<<信息安全技术教程>>

图书基本信息

书名：<<信息安全技术教程>>

13位ISBN编号：9787302305248

10位ISBN编号：7302305242

出版时间：2013-1

出版时间：清华大学出版社

作者：杜彦辉

页数：383

字数：615000

<<信息安全技术教程>>

内容概要

《信息安全技术教程》从信息安全领域的基础入手，系统、全面地介绍信息安全理论和实践知识，并尽可能地涵盖信息安全技术的主要内容，对发展起来的新技术做详细介绍。
此外，还增加实践内容，介绍相关工具软件以及具体信息安全技术实施的具体方法。

《信息安全技术教程》共19章，主要内容包括信息安全基础知识、密码技术、认证技术、安全协议、安全事件处理、访问控制与权限设置、防火墙技术、入侵检测、系统安全扫描技术、病毒防范与过滤技术、信息安全风险评估技术、灾难备份与恢复技术、计算机与网络取证技术、操作系统安全、操作系统加固、安全审计原则与实践、应用开发安全技术、信息安全建设标准、构建企业安全实践等。

《信息安全技术教程》结构清晰、内容翔实，具有很强的可读性，适合作为高等院校信息安全专业本科生和相关专业的高年级本科生或研究生教材，也适合供相关科研人员和对信息安全相关技术感兴趣的读者阅读。

<<信息安全技术教程>>

书籍目录

章节摘录

版权页： 插图： 3.3 认证技术 随着网络安全技术的不断发展，已经出现了多种不同的认证技术。
根据不同的功能水平和安全需要，这些认证技术可以单独使用，也可以同时使用。
主要的认证技术包括口令认证、公开密钥认证、远程认证、匿名认证和数字签名认证。
3.3.1 口令认证 口令认证是最古老、最简单的一种认证方法，经常作为系统的默认设置。
口令认证包括可重用口令认证、一次性口令认证、挑战应答口令认证和混合口令认证。
1.可重用口令认证 可重用口令认证有两种类型：用户（user）认证和客户端（client）认证。
用户认证通常由申请使用系统资源的用户发起。
接到用户的资源使用请求后，服务器向用户索要用户名和口令，然后将这些信息和数据库上的信息进行比对，如果匹配成功，用户请求被允许，可以访问系统资源。
例如，人们在使用电脑时，需要输入用户名和口令，就是最简单的用户认证。
客户端认证 一般情况下，用户请求服务器的认证，然后被授权使用系统资源。
用户通过认证并不意味着可以自由使用任何想要的系统资源。
通过认证只是说明用户被授权使用所请求的那些资源，但并不能超过这个限度。
这种类型的认证就叫做客户端认证。
这种认证根据用户的身份，使用户受限访问系统的资源。
可重用口令认证方法简单、运行速度快、使用广泛，但也存在着一系列的问题。
为了避免记忆复杂口令，用户常会选择简单口令，或把口令值记录下来，增加了安全隐患。
同时，随着计算机计算水平的提高，通过蛮力攻击能够很容易破解系统的口令值。
2.一次性口令认证 一次性口令认证也被称为会话认证，认证中的口令只能被使用一次，然后被丢弃，从而减少了口令被破解的可能性。
在一次性口令认证中，口令值通常是被加密的，避免明文形式的口令被攻击者截获。
最常见的一次性口令认证方案是S／Key和Token方案。
（1）S／Key口令 这种口令认证基于MD4和MD5加密算法产生，采用客户—服务器模式。
客户端负责用hash函数产生每次登录使用的口令，服务器端负责一次性口令的验证，并支持用户密钥的安全交换。
在认证的预处理过程中，服务器将种子以明文形式发送给客户端，客户端将种子和密钥拼接在一起得到S。
然后，客户端对S进行hash运算得到一系列一次性口令。
也就是说，第一次口令是通过对S进行N次hash运算得到，下一次的口令是通过对S进行N—1次hash运算得到。
在服务器端保存着用户上一次成功登录的口令值，因此，当用户访问系统时，服务器只需要将本次传输过来的口令进行一次hash运算。
如果得到结果和存储的值一致，就验证了用户身份的正确性。

<<信息安全技术教程>>

编辑推荐

《教育部实用型信息技术人才培养系列教材:信息安全技术教程》结构清晰、内容翔实，具有很强的可读性，适合作为高等院校信息安全专业本科生和相关专业的高年级本科生或研究生教材，也适合供相关科研人员和对信息安全相关技术感兴趣的读者阅读。

版权说明