上海市重点课程配套教材

重点大学信息安全专业规划系列教材

信息安全技术解析与开发实践

訾小超 薛质 姚立红 蒋兴浩 潘理 编著

李建华 主审

清华大学出版社

上海市重点课程配套教材

重点大学信息安全专业规划系列教材

信息安全技术解析与开发实践

訾小超 薛质 姚立红 蒋兴浩 潘理

编著

李建华

主审

清华大学出版社

北京

内 容 简 介

本书以信息安全技术开发实践为目标导向，围绕如何开发相应的信息安全原型系统编写，书中详细阐述了 Linux 内核级安全、网络防火墙、安全脆弱性检测，以及攻击检测这四类典型信息安全技术的实现解析和开发过程。本书分为上下两篇，上篇为技术解析篇，重点介绍这四类信息安全技术的基本概念和原理，并对进行相关信息安全技术开发实践所需要的关键方法和技术措施做了详细的探讨；下篇为开发实践篇，以实例方式阐述如何实现信息安全技术和原型系统的开发实践，本篇共十章，每章阐述一个信息安全相关原型系统的具体开发过程。

本书可作为高等院校信息安全、计算机科学与应用等专业的高年级本科生或研究生信息安全技术开发实践或课程设计的教材，也可作为相关信息安全技术原理类课程的参考书。本书以实例的形式展示了十几种操作系统和网络相关的常用开发技术，本书也适合从事相关软件开发的工程师和技术人员参阅。

图书在版编目(CIP)数据

信息安全技术解析与开发实践/訾小超等编著. —北京：清华大学出版社，2011.7
(重点大学信息安全专业规划系列教材)
ISBN 978-7-302-25568-0

Ⅰ. ①信…　Ⅱ. ①訾…　Ⅲ. ①信息系统—安全技术　Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2011)第 095066 号

责任编辑：魏江江
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　　**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 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：185×260　**印　张**：19.75　**字　数**：478 千字
版　　次：2011 年 7 月第 1 版　　**印　　次**：2011 年 7 月第1 次印刷
印　　数：1～3000
定　　价：29.50 元

产品编号：041773-01

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才。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。

重点大学信息安全专业规划系列教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

前　言

在信息安全专业的课程体系中，信息安全技术相关的开发实践是非常重要的环节。这类开发实践不仅能够培养学生的动手实践能力，激发对学习和钻研信息安全技术的兴趣和热情，还能在很大程度上加深对信息安全基本原理和技术的理解。

编者近年来负责上海交通大学信息安全专业软件课程设计的教学工作，该课程设计旨在通过进行相应的信息安全技术开发实践，来提高与信息安全相关的实践动手能力，从而加深对信息安全技术和相应信息安全工具的理解和掌握。在课程施教过程中，编者发现目前介绍信息安全原理和技术的书籍和教材很多，涉及信息安全技术和信息安全工具实现过程的书籍或教材却很少。难以找到一本合适的教材或参考书，指导学生顺利完成某类信息安全工具的开发，也不能在较短时间内搜集到进行信息安全技术开发实践所必备的知识。为了提高教学质量，帮助学生在较短时间内真正入手并顺利完成有关的信息安全技术开发实践，编者在综合多年科研及教学经验和成果的基础上撰写了本书，希望能够推动和促进国内信息安全专业在信息安全技术开发实践上的本科教育和课程建设。

信息安全是一门外延很广的学科，所涉及的信息安全技术众多。本书从中挑选出具有代表性且经常涉及到的四类信息安全技术进行实现解析和开发过程的探讨，这四类信息安全技术包括：Linux 内核级安全技术、网络防火墙技术、安全脆弱性检测技术、攻击检测技术。

本书分为上下两篇，上篇为“技术解析篇”，下篇为“开发实践篇”。“技术解析篇”重点介绍这四类信息安全技术的基本概念和原理，并对进行相关信息安全技术开发实践所需要的关键方法和技术措施进行详细的探讨。“技术解析篇”是本书进行相关信息安全技术开发实践的基础，该篇内容与其他介绍信息安全技术原理的书籍明显不同在于，本书以引导读者进行相应的信息安全技术开发实践为目标导向，围绕如何开发相应的信息安全原型系统编写。

“技术解析篇”共包含 7 章，第 1 章“Linux 内核级安全开发基础”和第 2 章“Linux 内核级安全机制实现解析”系统性地阐述进行 Linux 内核级安全机制开发的基本原理和技术基础。第 3 章“网络防火墙功能与结构解析”、第 4 章“网络防火墙的技术类型”及第 5 章“各类型防火墙实现解析”从原理、技术到实现全面阐述开发实现目前主要类型网络防火墙所需的各种知识。第 6 章“系统脆弱性检测技术及实现解析”对安全脆弱性检测的作用和技术分类进行了详细的介绍，重点分析两种典型的脆弱性检测技术（即

端口扫描技术和弱口令扫描技术)的原理及实现方法。第 7 章“入侵检测技术及实现解析”对入侵检测的主要技术和方法、入侵检测系统的工作原理和组成结构,以及入侵检测系统的实现技术进行详细的阐述。

