<<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：9787302229728

10位ISBN编号：7302229724

出版时间：2010-7

出版时间：清华大学

作者：斯托林斯

页数：417

前言

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. Two trends have come together to make the topic of this book of vital interest. First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Second, the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security.It is the purpose of this book to provide a practical survey of network security applications and standards. The emphasis is on applications that are widely used on the Internet and for corporate networks, and on standards (especially Internet standards) that have been widely deployed. This book is intended for both an academic and a professional audience. As a textbook, it is intended as a one-semester undergraduate course on network security for computer science, computer engineering, and electrical engineering majors. It covers the material in IAS2 Security Mechanisms, a core area in the Information Technology body of knowledge; and NET4 Security, another core area in the Information Technology body of knowledge. These subject areas are part of the Draft ACM/IEEE Computer Society Computing Curricula 2005.

<<网络安全基础>>

内容概要

本书由著名作者William Stallings编写，以当今网络安全的实际解决方案为基础，既简明扼要，又全面系统地介绍了网络安全的主要内容，包括基本原理、重要技术、主要方法和重要的工业标准等。
全书共包含11章。
除第1章引言外，其余各章分为三大部分叙述：第一部分是密码学，重点介绍分组密码、流密码，消息认证码、安全杂凑函数、公钥密码和数字签名等的基本原理、主要方法和重要应用场景等，并简要介绍了几种常用的典型算法，包括DES算法、AES算法、RC4算法和RSA算法等；第二部分是网络安全应用，简要介绍了传输层安全中的SSL／TLS协议、无线局域网安全及WAP协议、电子邮件安全与PGP与SIM，ME协议、IP层安全与IPsec协议等。
第三部分是系统安全，简要介绍了入侵检测与口令管理、恶意软件与防火墙等。
　　本书以最新和实用的网络安全知识为主题，采用深入浅出的叙述手法，每章末尾还给出一定的推荐读物和思考练习题。
因此，本书既是高等学校网络安全基础课程的好教材，也是工程技术人员和网络爱好者了解网络安全基本概貌的好读物。

作者简介

作者：（美国）斯托林斯（William Stallings）

<<网络安全基础>>

书籍目录

章节摘录

插图：3DES has two attractions that assure its widespread use over the next few years. First, with its 168-bit key length, it overcomes the vulnerability to brute-force attack of DEA. Second, the underlying encryption algorithm in 3DES is the same as in DEA. This algorithm has been subjected to more scrutiny than any other encryption algorithm over a longer period of time, and no effective cryptanalytic attack based on the algorithm rather than brute force has been found. Accordingly, there is a high level of confidence that 3DES is very resistant to cryptanalysis. If security were the only consideration, then 3DES would be an appropriate choice for a standardized encryption algorithm for decades to come.The principal drawback of 3DES is that the algorithm is relatively sluggish in software. The original DEA was designed for mid-1970s hardware implementation and does not produce efficient software code. 3DES, which has three times as many rounds as DEA, is correspondingly slower. A secondary drawback is that both DEA and 3DES use a 64-bit block size. For reasons of both efficiency and security, a larger lock size is desirable.Because of these drawbacks, 3DES is not a reasonable candidate for long-term se. As a replacement, NIST in 1997 issued a call for proposals for a new Advanced ncryption Standard (AES), which should have a security strength equal to or better han 3DES and significantly improved efficiency. In addition to these general equirements, NIST specified that AES must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits. Evaluation criteria included security, computational efficiency, memory requirements, hardware and software suitability, and flexibility.

编辑推荐

《网络安全基础:应用与标准(第4版)(影印版)》：大学计算机教育国外著名教材系列

版权说明