<<网络安全技术>>

图书基本信息

书名：<<网络安全技术>>

13位ISBN编号：9787302293910

10位ISBN编号：7302293910

出版时间：2013-1

出版时间：清华大学出版社

作者：曾湘黔 编

页数：341

字数：549000

<<网络安全技术>>

内容概要

《网络安全技术》全面系统地介绍了计算机网络安全技术。
全书共分13章，内容包括网络安全概述、密码学与信息安全、网络安全协议、网络设备常见安全技术、internet安全技术、网络操作系统安全分析及防护、防火墙技术、入侵检测技术、网络嗅探技术、端口扫描技术与漏洞扫描技术、网络病毒防范技术、黑客攻击与防护技术、网络安全解决方案。

《网络安全技术》每章都有思考题，有针对性地帮助读者理解本书的内容。

《网络安全技术》可作为高校计算机及其相关专业“网络安全技术课程”教材，也可供相关的技术人员使用。

<<网络安全技术>>

书籍目录

章节摘录

版权页： 插图： 实际上，这种服务并不能消除服务的抵赖性，也就是说，它并不能防止一方否认另一方对某件已发生的事情所做出的声明。
它所能够做的只是提供无可辩驳的证据，以支持快速解决任何这样的纠纷。
抗抵赖服务的出发点不仅仅由于在通信各方之间存在着相互欺骗的可能性，另外它也反映了这样一个现实，即没有任何一个系统是完备的，而且也可能出现通信双方最终达不成一致协议这样的情况。
（1）数据源的抗抵赖 向数据接收者提供数据来源的证据，以防止发送者否认发送该数据或其内容的任何企图。
（2）传递过程的抗抵赖 向数据发送者提供数据已到目的地的证据，以防止收信者否认接收该数据或其内容后的任何事后的企图。
2.安全机制 为了支持以上的安全服务，ISO安全体系结构定义了8大类安全机制：加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、通信业务填充机制、路由控制机制和公证机制。
这些安全机制可以设置在适当的层次上，以便提供某些安全服务。
1）加密机制 加密是提供数据保护最常用的方法。
加密算法按密钥的类型可分为对称密钥算法和非对称密钥（也称公开密钥）算法；按密码体制可分为序列密码算法和分组密码算法。
这些算法具有不同的优缺点，根据加密的层次和加密对象可采用不同的算法。
由于加密机制的存在，就有密钥管理机制。
2）数字签名机制 在通信双方交换数据时，为防止否认、伪造、篡改、冒充等，采用数字签名技术。
数字签名机制还规定了两个过程：一是对数据单元签名，二是验证已签名的数据单元。
签名机制的本质特征是只能使用签名者私有信息签名。
因此，当验证签名时，可在事后的任何时候向第三方（如审查员或仲裁员）证实只有私有信息的唯一持有者才能产生这个签名。
3）访问控制机制 访问控制机制是按照事先确定的规划，决定主题对客体的访问是否合法。
当主体试图非法使用未经授权使用的资源（客体）时，访问机制的功能将拒绝这一企图，并可附带报告这一事件给审计跟踪系统，审计跟踪产生一个报警或形成部分追踪审计。
访问控制机制的实现常常基于一种或多种机制措施，如访问控制信息库、鉴别信息（如口令）、权力、安全标志、试图访问的时间、试图访问的路由和访问的持续时间等。
4）数据完整性机制 数据完整性包括两种形式：数据单元完整性和数据单元序列的完整性。
保证数据完整性的一般方法是：发送实体在数据单元上加标记，这个标记是数据本身的函数，是经过加密的；接收实体产生对应的标记，并将所产生的标记与接收到标记相比较，以确定在传输过程中疏忽是否被修改过。
数据单元序列的完整性是要求数据编号的连续性和时间标记的正确性（不是过时的），以防止假冒、丢失、重发、插入或修改数据。
5）鉴别交换机制 鉴别交换机制是以交换信息的方式来确认实体身份的机制。
用于鉴别交换的技术有：①口令。
由发方实体提供，收方实体检测。
②密码技术。
将交换的数据加密，只有合法用户才能解密。
③使用该实体的特征或拥有物。
这时采用的技术是指纹识别和身份卡等。

<<网络安全技术>>

编辑推荐

《普通高等学校网络工程专业规划教材:网络安全技术》每章都有思考题，有针对性地帮助读者理解《普通高等学校网络工程专业规划教材:网络安全技术》的内容。
《普通高等学校网络工程专业规划教材:网络安全技术》可作为高校计算机及其相关专业“网络安全技术课程”教材，也可供相关的技术人员使用。

版权说明