21世纪

高等学校信息安全专业规划教材

软件安全实现
—— 安全编程技术

郭克华 主 编
王伟平 刘 伟 副主编

清华大学出版社

21世纪高等学校信息安全专业规划教材

软件安全实现
——安全编程技术

主　编　郭克华
副主编　王伟平　刘　伟

清华大学出版社
北　京

内 容 简 介

本书共分为16章，针对安全编程技术进行讲解，主要涵盖了基本安全编程、应用安全编程、数据保护编程以及其他内容共四大部分：第一部分包含内存安全、线程/进程安全、异常/错误处理安全、输入安全，第二部分包含国际化安全、面向对象的编程安全、Web编程安全、权限控制、远程调用和组件安全、避免拒绝服务攻击等内容，第三部分包含数据加密保护、其他保护、数字签名等内容，最后一部分包含软件安全测试和代码性能调优。每章后面都有配套练习，用于对本章进行总结演练。

针对安全编程技术，本书不局限于某一门特定语言，而是将编程过程中的通用安全问题进行全面总结，逐步引领读者从基础到各个知识点进行学习，以便能开发出安全可靠的系统。全书内容由浅入深，并辅以大量的实例说明，每一个章节以实际案例为起点进行讲解，通俗易懂。

全书所有实例的源代码均可在清华大学出版社的网站上下载，供读者学习参考使用。

本书可作为有一定编程基础的程序员的学习用书，也可供有经验的开发人员深入学习使用，更可以为高等学校、培训班作为教材使用，对于缺乏安全编程实战经验的程序员而言，阅读本书可以快速积累经验，提高编程水平。

图书在版编目(CIP)数据

软件安全实现——安全编程技术/郭克华主编. —北京：清华大学出版社，2010.6
(21世纪高等学校信息安全专业规划教材)
ISBN 978-7-302-22261-3

Ⅰ. ①软… Ⅱ. ①郭… Ⅲ. ①程序设计—安全技术—高等学校—教材 Ⅳ. ①TP311

中国版本图书馆CIP数据核字(2010)第046563号

责任编辑：魏江江　徐跃进
责任校对：焦丽丽
责任印制：杨　艳
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**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
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：17.75　**字　数**：406千字
版　　次：2010年6月第1版　　**印　　次**：2010年6月第1次印刷
印　　数：1～3000
定　　价：29.00元

产品编号：033270-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人次。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新

Note

能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

（3）实施精品战略，突出重点。规划教材建设把重点放在专业核心（基础）课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

（4）支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

（5）依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21 世纪高等学校信息安全专业规划教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

前言

安全编程技术是一门学科，涵盖的编程语言较多，所需要讨论的问题也较广，因此，目前对于安全编程技术的讲解很容易陷入误区：要么只是针对某一门语言讲解安全问题；要么泛泛而谈，缺乏具体案例。本书针对编程中常见的安全问题进行了阐述，不局限于某一门特定语言，但是每一个话题却以简单、通俗、易懂的案例进行讲解，逐步引领读者从基础到各个知识点进行学习，从而开发出安全可靠的系统。本书涵盖了内存安全、线程/进程安全、异常/错误处理安全、输入安全、国际化安全、面向对象的编程安全、Web 编程安全、权限控制、远程调用和组件安全、避免拒绝服务攻击、数据加密保护、数字签名、安全测试和程序性能调优等内容。每章后面都有配套练习，用于对本章内容进行总结演练。

