高等学校网络空间安全专业规划教材

信息安全实用教程

沈鑫剡 等 编著

清华大学出版社

...络空间安全专业规划教材

信息安全实用教程

沈鑫剡 沈梦梅 俞海英 李兴德 邵发明 编著

清华大学出版社
北京

内 容 简 介

本书着重培养读者解决实际生活中的信息安全问题的能力，重点讨论病毒防御技术、移动通信安全技术、电子商务和移动支付安全技术、数据安全技术、Windows 7 网络安全技术与 Windows 7 安全审计技术等。

作为面向非计算机专业的信息安全教材，作者基于“大学计算机基础”课程组织教材内容，以浅显易懂的方式阐述信息安全的基础理论，在讨论具体安全技术时，基于信息安全基础理论阐述安全技术的实现原理，让读者知其所以然。

本书内容组织严谨、叙述方法新颖，是一本理想的非计算机专业本科生的信息安全教材，也可作为实用型计算机专业的信息安全教材。对所有需要具备一定信息安全问题解决能力的人员而言，本书是一本非常合适的参考书。

图书在版编目(CIP)数据

信息安全实用教程/沈鑫剡等编著. —北京：清华大学出版社，2018
(高等学校网络空间安全专业规划教材)
ISBN 978-7-302-50315-6

Ⅰ. ①信… Ⅱ. ①沈… Ⅲ. ①信息安全－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2018)第 114975 号

责任编辑：袁勤勇　郭　赛
封面设计：傅瑞学
责任校对：李建庄
责任印制：沈　露

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 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：16.5　　**字　　数**：381 千字
版　　次：2018 年 9 月第 1 版　　**印　　次**：2018 年 9 月第1次印刷
定　　价：39.00 元

产品编号：077039-01

前言

随着计算机应用尤其是移动支付和电子商务的普及，信息安全与人们的日常生活息息相关。保证移动通信、移动支付和电子商务的安全性，保证计算机系统不被病毒侵害，保证计算机中数据的保密性、完整性和可用性，最大限度地利用 Windows 操作系统的网络安全功能，尽量保留黑客入侵计算机系统的证据等，已经成为所有人的必备技能。因此，对非计算机专业学生普及信息安全基础知识，培养学生解决实际生活中的信息安全问题的能力，已成为十分迫切的事情。

目前，面向非计算机专业的信息安全教材通常都有以下两个问题：一是教材内容往往是计算机专业网络安全或信息安全教材的简化版，非计算机专业特性不明显；二是教材内容偏重于理论，缺乏培养解决实际信息安全问题的能力的内容。因此，作者编写了这本以理工类非计算机专业本科生为教学对象的信息安全教材。

本书有以下特色：一是基于“大学计算机基础”课程组织教材内容；二是以浅显易懂的方式阐述信息安全的基础理论；三是在讨论具体安全技术时，基于信息安全基础理论阐述安全技术的实现原理，让读者知其所以然；四是着重培养读者解决实际生活中的信息安全问题的能力，重点讨论病毒防御技术、移动通信安全技术、电子商务和移动支付安全技术、数据安全技术、Windows 7 网络安全技术与 Windows 7 安全审计技术等。因此，本书是一本理想的非计算机专业本科生的信息安全教材，也可作为实用型计算机专业的信息安全教材，本书对所有需要具备一定信息安全问题解决能力的人员而言，也是一本非常好的参考书。

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信息安全教材有一定区别的新教材，书中的错误和不足之处在所难免，殷切希望使用本书的教师和学生批评指正。作者的 E-mail 地址为 shenxinshan@163.com。

作　者

2018 年 6 月

目录

第 1 章 概　述

信息技术领域中的信息其实就是计算机用于表示信息的各种类型的数据。因此，信息安全就是存储在计算机中和经过网络传输的各种类型数据的安全。智能手机既是一个完整的计算机系统，又是一个移动通信设备，智能手机随时随地可以上网的特性和智能手机配备的各种类型的传感器，使得以智能手机为终端设备的移动互联网拥有多种传统互联网所没有的应用。

