<<信息安全概论>>

图书基本信息

书名：<<信息安全概论>>

13位ISBN编号：9787040123142

10位ISBN编号：7040123142

出版时间：2003-9

出版时间：高等教育

作者：段云所

页数：257

字数：330000

前言

随着网络应用的发展和普及，网络与信息安全的重要性日益突出。
国内外有关信息安全的研究与开发力度都在不断加大。
学术界研究力量明显增加，许多大学和科研机构都设立了信息安全研究室（所、院）。
科技主管部门也加大支持力度，如“十五”期间，国家“863”计划专门设立信息安全主题，重点支持信息安全领域关键技术的研究和产业化。
有关部门也出台了相应法规、标准、指南，成立专门的测评认证机构，加强对信息安全的监管。
产业界涌现了大批信息安全公司，仅防火墙一个产品，国内就有几百家公司在研制生产。
行业用户也加大投入，很多行业纷纷制定技术规范和总体方案，并组织产品选型。
实施安全建设。
普通个人用户也十分关心自己计算机的安全和隐私。
总之，信息安全弓I起了社会各界的广泛关注，面对这样的局面，高等院校开始将信息安全纳入主修课程，本书正是为适应这样的需求而编写的。
本书是作者在北京大学开设信息安全课程的讲义的基础上完成的，比较全面地论述了信息安全的基础理论和技术原理，包括密码理论与应用、身份认证、访问控制、审计、安全脆弱性分析、入侵检测、防火墙、安全协议等。
为了让学生能更好地将理论和原理与应用结合起来，还安排了安全标准和应用安全等内容。
在具体编排上既考虑内容的完整性，又考虑到课时的限制，因此，大部分章节适合一周（3~4学时）内讲授，少数章节需要5～6学时，但根据具体情况可删节。
全部课程约需50~60学时，适合一学期讲授。
本书被列为普通高等教育“十五”国家级规划教材。
本书的编写得到高等教育出版社的大力支持。
北京大学计算机系的研究生刘迎、胡嵩、张锦懋、武勇、张明、徐鹏为本书的编写做了很多工作。
在此一并表示衷心感谢。
由于编者水平有限，时间仓促，书中难免有错误和不当之处，敬请读者和同行专家批评指正。

<<信息安全概论>>

内容概要

本书被列为普通高等教育“十五”国家级规划教材。
本书系统地论述了信息安全的理论、原理、技术和应用。
主要内容有：对称加密算法（DES、AES）、公钥密码算法（RSA、ECC）安全散列算法（SHA）、数字签名（DSS）、数字证书、认证机构CA、身份认证、访问控制、安全审计、安全威胁分析、安全扫描、入侵检测、防火墙、IPSec协议、SSL协议、安全评估标准（TCSEC、CC、GB17859）、Web安全、Email安全（PGP、S/MIME）、电子商务安全（SET协议）等。
本书适合作为高等院校本科或研究生教材使用，也可供研究或开发人员参考。

<<信息安全概论>>

书籍目录

章节摘录

插图：公钥证书按包含的信息分为两种：一种是身份证书，能够鉴别一个主体与它的公钥关系，证书中列出了主体的公钥；另一类是属性证书，是包含了实体属性的证书，属性可以是成员关系、角色、许可证或其他访问权限。
使用属性证书可以鉴别许可证、凭据或其他属性。
现在讨论最多的是身份证书，这类证书提供了认证、数据完整性和机密性。
但是它虽然解决了安全传输问题，但还不足以提供授权。
因为在授权中，更多考虑的是主体的属性而不是身份，根据这些属性决定授权。
为了管理方便、安全，可互操作，通常将这些授权信息从身份中提取出来，与公钥证书同样的方式加以保护，这就是属性证书。
证书中签名算法标识符是用来标识签署证书所用的数字签名算法和相关参数。
如SHA一1和RSA.的对象标识符就用来说明该数字签名是利用RSA对SHA.1杂凑加密。
主体公钥信息包括主体的公钥及所用的加密算法。
可选的扩展项包括：机构密钥标识符（用来区分同一个颁发者的多对证书签名密钥1、主体密钥标识符（用来区分同一个证书拥有者的多对密钥）、密钥用途（指明运用证书中的公钥可完成的各项功能和服务）、扩展密钥用途（说明证书中的公钥的特别用途）、CRI。
分布点、私钥使用期、证书策略（一系列的与证书颁发和使用有关的策略对象标识符和可选的限定符）、主体别名（如主体的邮件地址、IP地址等）、CA别名（如CA的邮件地址、IP地址等）、主体目录属性（证书拥有者的一系列属性）等。
有必要对CRL分布点进一步解释。
当一个给定的PKI系统的CRL.变得非常大时，就要创建许多小的CRI。
用于分发，而不是使用单一的大CRL。
这些较小的CRI。
可以更容易检索和处理。
为了使用CRL。
分布点，CA需要提供一个指向位于颁发证书中CRI_，分布点扩展项中的位置的指针。
该指针包括一个DSN名字、一个II，地址或者一个Web服务器上的特定文件名，可以使依托主体定位CLR分布点。

编辑推荐

《信息安全概论》是普通高等教育“十一五”国家级规划教材

版权说明