<<网络安全与信息保障>>

图书基本信息

书名：<<网络安全与信息保障>>

13位ISBN编号：9787302268642

10位ISBN编号：7302268649

出版时间：2012-1

出版时间：清华大学出版社

作者：仇建平

前言

路由与交换型网络基础与实践教程随着计算机网络技术的飞速发展，互联网已经深入到社会的各个方面，它对人们的工作方式、生活方式甚至思维方式都产生了巨大的影响，因此，可以说互联网已经成为现代人生活中不可缺少的一部分。

但是，人们在享受互联网所带来愉悦的同时，也不可避免地受到一系列网络及信息安全问题的困扰：网络上充斥虚假信息、非法信息，病毒日益猖狂，黑客攻击无孔不入等，这些都严重危及到个人、企事业单位乃至国家的信息安全。

研究如何采取有效的方法来保护重要信息变得越来越有必要，本书便是在这样一个大背景下编撰而成的。

本书立足于当前网络安全与信息保障的具体实践，深刻而全面地反映了现代网络安全与信息保障的新理论、新方法、新成果。

本书在内容的选择上注重学术性、实用性、创新性与可获得性，同时也综合考虑了不同学校和不同单位的教学实际，力求内容典型、精炼、新颖，具有代表性和可操作性。

创造性地将网络安全与信息保障工具融进了传统教学中，充分揭示了网络安全与信息保障的新进展；系统而全面地介绍了常用的网络安全与信息保障理论；集中介绍了网络安全与信息保障实践，相关实验的介绍基本涵盖了网络安全与信息保障有关的内容；系统而全面地阐述了网络攻防的途径与方法，重点介绍了网络攻防的实例；系统而全面地总结了网络安全与信息保障的国内外进展。

其中，网络攻防是国内相近专著和教材中所未包含的全新内容。

在全面总结当前国内外网络安全与信息保障和利用教材、专著、教学实践经验的基础上，提炼出基本适合于网络安全与信息保障教学、能力教育与培养的核心内容，在教学实践基础上增加了创新性的新内容，相关内容丰富了网络安全与信息保障理论，对于增强学生的相关能力，提高综合素质都有重要的意义。

因此，本书作为一本以信息安全为核心的教材，从实用和可获得性理论的角度出发专门介绍网络攻防的方法和技巧，这是国内对网络安全与信息保障课教学实践和教材使用上的大胆创新，对于全面提高信息管理、计算机科学与技术专业学生的信息素质和综合利用相关工具进行信息安全管理的能力、增强学生的信息安全意识和管理信息能力都有重要的现实意义和深远影响。

编者　　2011年9月

<<网络安全与信息保障>>

内容概要

《21世纪高等院校计算机网络工程专业规划教材：网络安全与信息保障》全面介绍了网络安全与信息保障的基本框架，网络安全与信息保障的基本理论，以及网络安全与信息保障方面的管理、配置和维护，具有如下特点。
内容先进，结构新颖。
书中吸收了国内最先进的新技术、新知识、新方法和国际通用准则，注重科学性、先进性、操作性。
?注重实用的特色。
坚持“实用、特色、规范”的原则，突出实用及素质能力培养，在内容安排上，通过大量案例将理论知识与实际应用有机结合。
资源配套。
《21世纪高等院校计算机网络工程专业规划教材：网络安全与信息保障》提供配套的电子教案，并有辅助的实验，内容包括学习指导、实验教学、练习测试和课程设计等。
《21世纪高等院校计算机网络工程专业规划教材：网络安全与信息保障》可作为本科院校计算机类、信息类、电子商务类和管理类专业的信息安全相关课程的教材，也可作为培训及参考用书，还可作为高职院校相关专业师生的选修教材。

<<网络安全与信息保障>>

书籍目录

章节摘录

版权页：插图：信息和支持进程、系统以及网络都是重要的业务资产。
为保证组织富有竞争力，保持现金流顺畅和组织赢利，以及遵纪守法和维护组织的良好商业形象，信息的保密性、完整性和可用性是至关重要的。
各个组织及其信息系统和网络所面临的安全威胁与日俱增，来源也日益广泛，包括利用计算机欺诈、窃取机密、恶意诋毁破坏等行为，以及火灾或水灾。
危害的来源多种多样，如计算机病毒、计算机黑客行为、拒绝服务攻击等，这些行为呈蔓延之势、用意更加险恶，而且手段更加复杂。
组织对信息系统和服务的依赖意味着自身更容易受到安全威胁的攻击。
公共网络与专用网络的互联以及对信息资源的共享，增大了对访问进行控制的难度。
分布式计算尽管十分流行，但降低了集中式专家级控制措施的有效性。
很多信息系统在设计时，没有考虑到安全问题。
通过技术手段获得安全保障十分有限，必须辅之以相应的管理手段和操作程序才能得到真正的安全保障。
确定需要使用什么控制措施需要周密计划，并对细节问题加以注意。
作为信息安全管理的最基本要求，组织内所有的雇员都应参与信息安全管理。
信息安全管理还需要供应商、客户或股东的参与。
也需要参考来自组织之外的专家建议。
如果在制定安全需求规范和设计阶段时就考虑到了信息安全的控制措施，那么信息安全控制的成本会很低，并更有效率。
1.网络安全潜在威胁计算机网络所面临的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。
影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；也有可能是外来黑客对网络系统资源的非法使用。
目前，归结起来网络安全所面临的主要潜在威胁有以下几方面。
（1）信息泄密。
主要表现为网络上的信息被窃听，这种仅窃听而不破坏网络中传输信息的网络侵犯者称为消极侵犯者。
（2）信息被篡改。
这就是纯粹的信息破坏，这样的网络侵犯者称为积极侵犯者。
积极侵犯者截取网上的信息包，并对之进行更改使之失效，或者故意添加一些有利于自己的信息起到信息误导的作用。
积极侵犯者的破坏作用最大。
（3）传输非法信息流。
用户可能允许自己同其他用户进行某些类型的通信，但禁止其他类型的通信，如允许电子邮件传输而禁止文件传送。

编辑推荐

《21世纪高等院校计算机网络工程专业规划教材:网络安全与信息保障》内容包括网络安全概述、网络安全与信息加密技术概述、数字签名和认证技术、信息隐藏技术等。

<<网络安全与信息保障>>

版权说明