1.1　信息和日常生活

随着互联网尤其是以智能手机为终端设备的移动互联网的普及，人们的日常生活已经和信息息息相关。信息技术领域中的信息其实就是计算机中用于表示信息的各种类型的数据，因此，和人们日常生活息息相关的信息其实就是计算机中用于表示信息的各种类型的数据。

1.1.1　信息的定义

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，甚至企业和国家的兴衰存亡。

1.1.2　日常生活中的信息

1. 数据类型

人们在日常生活中感受到的、信息技术范畴中的信息其实是计算机用于表示信息的数据，即计算机采集、存储和处理的数据，包括文字、数值、图形、图像、音频和视频等多种类型。计算机中的文字是指用于组成文本的各种字符，这些字符包括英文字母、汉字及其他国家的文字等。计算机中的数值是指表示量的多少的数，可以是整数、实数、十进制数、二进制数、八进制数、十六进制数等。图形是指由外部轮廓线条构成的矢量图，计算机可以对矢量图进行移动、缩放、旋转和扭曲等变换。图像由无数个独立的像素组成，每个像

素独立显示颜色，计算机可以对图像进行移动、缩放等变换，但不能进行旋转和扭曲等变换。音频是指人类可以听到的一切声音。视频是指各种动态影像，每秒超过 24 帧的连续变化的图像也是动态影像。

计算机统一用二进制数表示所有类型的数据，包括文字、数值、图形、图像、音频和视频等。因此，计算机首先需要解决用二进制数存储，并且能够还原所有类型数据的问题。

2. 日常生活中的数据实例

纯文本中的字符属于文字类型的数据，因此，可以由文字类型数据构成纯文本，如完全由文字组成的文档、短消息等。电子商务中的单价、消费金额、购货数量等属于数值类型数据。点、线、面组成的几何图形和由类似 AutoCAD 等绘图软件生成的图形属于图形类型数据。照片等属于图像类型数据。音乐、通话录音等属于音频类型数据。录像、电影等属于视频类型数据。

3. 数据与隐私

人们在日常生活中不断地产生、存储、处理和传输数据，有些数据涉及个人隐私，这些数据的泄露会对人们的生活产生不良的影响，如自拍的照片、记录通话过程的电话录音、拍摄的视频、电子交易过程中输入的账号和密码、作为支付凭证的二维码、电话本中的联系人等。对于个人而言，信息安全就是保证这些数据在存储、处理和传输过程中不被泄露、破坏和篡改。

1.2 信息和网络

智能手机随时随地可以上网的特性和智能手机配备的各种类型的传感器使得以智能手机为终端设备的移动互联网得到广泛应用，移动支付、共享单车等都是移动互联网的典型应用。互联网和移动互联网的广泛应用使得信息安全与人们的日常生活更加息息相关，同时也使得信息安全成为一个更加复杂的问题。

1.2.1 互联网和移动互联网

1. 传统互联网

(1) 互联网结构

传统互联网的结构如图 1.1 所示，主要由三部分组成，分别是各种类型的传输网络、互连传输网络的路由器和主机，主机包括终端和服务器。互联网的核心功能是实现主机

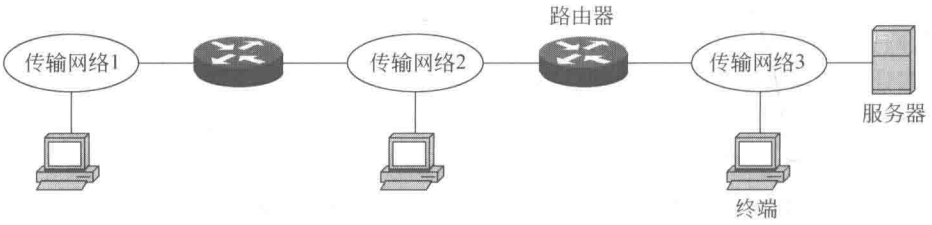

图 1.1 互联网结构

之间的通信过程。实现主机之间通信过程的目的是为了共享资源。根据共享的资源是集中在服务器中还是分布在所有主机中，可以将实现资源共享的应用结构分为客户/服务器结构和对等结构。

