<<网络安全原理与技术>>

图书基本信息

书名：<<网络安全原理与技术>>

13位ISBN编号：9787030288394

10位ISBN编号：7030288394

出版时间：2010-10

出版时间：科学出版社

作者：冯登国，徐静　编著

页数：336

前言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。
计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。
数字化的生存方式席卷全球。
农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。
古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。
电子政务、电子商务等各种信息化应用之花，如雨后春笋，在华夏沃土上竞相开放，炎黄子孙们，在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。
科学规律的掌握，非一朝一夕之功。
治水、训火、利用核能都曾经经历了多么漫长的时日。
不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。
生产力的发展，为社会创造出许多新的使用价值。
但是，工具的不完善，会限制这些使用价值的真正发挥。
信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性，存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾驭技能不足的情况下损害着人们自身的利益。
世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。
传统社会存在的不文明、暴力，在信息空间也同样存在。
在这个空间频频发生的有些人利用系统存在的脆弱性，运用其“暴智”来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。
人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。
随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点，因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

<<网络安全原理与技术>>

内容概要

本书主要介绍了一系列安全技术和用于保护计算机网络的安全协议、安全策略。
主要内容包括：一方面是基本的术语、概念、方法和技术的介绍，包括密码技术，实现安全服务的方法和策略，IDS技术，网络攻击技术和PKI技术；另一方面是一些典型的安全协议标准和技术标准的介绍，包括IPSec协议，TLS协议，IKE协议，PGP协议，3G安全体系，无线局域网安全标准IEEE 802．1li和安全评估准则。
为便于读者掌握和巩固所学知识，书中配备了大量习题。
本书可作为高等院校计算机、通信、信息安全、密码学等专业的硕士生和本科生的教材，也可供从事相关专业的教学、科研和工程技术人员参考。

<<网络安全原理与技术>>

书籍目录

章节摘录

插图：随着信息技术的发展与应用，信息安全的内涵在不断的延伸，要对信息安全给出一个精确的定义似乎很难，但当前情况下，信息安全可被理解为在既定的安全密级的条件下，信息系统抵御意外事件或恶意行为的能力，这些事件和行为将危及所存储、处理或传输的数据以及经由这些系统所提供的服务的可用性、机密性、完整性、非否认性、真实性和可控性。
这六种性质的具体含义如下：1）可用性（availability）是指尽管存在可能的突发事件如供电中断、自然灾害、事故或攻击等，但用户依然可得到或使用数据，服务也处于正常运转状态。
2）机密性（confidentiality）是指保护数据不受非法截获和未经授权浏览。
这一点对于敏感数据的传输尤为重要，同时也是通信网络中处理用户的私人信息所必须的。
3）完整性（integrity）是指保障被传输、接收或存储的数据是完整的和未被篡改的。
这一点对于保证一些重要数据的精确性尤为关键。
4）非否认性（non-repudiation）是指保证信息行为人不能事后否认曾经对信息进行的生成、签发、接受等行为。
这一点可以防止参与某次通信交换的一方事后否认本次交换曾经发生过。
5）真实性（authenticity）是指保证实体（如人、进程或系统）身份或信息、信息来源的真实性。
6）可控性（controllability）是指保证信息和信息系统的授权认证和监控管理。
这一点可以确保某个实体（人或系统）的身份的真实性，也可以确保执政者对社会的执法管理行为。
信息网络作为一种传输信息系统，由于其广泛的应用，其安全问题日益突出，也成为人们关注的一个焦点。
信息网络安全（简称网络安全）问题的解决除了要考虑网络自身的安全因素之外，还必须综合考虑操作系统、数据库、应用系统、人员管理等因素，但本书主要侧重于介绍网络自身的安全因素。
目前网络安全已不再是军方和政府要害部门的一种特殊需求。
实际上所有的网络应用环境包括银行、电子交易、政府（无密级的）、公共电信载体和互联／专用网络都有网络安全的需求。
关于这些典型应用环境的安全需求参见表1.1。

编辑推荐

《网络安全原理与技术(第2版)》：信息安全国家重点实验室。

版权说明