# <<网络信息安全技术概论>>

## 图书基本信息

书名：<<网络信息安全技术概论>>

13位ISBN编号：9787030273802

10位ISBN编号：703027380X

出版时间：2010-5

出版时间：科学出版社

作者：吕林涛 编

页数：327

## 前言

进入21世纪以来，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世纪发展的潮流和核心。
Internet／Intranet的发展，使得信息化带动了社会的工业化、现代化，网络技术为人类的进步作出了巨大的贡献。
网络的发展使人们可以通过一个终端与世界相连接，世界变得越来越小，人类的交往变得越来越便利，与此同时，个人机密数据、口令、银行账号等个人信息的隐私性安全问题日益凸显，这使得机遇与挑战并存。
随着信息技术的发展，特别是计算机网络技术的发展，人们的诸多活动越来越多地依赖于网络空间，然而，网络空间并非总是安全的。
当前，我国的网络信息安全正面临着严峻的挑战。
一方面随着电子政务工程的启动、电子商务的开展以及国家关键基础设施的网络化，网络安全的需要更加严格和迫切。
另一方面，黑客攻击、病毒传播以及形形色色的网络攻击日益增加，网络安全防线十分脆弱。
因此，网络信息安全在信息社会中将扮演极为重要的角色，它直接关系到国家安全、企业经营和人们的日常生活。
网络安全不仅是一个技术问题，也是法律问题和社会问题，所以网络安全教育必须与信息教育同步开展。
信息科技工作者除了要掌握专业技术以外，还应具有良好的网络文化道德，懂得网络管理的政策法规，能营造良好的网络文化氛围，不做网上违法的事情。
所以，网络安全教育包括网络安全技术与网络安全法规两个方面。
无疑网络信息安全问题的研究和技术的开发是现在和将来相当时期内重要的热点。
在计算机、信息学科的专业教育中开设网络信息安全的课程，旨在让学生们从一开始学习网络技术时就树立建立安全网络的观念，掌握网络安全的基本知识，了解设计和维护安全的网络体系及其应用系统的基本手段和常用方法，为从事信息网络的研究和开发打下良好的基础。
本书分为13章，通过对网络安全的基本概念、安全标准和网络安全防护体系、数据加密技术、密钥管理技术、数字签名和认证技术、黑客技术、漏洞扫描技术、入侵检测技术、Internet的基础设施安全、防火墙技术、计算机病毒与恶意代码防治技术、基于生物特征的身份认证技术、信息隐藏技术和网络信息审计等技术的阐述，较全面地介绍了计算机网络信息安全的基本理论和关键技术；对当前常用的网络安全技术的原理和应用进行了详细的阐述，每章均附有习题。
在此基础之上，基于生物特征的身份认证技术、信息隐藏技术和网络信息审计技术等可作为进一步学习的技术。
为了加强网络法规的教育，在附录中提供了与网络安全相关的部分法规，供读者工作、学习参考之用。
因此，本书既能够作为初学者的教材与自学用书，也可作为网络工作者常备的参考书。

# <<网络信息安全技术概论>>

## 内容概要

《网络信息安全技术概论（第2版）》系统介绍了计算机网络信息安全的基本理论和关键技术，主要内容包括：网络安全的基本概念、安全标准和网络安全防护体系、数据加密技术、密钥管理技术、数字签名和认证技术、黑客技术、漏洞扫描技术、入侵检测技术、Internet的基础设施安全技术、防火墙技术、计算机病毒与恶意代码的防治、基于生物特征的身份认证技术、信息隐藏技术和网络信息审计技术等。

《网络信息安全技术概论（第2版）》的附录给出了近年来国家有关部门出台的网络安全方面的主要相关法规。

《网络信息安全技术概论（第2版）》可作为高等学校信息安全、计算机科学与技术、信息管理和通信等专业及其他IT有关专业本科生和研究生的教材，也可作为从事网络信息安全技术的教学、科研和工程技术人员的参考书。

# <<网络信息安全技术概论>>

## 书籍目录

## 章节摘录

插图：1.1.1网络安全的基本概念网络安全从其本质上来讲就是网络上的信息安全。
从广义来说，凡是涉及网络匕信息的保密性、完整性、可用性、真实性和可控性的相关技术与原理，都是网络安全所要研究的领域。
网络安全是指网络系统的硬件、软件及其系统中的数据的安全，它体现于网络信息的存储、传输和使用过程。
所谓的网络安全性就是网络系统的硬件、软件及其系统中的数据受到保护，不会由于偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。
从不同的角度来说，网络安全具有不同的含义。
从一般用户的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改等手段对用户信息的损害和侵犯，同时也希望用户信息不受非法用户的非授权访问和破坏。
从网络运行和管理者角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源的非法占用及非法控制等威胁，制止和防御网络“黑客”的攻击。
对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，给国家造成巨大的经济损失，甚至威胁到国家安全。
从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

## 编辑推荐

《网络信息安全技术概论(第2版)》：普通高等教育“十一五”规划教材

# <<网络信息安全技术概论>>

## 版权说明