高等学校网络空间安全专业规划教材

网络安全

沈鑫剡 等 编著

清华大学出版社

642

■ 高等学校网络空间安全专业规划教材

网络安全

沈鑫剡 俞海英 伍红兵 李兴德 编著

清华大学出版社
北京

内 容 简 介

本书将网络安全理论、网络安全协议和主流网络安全技术有机集成在一起，既能让读者掌握完整、系统的网络安全理论，又能让读者具备运用网络安全协议和主流网络安全技术解决实际网络安全问题的能力。

全书内容分为三部分，一是网络安全理论，包括加密算法、报文摘要算法等；二是网络安全协议，包括 IPSec、TLS、HTTPS、DNS Sec、SET、S/MIME 等；三是主流网络安全技术，包括以太网安全技术、无线局域网安全技术、互联网安全技术、虚拟专用网络、防火墙、入侵检测系统、病毒防御技术和计算机安全技术等。主流网络安全技术是本书的重点。

本书以通俗易懂、循序渐进的方式叙述网络安全知识，并通过大量的例子来加深读者对网络安全知识的理解。本书内容组织严谨，叙述方法新颖，是一本理想的计算机专业本科生的网络安全教材，也可作为计算机专业研究生的网络安全教材，对从事网络安全工作的工程技术人员，也是一本非常好的参考书。

图书在版编目(CIP)数据

网络安全/沈鑫剡等编著. —北京：清华大学出版社，2017
(高等学校网络空间安全专业规划教材)
ISBN 978-7-302-46723-6

Ⅰ. ①网… Ⅱ. ①沈… Ⅲ. ①计算机网络－网络安全－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 040284 号

责任编辑：袁勤勇　薛　阳
封面设计：傅瑞学
责任校对：焦丽丽
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：27.75　　**字　　数**：637 千字
版　　次：2017 年 8 月第 1 版　　**印　　次**：2017 年 8 月第1次印刷
印　　数：1～2000
定　　价：59.00 元

产品编号：069871-01

本书特色

本书有机集成网络安全理论、网络安全协议和主流网络安全技术，结合网络安全理论讨论主流网络安全技术的实现原理，让读者知其所以然。

在具体网络环境下讨论运用网络安全协议和网络安全技术解决实际网络安全问题的方法和过程，培养读者运用网络安全协议和网络安全技术解决实际网络安全问题的能力。

配套的实验教材《网络安全实验教程》与本书相得益彰，使得课堂教学和实验形成良性互动。

前言

对于一本以真正将读者领进网络安全知识殿堂为教学目标的教材，一是必须提供完整、系统的网络安全理论，这样才能让读者理解网络安全技术的实现机制，具有进一步研究网络安全技术的能力；二是必须深入讨论当前主流网络安全技术，同时，结合网络安全理论讨论主流网络安全技术的实现原理，让读者知其所以然。三是需要在具体网络环境下讨论运用网络安全协议和网络安全技术解决实际网络安全问题的方法和过程，让读者具备运用网络安全协议和网络安全技术解决实际网络安全问题的能力，解决读者学以致用的问题。

本书的特点是将网络安全理论、网络安全协议和主流网络安全技术有机集成在一起。既能让读者掌握完整、系统的网络安全理论，又能让读者具备运用网络安全协议和主流网络安全技术解决实际网络安全问题的能力。

全书内容分为三部分，一是网络安全理论，包括加密算法、报文摘要算法等；二是网络安全协议，包括 IPSec、TLS、HTTPS、DNS Sec、SET、S/MIME 等；三是主流网络安全技术，包括以太网安全技术、无线局域网安全技术、互联网安全技术、虚拟专用网络、防火墙、入侵检测系统、病毒防御技术和计算机安全技术等。主流网络安全技术是本书的重点。

本书有配套的实验书《网络安全实验教程》，实验教材提供了在 Cisco Packet Tracer 软件实验平台上运用本书提供的理论和技术设计，配置和调试各种满足不同安全性能的安全网络的步骤和方法，学生可以用本书提供的安全协议和安全技术指导实验，再通过实验来加深理解本书内容，使得课堂教学和实验形成良性互动。

作为一本无论在内容组织、叙述方法还是教学目标都和传统网络安全教材有一定区别的新书，书中疏漏和不足之处在所难免，殷切希望使用本书的老师和学生批评指正。作者 E-mail 地址为：shenxinshan@163.com。

