

<<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：9787030322043

10位ISBN编号：7030322045

出版时间：2011-7

出版时间：科学出版社

作者：覃建诚，白中英 编著

页数：272

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<网络安全基础>>

内容概要

《网络安全基础》由覃健诚、白中英编著，立足于网络多层纵深防御体系架构，将网络安全划分成6个层次，并分别介绍了各个层次上的典型技术和理论知识。本书共8章：第1章网络安全概论，第2章安全理论基础知识，第3章物理级安全，第4章操作系统级安全，第5章系统软件级安全，第6章应用程序级安全，第7章业务级安全，第8章内容级安全。

《网络安全基础》以安全防御为主导，将攻击与防御内容相结合，理论基础与实际技术并重。全书结合作者在网络安全方面所做的科研工作，着眼于建立相对完整的知识框架和应用基础，内容既具有基础性，同时又跟踪时代性前沿以启发创新。

本书可作为高等院校计算机和信息类专业高年级本科生及相关专业研究生的专业基础课教材，也可作为信息产业工程技术人员的参考书。

<<网络安全基础>>

书籍目录

前言

第1章 网络安全概论

- 1.1 从信息安全到网络安全
 - 1.1.1 信息安全的未来发展
 - 1.1.2 信息安全的概念
 - 1.1.3 网络安全的知识体系
 - 1.1.4 信息安全的未来趋势
- 1.2 网络安全的层次结构
- 1.3 网络攻防与信息战简介
 - 1.3.1 网络攻防典型阶段
 - 1.3.2 网络攻防示例
 - 1.3.3 信息战
- 1.4 多层纵深防御体系及其策略
 - 1.4.1 安全防御的可用策略
 - 1.4.2 纵深防御的意义
 - 1.4.3 多层纵深防御体系架构
- 1.5 网络安全技术的相关学科

第2章 安全理论基础知识

- 2.1 现代密码学
 - 2.1.1 保密通信系统模型
 - 2.1.2 单密钥加密模式
 - 2.1.3 双密钥加密模式
 - 2.1.4 无密钥加密模式
 - 2.1.5 生物特征
 - 2.1.6 量子密码学
- 2.2 计算机网络
 - 2.2.1 OSI七层网络模型
 - 2.2.2 TCP/IP协议
 - 2.2.3 有线网络
 - 2.2.4 无线网络
- 2.3 并行计算体系结构
 - 2.3.1 计算机体系结构简介
 - 2.3.2 单处理机并行技术
 - 2.3.3 多处理机并行技术
 - 2.3.4 分布式并行技术
- 2.4 可靠计算
 - 2.4.1 系统可靠性与产品质量控制
 - 2.4.2 RAID、ECC与CRC
 - 2.4.3 虚拟机与机群技术
 - 2.4.4 网络存储与容灾备份
 - 2.4.5 软件可靠性
- 2.5 可信任计算
 - 2.5.1 安全计算的可信任基础
 - 2.5.2 可信任模块TPM与TCM
 - 2.5.3 PKI及其认证中心