1. 本书的知识体系

学习本书，需要具有一定的编程基础，至少要对常见语言，如 C++、.NET、Java 有所了解。

本书的知识体系结构如图 1 所示，遵循循序渐进的原则，逐步引领读者从基础到各个知识点的学习。

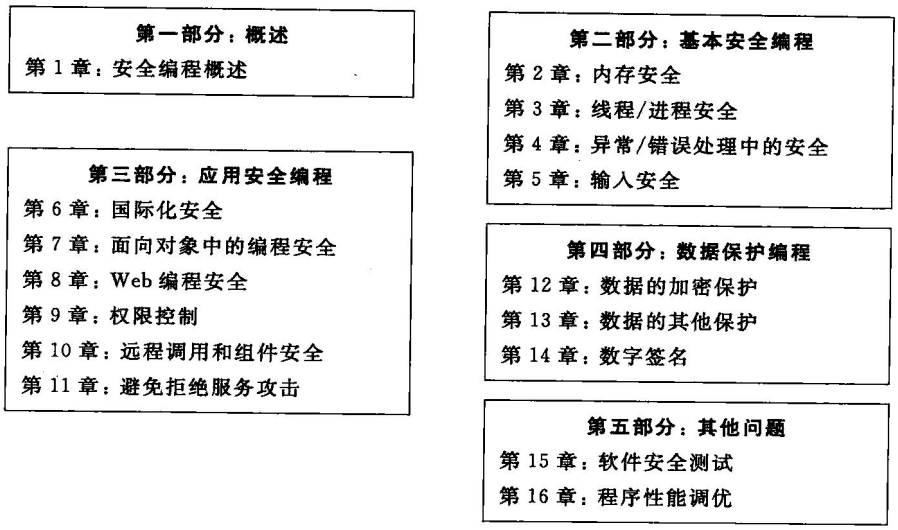

图 1

Note

2. 章节内容介绍

全书共分为16章。

第1章 首先讲解软件安全的概念，然后引出安全编程技术讨论的话题。

第2章 介绍编程中的内存安全，如溢出、字符串操作等。

第3章 介绍编程中的线程和进程安全，对线程同步、协作、死锁等安全问题问题进行讲解。

第4章 介绍异常和错误处理中的安全，从异常的出现到异常的捕捉和处理进行安全方面的讲解。

第5章 讲述输入安全，包括普通输入安全、数据库输入安全以及文件访问中的一些安全问题。

第6章 为国际化安全，讲解国际化过程中的编码和溢出问题。

第7章 讲解面向对象编程中的安全问题。

第8章 介绍Web编程安全，涵盖了目前常见的Web编程安全中的常见问题，如URL操作安全、跨站脚本、SQL注入等。

第9章 针对权限控制中的安全问题进行详细讲解。

第10章 首先讲解远程调用安全，然后讲解组件安全，涵盖了Java和.NET体系中常见组件标准的安全问题讲解。

第11章 讲解拒绝服务攻击的避免方法。

第12章 针对数据保护，讲解加密技术。

第13章 讲解数据的其他保护措施。

第14章 介绍数据保护的另一个技术：数字签名的实现。

第15章 针对测试人员，讲解软件安全测试。

第16章 讲解程序性能调优，严格讲这不是安全编程技术的范围，但是可以为编写安全的系统提供帮助。

本书可作为有一定编程基础的程序员的学习用书，也可供有经验的开发人员深入学习使用，更可以为高等学校、培训班作为教材使用，对于缺乏安全编程实战经验的程序员来说，可用来快速提高编程水平。

全书所有实例的源代码均可在清华大学出版社的网站上下载，供读者学习参考，所有程序均经过了作者精心的调试。

由于时间仓促和作者的水平有限，书中的错误和不妥之处在所难免，敬请读者批评指正。

有关本书的意见反馈和咨询，读者可在清华大学出版社网站的相关栏目中与作者进行交流。

本书配套光盘中的内容，读者也可以在清华大学出版社网站下载。

作　者

2010年3月

目 录

Note

Note

第1章

安全编程概述

现代生活中，计算机的应用已经越来越广泛，给人们的生活带来了巨大的方便。计算机系统的安全问题也越来越受到重视。软件，是组成计算机应用的一个重要部分，当软件由于不安全而遭受攻击，或者运行期间出现错误时，会给用户带来巨大的损失。如犯罪分子利用软件漏洞来获取有价值的信息，用于牟取利益；又如软件因为开发时没有考虑运行时的具体情况，而造成运行的突然崩溃，等等。

越来越频繁的软件安全隐患对软件的开发者——软件工程师，提出了更高的要求，要求程序员能够编写出错误较少的程序，并且能够及时修复软件出现的突发问题，切实为软件使用者服务。本书讲解的安全编程技术主要就是针对这些问题。安全编程是软件质量的重要保证，在软件开发和程序设计中具有重要地位。