(2) 客户/服务器结构

客户/服务器(Client/Server，C/S)结构如图1.2所示，资源集中在服务器中，客户只能共享服务器中的资源。当客户需要访问服务器中的资源时，需要向服务器发送服务请求，服务请求中需要指定访问的资源，服务器根据服务请求中指定的资源，完成该资源的访问过程，并将访问结果通过服务响应反馈给客户。

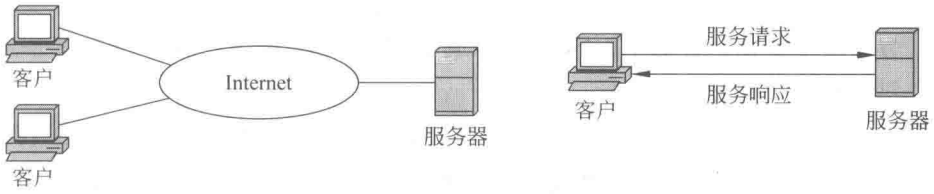

图1.2 客户/服务器结构

(3) 对等结构

对等结构(Peer to Peer，P2P)如图1.3所示，主机不再划分为客户和服务器，所有主机都是对等的，共享的资源分布在所有主机中，因此，每一台主机既是服务请求者，又是服务提供者。

2. 移动互联网

(1) 移动互联网结构

移动互联网是移动终端和互联网的有机结合。移动互联网结构如图1.4所示，笔记本式计算机和平板电脑通过无线局域网接入Internet，智能手机通过无线局域网或通用分组无线业务(General Packet Radio Service，GPRS)、3G、4G等无线数据通信网络接入Internet。

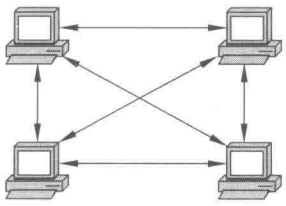

图1.3 对等结构

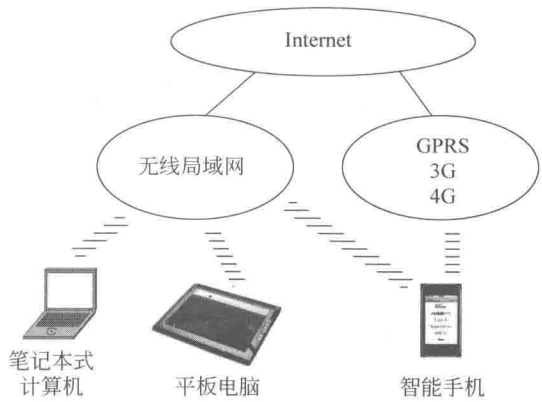

图1.4 移动互联网结构

(2) 移动互联网的要素

移动互联网的要素有三个：一是移动终端，尤其是智能手机；二是无线通信网络；三

是移动互联网应用。

一切便于携带且采用无线通信技术的网络终端都属于移动终端，智能手机无疑是最普及的移动终端。智能手机本身是一个计算机系统，可以安装操作系统，运行应用软件。但智能手机与一般计算机系统相比，又有着以下不同。

- 方便携带。这一特性使得人们随时随地都可以使用智能手机。
- 方便使用。智能手机的触摸屏界面使得任何人都能够操作智能手机，因此智能手机成为使用最普遍的计算机系统。
- 方便连接。智能手机普遍支持无线局域网和无线数据通信网络，这使得智能手机几乎在任何地方都能连接互联网。
- 方便身份鉴别。智能手机的 SIM 卡或 UIM 卡中存有用户身份标识符，从而可以对手机用户身份进行鉴别。
- 丰富的传感器。智能手机配备丰富的传感器，使得智能手机可以完成定位、拍照、摄像、扫描和跟踪等功能。
- 移动通信设备。智能手机作为移动通信网络的移动通信设备，可以实现移动语音通信和短消息的发送、接收过程。