<<网络安全基础>>

2.5.4 网络信任的去中心化

2.6 信息编码理论

2.6.1 信息论基础

2.6.2 信源编码与数据压缩

2.6.3 信道编码与检错纠错

2.6.4 保密编码与纠错密码理论

第3章 物理级安全

3.1 硬件设施防护

3.1.1 人为物理接触

3.1.2 外界环境灾害

3.1.3 设施自身故障

3.2 网络线路防护

3.2.1 有线侦听及侵扰

3.2.2 无线侦听及侵扰

3.2.3 线路破坏

3.2.4 ARP欺骗

3.3 操作人员防护

3.3.1 人为失误

3.3.2 社交工程学攻击

3.3.3 内部人员侵害

3.4 物理级安全措施

3.4.1 物理隔离与电磁屏蔽

3.4.2 硬件冗余备份及写保护

3.4.3 芯片级安全设施

3.4.4 灾备移动服务器

第4章 操作系统级安全

4.1 系统漏洞

4.1.1 操作系统安全基础

4.1.2 端口扫描与主机漏洞扫描

4.1.3 升级补丁与零日攻击

4.1.4 缺陷屏蔽与功能屏蔽

4.2 恶意代码

4.2.1 病毒、木马、蠕虫

4.2.2 强制性软件与逻辑炸弹

4.2.3 Rootkit

4.2.4 恶意代码查杀

4.3 操作系统级安全措施

4.3.1 进程任务监控

4.3.2 防火墙与沙盒模型

4.3.3 IDS与IPS

4.3.4 虚拟网络与虚拟机机群

第5章 系统软件级安全

5.1 数据库防护

5.1.1 系统软件及其安全层次

5.1.2 数据库入侵与权限提升

5.1.3 数据库账号与权限设置

5.1.4 数据备份与恢复策略

<<网络安全基础>>

5.2 Web站点防护

- 5.2.1 网页篡改与钓鱼网站
- 5.2.2 网站基本安全设置
- 5.2.3 网站安全保护体系

5.3 DNS域名解析

- 5.3.1 DNS域名系统架构
- 5.3.2 动态DNS与缓存投毒
- 5.3.3 DNS劫持及其防范

5.4 邮件服务器

- 5.4.1 SMTP、POP3与IMAP4协议
- 5.4.2 邮件转发与匿名发送
- 5.4.3 邮件服务器安全设置

5.5 常规安全防护

- 5.5.1 默认设置与定制性安全
- 5.5.2 权限控制与ACL
- 5.5.3 SSH加密与安全审计

第6章 应用程序级安全

6.1 常见应用程序缺陷

- 6.1.1 缓冲区溢出漏洞
- 6.1.2 SQL注入和脚本注入漏洞
- 6.1.3 异常数据处理漏洞
- 6.1.4 程序后门与信息泄漏

6.2 Web应用程序安全

- 6.2.1 Web应用程序的基本原理
- 6.2.2 常见应用程序级防御
- 6.2.3 国际机场安检模式
- 6.2.4 代码审查、质检及形式化

6.3 浏览器插件与远程监控一

- 6.3.1 插件的安全隐患
- 6.3.2 XSS跨站脚本攻击
- 6.3.3 浏览器的区域安全设置
- 6.3.4 远程监控与音视频入侵

第7章 业务级安全

7.1 身份认证与权限控制

- 7.1.1 统一身份认证及单点登录
- 7.1.2 CA认证体系与信誉度担保
- 7.1.3 因素认证及验证码
- 7.1.4 U盾与生物特征认证
- 7.1.5 账号管理与权限控制

7.2 数字签名

- 7.2.1 摘要与散列函数
- 7.2.2 数字签名及其验证
- 7.2.3 碰撞攻击与篡改
- 7.2.4 数据重传与中间人攻击

7.3 安全多方计算

- 7.3.1 秘密共享
- 7.3.2 多方排序

<<网络安全基础>>

7.3.3 多方签名与电子投票

第8章 内容级安全

8.1 信息访问控制

8.1.1 数据访问权限

8.1.2 备份保护与加密存储

8.1.3 数据销毁与恢复

8.1.4 保密通信与VPN

8.2 信息隐藏

8.2.1 信息隐藏的基本原理

8.2.2 典型隐藏方法

8.2.3 隐藏信息分析

8.3 DRM数字版权管理

8.3.1 知识产权

8.3.2 数字水印

8.3.3 防盗版技术

参考文献

章节摘录

版权页：插图：第1章 网络安全概论 计算机网络是现代信息的载体。

本章全方位地对网络安全的概念加以介绍：纵向——讲述信息安全的历史与发展趋势；横向——讲述网络安全的层次结构划分和多层纵深防御体系；深度——列举网络安全技术的主要相关学科。从而给读者一个网络安全的宏观印象，以便他们系统全面地学习网络安全知识。

1.1 从信息安全到网络安全 1.1.1 信息安全的 历史发展 信息安全这一术语的诞生与人类通信技术的进步密切相关。

信息安全的研究可分如下五个阶段。

第一阶段：古典密码时代。

如果把信息视作一种客观存在，那么人类历史从很早以前就已经在使用信息。

对信息安全的保护也可以追溯到公元前400多年，甚至更早。

大约公元前440年，在古希腊战争中出现“隐写术”，它将情报写在头上，利用头发掩盖。

大约公元前400年，斯巴达人用羊皮纸绕在锥形棒上，写上情报。

羊皮纸解开之后，信息杂乱无章，只有绕在同样大小的锥形棒上才能够重新呈现出来。

大约公元前100年的古罗马时代，凯撒（Caesar）密码是凯撒大帝用来保护重要军事情报的加密系统，它是一种置换密码，通过将字母按顺序推后3位起到加密作用，如将字母A换作字母D，将字母B换作字母E。

凯撒密码是一种古典密码术，比起现代密码学中的各种加密算法，显然太简单了，但它已经具备了密码学中的一些基本要素。

明文是指原始的、可以直接认知的信息。

密文是指加密之后得到的、不能直接认知的信息。

密钥是指加密、解密过程中要用到的关键信息。

加密是指把原始信息（明文）转化为不可直接认知的信息（密文）的正常过程。

解密是指把加密后的信息（密文）转化为原始信息（明文）的正常过程。

破解是指在没有密钥的情况下，以非正常的方式从密文中提取全部或部分明文信息，或者获取到全部或部分密钥信息的过程。

凯撒密码中，全部字母推后3位，密钥其实就是3。

这个密钥在当时是不公开的。

【例1】解密凯撒密码的密文“KHOOR ZRUOG”。

解：把密文字母推前3位，得到明文“HELLO WORLD”。

编辑推荐

《普通高等教育计算机类特色专业系列规划教材:网络安全基础》由覃健诚、白中英编著，内容理论性和实用性并重。

作者根据多年从事网络安全工作的经验认识到，形形色色的安全问题的本质“万变不离其宗”，新技术总是在原有知识的基础上诞生的，只要懂理论就能够理解，也能够想出应对办法。

作者在《普通高等教育计算机类特色专业系列规划教材:网络安全基础》提出了多层纵深防御体系架构，将网络安全划分成多个层次，从物理层到内容层，各层可以动态部署各种安全技术，形成纵深防御体系。

这种架构可以使孤立防线的网络安全的脆弱性得到有效改观。

《普通高等教育计算机类特色专业系列规划教材:网络安全基础》定位于网络安全的入门教材，着眼于建立相对完整的知识框架和应用基础。

《普通高等教育计算机类特色专业系列规划教材:网络安全基础》没有对各种安全技术作深入详尽的论述，仅列举出涉及的理论知识和部分典型技术，点到为止。

要想深入学习网络安全的各种具体内容，可以参考相关的专业文献资料。

基础性与时代性结合，具有完整的知识框架。

立足网络各层纵深防御体系，六个安全层次。

涉及各种网络安全相关技术，攻击与防御相结合。

以例子揭示深奥原理，通俗易懂，逐步配套资源库光盘。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>