<<网络安全与管理>>

图书基本信息

书名：<<网络安全与管理>>

13位ISBN编号：9787302299493

10位ISBN编号：7302299498

出版时间：2012-10

出版时间：张素娟、吴涛、 朱俊东 清华大学出版社 (2012-10出版)

作者：张素娟，吴涛，朱俊东 著

页数：401

<<网络安全与管理>>

内容概要

《高等院校计算机教育系列教材：网络安全与管理》结合作者多年从事网络管理的经验，由浅入深地介绍了网络安全和网络管理的相关内容。
从基础理论知识，到实际应用，再到具体配置，结合例证和最新技术发展及趋势，全面介绍了如何加强网络的安全性和可管理性。
本内容理论充足，覆盖范围广泛、层次分明。

全书共分为11章，各章的主要内容说明如下：第1、2章介绍了网络安全的基本概念、基本要求、安全体系和安全协议等基础理论知识；第3章介绍了加密及加密算法的相关理论；第4～6章分别从操作系统、Web站点和邮件系统出发介绍了相关的安全知识；第7章介绍了如何使用防火墙加强内网的安全性；第8章介绍了病毒的危害、种类及如何预防：第9章介绍了网络攻击及防护的相关知识：第10、11章介绍了网络管理的基本理论和技术，以及相关的网管软件。
综观全书，既有理论讲解，也有实际应用；既介绍了主流技术，也介绍了新技术的发展动向。

《高等院校计算机教育系列教材：网络安全与管理》既可以作为大学本科计算机及信息相关专业的教材，也为网络管理人员提供了很好的参考。

<<网络安全与管理>>

书籍目录

章节摘录

版权页： 插图： 在实际的CA认证环境中不可能只有一个CA中心，多个CA中心之间必然存在一个信任关系模型。
信任关系模型建立的目的是确保一个认证机构颁发的证书，能够被其他认证机构的用户所信任。
信任关系模型有：严格层次信任模型、分布式信任模型、以用户为中心的信任模型和交叉认证模型等。
CA认证中心的功能有以下几个方面。
（1）证书的颁发 认证中心负责接收、验证用户（包括下级认证中心和最终用户）的数字证书申请，同时将申请的内容进行备案，并根据申请的内容确定是否受理该数字证书申请。
如果认证中心接受该数字证书申请，则进一步确定给用户颁发何种类型的证书。
新证书用认证中心的私钥签名以后，发送到目录服务器供用户下载和查询。
为了保证消息的完整性，返回给用户的所有应答信息都要使用认证中心的签名。
（2）证书的更新 认证中心可以定期更新所有用户的证书，或者根据用户的请求来更新用户的证书。
（3）证书的查询 证书的查询功能分为两类，一类是证书申请的查询，认证中心根据用户的查询请求返回当前用户证书申请的处理过程；另一类是用户证书的查询，这类查询由目录服务器来完成，目录服务器根据用户的请求返回适当的证书。
（4）证书的作废 当用户的私钥由于泄密等原因造成用户证书需要申请作废时，用户需要向认证中心提出证书作废的请求，认证中心根据用户的请求确定是否将该证书作废。
另外一种证书作废的情况是证书已经过了有效期，认证中心将自动把证书作废。
证书的作废功能由认证中心通过维护证书作废列表（CRL，Certificate Revocation List）来完成。
（5）证书的归档 证书都具有一定的有效期，证书过了有效期之后就应该作废。
因为有时可能需要验证以前的某个交易过程中产生的数字签名，因此作废的证书不能简单地丢弃。
基于此类考虑，认证中心还应当具备作废证书和作废私钥的管理功能。

编辑推荐

《高等院校计算机教育系列教材:网络安全与管理》在编写时联系当前技术的发展，加入了大量新的技术和新的应用内容，既充分体现了时代特色，又实实在在地让读者领略到新技术所带来的实惠。
《高等院校计算机教育系列教材:网络安全与管理》既可以作为大学本科计算机及信息相关专业的教材，也为网络管理人员提供了很好的参考。

版权说明