作　者

2017 年 5 月

目录

第1章 概　述

信息技术范畴中的信息是指计算机中用文字、数值、图形、图像、音频和视频等多种类型的数据所表示的内容。网络环境下的信息系统由主机、链路和转发结点组成。信息分为由主机存储和处理的信息，经过链路传输的信息，转发结点中等待转发的信息等。因此，网络环境下的信息安全的内涵包括与保障网络环境下的信息系统中分布在主机、链路和转发结点中的信息不受威胁，没有危险、危害和损失相关的理论、技术、协议和标准等。网络环境下的信息安全也称为网络安全。

1.1 信息和信息安全

信息的表示方式和承载方式是不断变化的，因此，信息安全的目标和内涵也是不断变化的。目前提供服务的信息系统主要是网络环境下的信息系统，因此，信息安全目标与内涵都是基于保障网络环境下的信息系统的服务功能定义的。

1.1.1 信息、数据和信号

1. 信息

信息的定义多种多样，信息技术中的信息通常采用以下定义：信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的本质内容。

信息之所以重要，是因为它小到可以反映一个项目、一次活动的本质内容，如项目和活动计划、项目和活动实施过程等；大到可以反映一个企业、一个国家的本质内容，如企业核心技术、企业财务状况、国家核心机密等。这些本质内容事关项目、活动的成败，企业和国家的兴衰存亡。

2. 数据

数据是记录信息的形式，可以用文字、数值、图形、图像、音频和视频等多种类型的数据表示信息。由于计算机统一用二进制数表示各种类型的数据，因此，计算机统一用二进制数表示信息。

3. 信号

信号(Signal)是数据的电气或电磁表现。信号可以是模拟的，也可以是数字的，模拟信号是指时间和幅度都是连续的信号。数字信号是指时间和幅度都是离散的信号。由于计算机统一用二进制数表示各种类型的数据，因此，在计算机网络中，信号其实是二进制

位流的电气或电磁表现。

1.1.2 信息安全定义

安全是指不受威胁，没有危险、危害和损失。因此，信息安全是指信息系统中的信息不会因为偶然的或者恶意的原因而遭受破坏、更改和泄漏，信息系统能够持续、不间断地提供信息服务。

1.1.3 信息安全发展过程

1. 物体承载信息阶段

1）信息表示形式

早期用于承载信息的是物体，如纸张、绢等，将表示信息的文字、数值、图形等记录在纸张、绢等物体上。完成信息传输过程需要将承载信息的物体从一个物理位置运输到另一个物理位置。

2）存在威胁

物体承载信息阶段，对信息的威胁主要有两种，一是窃取承载信息的物体，二是损坏承载信息的物体。

3）安全措施

这个阶段的安全措施主要有物理安全和加密两种。物理安全用于保证记录信息的物体在储存和运输过程中不被窃取和毁坏。

加密是使得信息不易读出和还原的操作过程。如果记录在物体上的信息是加密后的信息，即使获得记录信息的物体，也无法读出或还原加密前的信息，即原始信息。如斯巴达克人将羊皮螺旋形地缠在圆柱形棒上后再书写文字，书写文字后的羊皮即使落入敌方手中，如果不能将羊皮螺旋形地缠在相同直径的圆柱形棒上，也是无法正确读出原始文字内容的。

古罗马采用凯撒密码。凯撒密码将每一个字符用字符表中后退三个的字符代替，这种后退是循环的，字符 Z 后退一个的字符是 A。这样原文 GOOD MORNING，用凯撒密码加密后变为 JRRG PRUQLKLJ，如果不知道凯撒密码的处理方法，即使得到文本 JRRG PRUQLKLJ，也无法还原原文 GOOD MORNING。

2. 有线通信和无线通信阶段

1）信息传输过程

首先对表示信息的文字、数值等数据进行编码，然后将编码转换成信号，经过有线和无线信道将信号从一个物理位置传播到另一个物理位置。也可以经过有线和无线信道直接将音频和视频信号从一个物理位置传播到另一个物理位置。

2）存在的威胁

有线通信和无线通信阶段，信息最终转换成信号后经过有线和无线信道传播，而信号传播过程中可能被侦听，因此，敌方可以侦听到经过有线和无线信道传播的信号，并通过侦听到的信号还原出信息。