目前常用的连接移动终端的无线通信网络有无线局域网和 GPRS、3G、4G 等无线数据通信网络，家庭和公共场所已经基本普及无线局域网，GPRS、3G、4G 等无线数据通信网络更是覆盖了城乡的每一个角落，因此，移动终端可以随时随地连接互联网。

用户已经开发了大量基于 Android 和 iOS 的应用程序，这些应用程序极大地拓展了智能手机的功能，使得智能手机成为一个无所不能的终端设备，真正做到一机在手、天下我有！

(3) 移动互联网带来的质变

与传统互联网相比，移动互联网具有以下变化。一是大量智能手机接入互联网。智能手机容易操作的特点，使得移动互联网用户数量剧增；二是智能手机随时随地连接互联网的特点，使得移动互联网产生了大量新的传统互联网所没有的应用方式；三是智能手机配备了丰富的传感器，使得移动互联网能够开发出基于位置服务(Location Based Services，LBS)、扫码支付等具有极大应用前景的新型应用领域；四是各种 App 使得智能手机成为一个无所不能的终端设备，订车、订餐、订票甚至家庭监控，都可一机完成。

1.2.2 互联网应用

与人们日常生活相关的互联网应用数不胜数，本节选择以下三种应用进行说明的原因有两个：一是这三种应用及其普及，是绝大多数人所熟悉的互联网应用；二是这三种应用都涉及安全问题，人们对这三种互联网应用普遍感到不安的是安全性，从而可以为讨论互联网环境下的安全问题拉开序幕。

1. 网上购物

网上购物应用系统如图 1.5 所示，用户通过终端接入 Internet，在银行开通网上银行，并开启网上支付功能。商家构建电商平台，允许用户通过互联网选购商品。

(1) 网上购物过程

基于网上支付完成网上购物的过程涉及以下步骤。

① 选择一家银行,在该银行设立一个账户,并为该账户开启网上支付功能。

② 登录电商平台,完成商品选购,支付方式选择网上支付,在商家支持的银行中选中设立账户的银行。

③ 验证银行支付界面,输入账户号码,输入用户身份鉴别信息,完成支付过程。不同银行的用户身份鉴别信息有所不同,如有的银行的用户身份鉴别信息包括设立账户时设定的用户名、密码和动态口令。动态口令是由银行设立账户时交付的动态口令牌产生的,通常情况下每分钟更新一次,银行必须保证动态口令牌产生的动态口令与银行为该账户产生的动态口令一致。图 1.6 所示为一种动态口令牌。

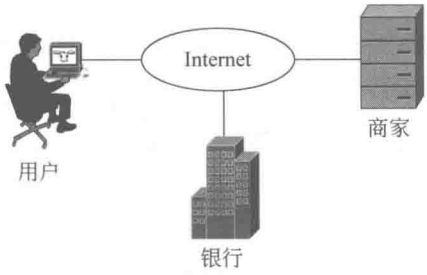

图 1.5 网上购物应用系统

图 1.6 动态口令牌

(2) 网上购物涉及的数据交换过程

网上购物涉及的数据交换过程如图 1.7 所示,用户首先登录商家网站选购商品,在这个阶段,用户和商家网站之间交换的数据主要是与选购商品有关的数据,如商品名称和数量等。用户完成商品选购后,进入支付阶段,支付方式选择网上支付,在商家支持的银行列表中选择用户开设账户的银行。用户选中开设账户的银行后,可以看到该银行弹出的支付界面。在这个阶段,商家与银行之间交换的数据主要是与支付有关的数据,如用户选购的商品清单和需要支付的金额等。用户看到银行弹出的支付界面后,需输入账号、用户名和密码,银行支付界面显示验证信息和商家提供的商品清单与应付金额,用户确认是开设账户的银行后,核对商品清单和应付金额,确认无误后输入动态口令,完成支付过程。在这个阶段,用户与银行之间交换的数据主要是和鉴别用户身份以及完成网上支付过程有关的数据,如账号、用户名、密码和动态口令等。