不过，实际的软件工程中，安全隐患的出现往往来源于多个方面，给软件系统带来的危害也是多方面的。安全问题的出现原因众多，而某些安全问题又具有不间断发生，难于调试等特点，因此，很难用一个单纯的理论来完全地阐述安全编程问题。基于这个考虑，安全编程的内容只能针对各个侧面来进行阐述，如异常情况下的安全、线程操作中的安全、数据安全加密等。

本章主要针对安全问题进行概述，首先讲解软件安全问题出现的原因，然后阐述软件安全问题的一些表现，并对安全问题进行分类，接下来基于软件开发生命周期，对软件工程中的安全问题进行详细介绍，最后介绍本书的内容。

1.1 软件的安全问题

1.1.1 任何软件都是不安全的

进入21世纪，随着计算机应用的普及，软件在人们的生活中已经渐渐成为一个较为普及的概念，软件也给人们的生活带来了巨大的方便。在日常生活中，人们几乎是随时都可以用到软件，如：

- 购物后结账时，商场收银台上运行的就是能够自动计算总价的软件；

Note

- 用手机进行通信时，手机中运行的是手机操作系统软件；
- 在 ATM 上取款时，ATM 中运行的是支持取款的一系列软件；
- 订飞机票时，也必须借助于飞机订票软件，等等。

对于普通用户来讲，这些软件的安全性可能还得不到完全的重视，或者不会有一个感性认识；一旦软件出现安全问题，用户也不能解决。对于用户来讲，这些安全问题的典型表现如下：

- 使用某些交易软件的过程中，某些敏感信息，如个人身份信息、个人卡号密码等信息被敌方获取并用于牟利；
- 访问某些网站时，服务器响应很慢，或者服务器由于访问量造成负载过大，造成突然瘫痪；
- 自己的系统中安装了具有漏洞的软件，漏洞没有解决，敌方找到漏洞并对本机进行攻击，造成系统瘫痪；
- 自己花费精力完成了一幅漂亮的风景画，放到网上去，没有考虑版权，被他人随意使用却无法问责，等等。

因此，这些安全问题应该在软件开发过程中就充分为用户考虑到。

在新的时期，对软件的开发提出了两个新的要求：加强软件复杂性和提高可扩展性要求。这两个要求促进了软件工程应用和研究的发展，但是也使软件安全变得更富有挑战性：

- 一方面，软件复杂了，安全问题也很复杂，无法得到全面的考虑，而工程进度又迫使开发者不得不在一定时间内交付产品，代码越多漏洞和缺陷也就越来越多；
- 另一方面，软件的可扩展性要求越来越高，系统升级和性能扩展成为很多软件必备的功能；可扩展性好的系统，由于其能够用较少的成本实现功能扩充，受到开发者和用户的欢迎；但针对可扩展性必须进行相应的设计，软件结构变得复杂。添加新的功能，也引入了新的风险。

怎样解决这些安全问题？

首先，大多数人可以想到的方法是软件测试，通过测试来减少软件中的缺陷。但是，由于软件系统规模越来越大，软件开发的进度要求越来越高，不可能在有限的时间内考虑所有安全方面的问题，即使进行了全方位的测试，也只能覆盖所有测试案例中的很小一部分。

如图 1-1 所示，模块 A 使用模块 B 和模块 C，以黑盒测试为例，如果模块 A 的输入有 X 种，模块 B 的输入有 Y 种，模块 C 的输入有 Z 种，理论上讲，应该对 $X \times Y \times Z$ 个组合进行全面的测试。但是，由于工程进度问题，实际上在测试时不可能兼顾全面，往往只是采用了一些具有代表性的测试案例来进行测试，但这些测试案例在设计的时候又不能保证具有最全面的代表性。如果想要将所有问题考虑到，除非进行穷举测试，而这种穷举测试基本上是不可能完成的。

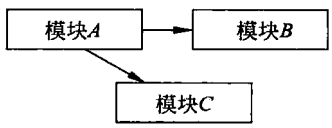

图 1-1

因此，软件测试无法完全保证软件的安全性。一方面是想要实现全面的测试，找出