
1.5 X.805安全体系框架
1.6 网络安全模型
1.7 安全评估与风险管理
1.7.1 评估方法
1.7.2 评估标准
1.7.3 评估的作用
1.7.4 安全风险管理
思考题
第2章 对称密码学
第3章 单向散列函数
第4章 公钥密码系统
第5章 因特网TCP/IP安全
第6章 VPN和IPSec
第7章 SSL和TLS
第8章 身份认证及其应用
第9章 访问控制与系统审计
第10章 防火墙技术
第11章 入侵检测系统
第12章 安全编程
第13章 恶意代码安全
第14章 无线局域网安全
参考文献

章节摘录

版权页：插图：威胁可能是主动性的（当系统状态可被改变时），也可能是被动性的（不改变系统状态但非法泄露信息）。
伪装成合法主体和拒绝服务是主动性威胁的例子，窃听获取口令是被动性威胁的例子。
威胁可能是由黑客、恐怖分子、破坏分子、有组织犯罪或政府发起的，但相当数量的威胁来自组织内部人员。
安全风险来源于安全脆弱性与安全威胁的结合。
例如，操作系统应用的溢出漏洞（即脆弱性）加上黑客的知识、合适的工具和访问（即威胁）可产生万维网服务器攻击的风险。
安全风险的后果是数据丢失、数据损坏、隐私失窃、诈骗、宕机及失去公共信任。
1.2.2 网络威胁的类型威胁定义为对脆弱性的潜在利用，这些脆弱性可能导致非授权访问、信息泄露、资源耗尽、资源被盗或者被破坏。
网络安全与保密所面，临的威胁可以来自很多方面，并且是随着时间的变化而变化。
网络安全的威胁可以是来自内部网或者外部网的，根据不同的研究结果表明，有80%-95%的安全事故来自内部网。
显然只有少数网络攻击来自互联网。
一般而言，主要的威胁种类有以下10种。

编辑推荐

《普通高等教育信息安全类国家级特色专业系列规划教材:网络安全》以实践能力为培养目标，以安全缺陷为教学实例，系统阐述网络安全的核心概念及关键技术。
以开放系统安全协议体系为框架，山浅入深，层层展开。
概念阐述直观，叙述简练，图文并茂，实例丰富。
内容攻防兼备，理论实践并重。
可赠送电子课件给任课教师。

第一图书网, tushu007.com

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