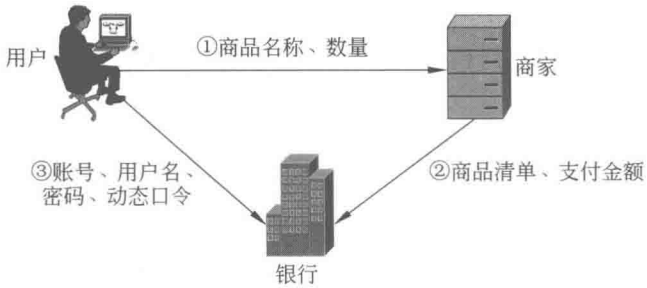

图 1.7 数据交换过程

(3) 网上购物涉及的安全问题

从图 1.7 所示的网上购物涉及的数据交换过程中可以看出，网上购物涉及的安全问题主要有以下几个：一是商家链接的银行支付界面有可能是伪造的银行支付界面，用于窃取用户输入的用户名、密码和动态口令等；二是用户与银行之间交换的与鉴别用户身份和完成网上支付过程有关的数据，如账号、用户名、密码和动态口令等，在传输过程中有可能被截获；三是商家与银行之间交换的与支付有关的数据，如用户选购的商品清单和用户需要支付的金额等，在传输过程中有可能被篡改；四是用户和商家可能否认曾经发送过的信息和进行过的操作，如用户否认曾经在某个电商平台选购商品、否认曾经进行过的支付操作，商家否认曾经向银行发送过商品清单等；五是用户终端和商家的电商平台可能无法正常工作。

2. 微信支付

微信支付应用系统如图 1.8 所示，微信客户端、微信支付系统和商家后台系统通过互联网连接在一起。商家门店通过商家专用网络与商家后台系统连接在一起。微信支付系统通过支付网络与各个微信支付系统支持的银行连接在一起。

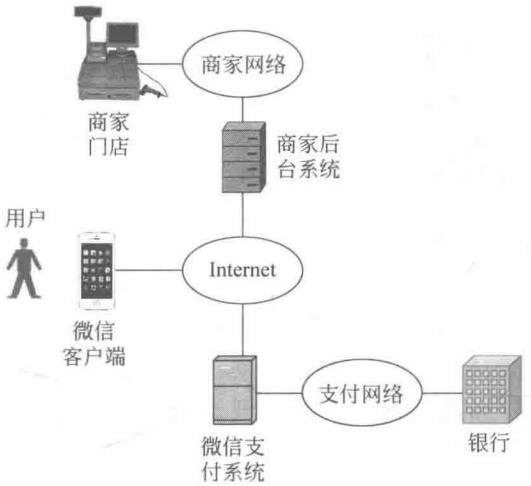

图 1.8 微信支付应用系统

(1) 微信扫码支付过程

微信扫码支付过程包括以下步骤：

① 用户在商家门店完成商品选购过程后，选择微信扫码支付；

② 商家门店生成二维码供用户扫描；

③ 用户用微信“扫一扫”扫描商家门店展示的二维码后，显示商家信息和支付金额，用户确认后，输入支付密码完成支付过程。

(2) 微信扫码支付涉及的数据交换过程

微信扫码支付工作流程如图 1.9 所示，经过互联网传输的数据主要是商家后台系统与微信支付系统之间交换的数据和微信客户端与微信支付系统之间交换的数据。当用户在商家门店完成商品选购过程后，商家门店生成订货信息，包括订单号、商品目录、单价和商品总价等。商家门店将订货信息发送给商家后台系统，商家后台系统生成预支付请求，

