<<网络安全基础>>

图书基本信息

书名：<<网络安全基础>>

13位ISBN编号：9787302239161

10位ISBN编号：7302239169

出版时间：2011-1

出版时间：斯托林斯(William Stallings)、白国强、 等 清华大学出版社 (2011-01出版)

作者：斯托林斯

页数：328

译者：白国强

<<网络安全基础>>

前言

由William Stallings编著的这本书，已成为网络安全方面最重要的一本教科书。
2007年笔者曾与其他人合作把本书第3版翻译为中文并推荐给读者。
现在它的第4版也已出版发行，我们再次把它（第4版）翻译为中文，希望它仍能够作为我国高校相关课程的教材使用，或作为普通网络安全爱好者学习和了解网络安全基本知识的参考书。
该书第4版保持了其一贯的特点，即完全从实用的角度出发，尽量用较小的篇幅对网络安全解决方案中实际使用的主要算法、重要协议和系统管理方法等方面的原理做全面而详细的介绍。
全书仍分为3大部分：第1部分为密码学，非常简要地介绍了常用的对称加密、消息认证和公钥密码等；第2部分为网络安全应用，介绍了各种重要网络安全工具和应用，包括密钥分配与用户认证、传输层安全、无线网络安全、电子邮件安全.和IP安全等；第3部分为系统安全，简述了系统级安全问题，包括网络入侵、恶意软件和防火墙等。
与第3版相比，第4版变化很大，总结起来主要体现为如下几个方面。
1.大幅度地调整了内容，包括：（1）在内容总量和一定篇幅下，作者采用“在线章节”（online chapters）的方法，直接删除了第3版中的部分章节和附录，把它们放在了网上：（2）增加了对随机数和伪随机数的介绍；（3）把第2部分网络安全应用的叙述由原来的自下而上顺序（从IP层到应用层及网络管理安全）改为自上而下（从用户认证到IP层安全）：（4）新增一章（第6章）专门介绍无线网络安全。
2.改写和充实了大部分章节，主要包括：（1）调整部分章内叙述顺序，使其更符合初学者逻辑：（2）对材料的叙述更符合实际情况，如IEEE、NIST标准等；（3）增加和更新叙述，使介绍的内容尽可能地符合最新的网络安全实际状况，如改IPv4为IPv6；（4）引入用户认证概念；（5）删除了SET（安全电子交易），改为对安全盾（SSH）的介绍等。
3.大量地充实了习题。
与第3版比较，各章习题几乎都得到了很大的扩充，随着教学实践的进行，这充分说明该书作为教材，其教学经验得到了积累。

<<网络安全基础>>

内容概要

在这样一个全球电子互连，电脑病毒和电子黑客充斥，电子窃听和电子欺诈肆虐的时代，安全不再是问题的确已经过去。
两大趋势使书中所讨论的内容显得尤为重要。
第一，计算机系统及其网络互连的爆炸性增长已经增强了机构和个人对利用这些系统存储与交换信息的依赖程度。
这样，进一步又使得人们意识到对保护数据和资源免遭泄漏，保障数据和信息的真实性，以及保护基于网络的系统免受攻击等问题的必要性。
第二，密码学和网络安全已经成熟，并正在开发实用而有效的应用来增强网络安全。

<<网络安全基础>>

作者简介

作者：（美国）斯托林斯（William Stallings） 译者：白国强 等斯托林斯（William Stallings），已经在全面理解计算机安全、计算机网络和计算机架构的技术发展方面做出了突出贡献。
他已是17部著作的作者，如果把修订版也算进去，则总共是该领域各，方面42本书的作者。
他的作品已经出现在相当多ACM和IEEE出版物中，包括Proceedings Of the IEEE和ACM Computer Reviews。
他已经11次获得了由教材与学术作者协会(Text and Academic Authors Association)颁发的最佳计算机科学教材年度奖。

<<网络安全基础>>

书籍目录

章节摘录

插图：DES的强度对DES强度的分析可以分解为两部分：对算法本身的分析和对使用56比特密钥的分析。
前一种情况指的是通过研究算法的性质而破译算法的可能性。
这些年来，对寻找和研究该算法的弱点进行了非常多的尝试，使得DES是现存加密算法中被研究得最彻底的一个。
尽管通过了那么多尝试，迄今为止仍然没有人成功找到DES的致命缺陷。
另外一个更重要的考虑是密钥长度。
56比特的长度有2个可能的密钥，约为7.2×10个。
因此，从表面看来，穷举攻击是不可行的。
穷举攻击时假设平均情况下必须有一半的密钥空间要被穷举，那么每微秒做一次DES加密的一台机器需要超过1000年（见表2.2）的时间来破解密文。
但是，每微秒做一次加密的假设过于保守了。
DES最终被确定为不安全是在1998年7月，电子前沿阵线（Electronic Frontier Foundation，EFF）宣布使用一个制造费用少于250000美元的专用“DES破解机（DES cracker）”就能够破解DES加密，所需的攻击时间不超过3天。
EFF公布了对这个机器的详细描述，使得其他人能够制造他们自己的破解机[EFF98]。
当然，硬件的价格将随着速度的提升而持续下降，使DES变得没有实际价值。
需要指出，密钥搜索（key-search）攻击不仅仅是运行经过全部可能的密钥那么简单。
除非已经给出了已知明文，不然破译还需要辨认出明文。
如果消息仅仅是直白的英语文本，那么很容易得到结果，尽管必须使辨认英语的工作自动化。
如果文本消息在加密前经过了压缩，那么辨认要困难得多。
同时如果消息是更一般的数据类型，比如用数字表示的文件，并且被压缩过，问题就变得更难以自动化。
因此，在穷举攻击之外，需要在一定程度上了解预期的明文，也需要一些能自动分辨出明文的方法。
EFF同样指出了这个问题，并且介绍了一些在很多情况下都有效的自动化技术。

编辑推荐

《网络安全基础:应用与标准(第4版)》：世界著名计算机教材精选

版权说明