并将预支付请求发送给微信支付系统，预支付请求中包含商家账号和订货信息等。微信支付系统为预支付请求创建一项记录，并将该记录标识符作为预支付交易链接发送给商家后台系统。商家后台系统生成预支付交易链接对应的二维码，将预支付交易链接对应的二维码发送给门店系统。门店系统展示预支付交易链接对应的二维码。用户用微信“扫一扫”扫描商家门店展示的预支付交易链接对应的二维码，然后将二维码扫描结果发送给微信支付系统。微信支付系统将用户的微信客户端与商家的预支付请求绑定在一起，然后向微信客户端发送支付验证，支付验证中包括商家信息和支付金额。微信客户端显示商家信息和支付金额，用户确认后输入支付密码，然后微信客户端向微信支付系统发送支付授权。微信支付系统确定微信客户端具有支付权限后，根据用户账号和商家账号绑定的银行卡，请求银行完成支付过程。银行完成支付过程后，向微信支付系统发送支付结果，支付结果中包括支付金额、用户账号、商家账号和订单号等信息。微信支付系统接收到银行发送的支付结果后，向商家后台系统和微信客户端发送支付成功信息，其中包含支付金额和订单号等信息，商家后台系统接收到支付成功信息后，向商家门店发送支付成功信息。商家门店接收到支付成功信息后，向用户提交商品。

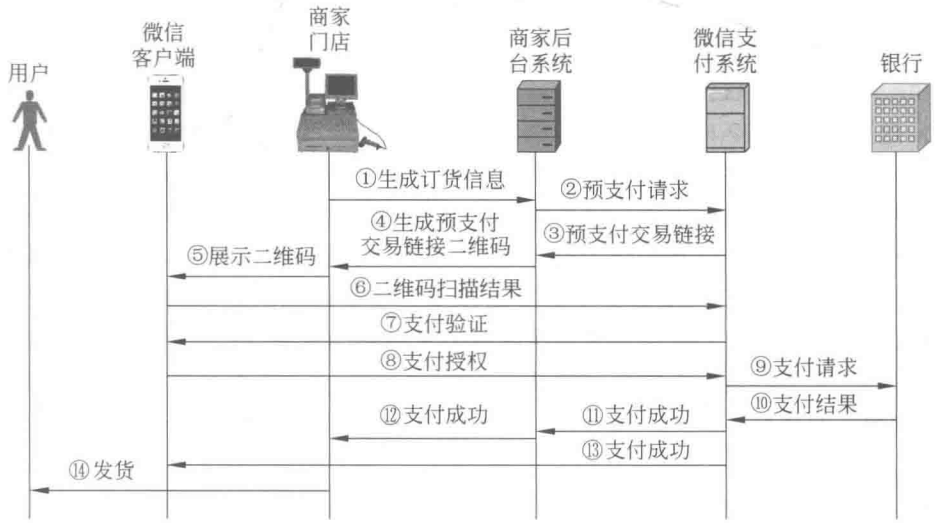

图 1.9 微信扫码支付工作流程

(3) 微信扫码支付涉及的安全问题

微信扫码支付涉及的安全问题主要有以下几个：一是如何确保预支付请求中指明的商家与发送预支付请求的商家是一致的；二是如何确保预支付请求在传输过程中不被篡改；三是如何确保预支付交易链接在传输过程中不被篡改；四是如何确保支付验证在传输过程中不被篡改；五是如何确保支付授权在传输过程中不被截获；六是如何确保微信客户端和商家后台系统无法否认曾经发送过的信息；七是如何确保微信客户端和微信支付系统能够正常工作。

3. 共享单车

共享单车应用系统如图 1.10 所示，目前存在两种类型的共享单车，一种类型的共享