“开发实践篇”以实例方式阐述如何实现信息安全技术和原型系统的开发实践,本篇共包含 10 章,每章阐述一个信息安全相关原型系统的具体开发过程。与“技术解析篇”对应,这 10 个开发实践分属于“技术解析篇”介绍的 4 类信息安全技术。“开发实践篇”中的第 8 章“基于 LSM 的文件访问控制原型实现”和第 9 章“基于系统调用重载的文件访问日志原型实现”属于 Linux 内核级安全机制开发类。第 10 章“内核模块包过滤防火墙的原型实现”、第 11 章“基于队列机制的应用层包过滤防火墙原型实现”、第 12 章“应用代理防火墙的原型实现”和第 13 章“透明代理防火墙的原型实现”属于网络防火墙开发类。第 14 章“端口扫描工具的原型实现”和第 15 章“弱口令扫描工具的原型实现”属于脆弱性检测技术开发类。第 16 章“基于特征串匹配的攻击检测系统原型实现”以及第 17 章“端口扫描检测系统的原型实现”则属于入侵检测系统开发类。本书中所有原型系统(或工具)的源代码均在 Linux 操作系统中调试通过,涉及到内核模块开发的原型系统对 Linux 内核版本有特定要求,在 Linux 系统的其他内核版本运行时需要进行相应的修改,对此有明确的说明。

为突出每种信息安全技术和原型系统实现的核心技术,“开发实践篇”中的每个开发实践过程都具有如下特点:①全部采用标准的 C 语言实现,不进行任何类库的封装,全面展示信息安全原型系统的底层核心实现技术;②开发实践中的源代码都经过针对性地提炼,尽可能精简读者比较熟悉且与核心技术关系不太密切的部分,如所有的原型系统全部采用最简单的命令行界面;③每个开发实践的 C 语言源代码控制在 200 行左右,同时配以详尽的注释,甚至包括函数间的调用关系图。

“开发实践篇”所实现的每个信息安全原型系统“刻意”包含最原始、最基本的安全功能,如对包过滤防火墙原型系统而言,只能支持一条包过滤规则,且该过滤规则只涉及源 IP 地址和目标 IP 地址。这一方面是因为本书旨在提高读者进行信息安全开发实践的动手能力,而不是向读者展示和提供一个功能完善的信息安全系统。另一方面,希望读者以本书的原型系统为基础进行相应的扩展开发实践,以切实提高自己的动手实践能力,为此本书特意对在原型系统上所能进行的后继扩展开发实践进行针对性阐述(见每章中的“扩展开发实践”部分),以引导读者在这些原型系统的基础上完成相应的扩展开发实践。

本书首要用途为信息安全技术开发实践或课程设计的教材,这也是作者撰写本书的初衷。任课教师可在讲解完原型系统的实现后,让学生在原型系统的基础上自行进行相关的扩展开发实践。因此本书在附录 A 中对所有的扩展开发实践题目进行了汇总,以方便任课教师组织学生选择他们感兴趣的扩展开发实践。本书也可作为信息安全原理和技术相关课程的参考书,通过研读本书中信息安全原型系统的实现技术及相关源代码,可加深学生对信息安全基本技术和原理的理解和掌握。

在阐述信息安全技术的具体开发实践过程中,本书以实例的形式向读者展示了十几种操作系统和网络相关的常用开发技术,因此本书也适合从事相关软件开发的工程师和技术人员参阅。这些开发技术主要包括 Linux 的内核模块开发、Linux 的字符设备驱动开发、Linux 安全模块(即 LSM)开发、Linux 的系统调用重载、基于 Netlink 通信的编程、基于 Netfilter 机制截获和控制 IP 报文、原始套接字编程、基于 Libpcap 的 IP 报文获取技术、基

于 Libnet 的底层协议报文组装技术、多线程编程技术、Web 代理服务器实现技术以及透明代理服务器实现技术等。

本书由訾小超主持编写和统稿，李建华教授主审。本书中的开发实践题目和章节结构由薛质教授精选及确定，訾小超负责完成第 1～5 章、第 8～13 章的编写，姚立红负责完成第 6～7 章、第 14～17 章的编写，薛质、蒋兴浩、潘理分别协助完成第 8～9 章、第 10～13 章及第 14～15 章的编写。蒋璐瑶、蔡汶楷、许可同学分别协助进行第 10～11 章、第 16 章、第 17 章的程序调试和材料整理。另外，夏业添同学参与了开发技术细节的程序验证工作。

本书编写过程得到上海交通大学信息安全工程学院领导和老师的大力支持，他们就本书的内容组织提出了很多宝贵的建议，在此深表感谢。本书的开发实践基本都源自于信息安全专业本科生的课程设计作业或科研创新项目，一些开发实践的源程序是在学生作业的基础上完善、修改而成。特别感谢修读软件课程设计的 05、06、07 级本科学生，以及参加编者指导的各类科研创新项目的同学。另外，个别原型系统的实现借鉴信息安全论坛一些开源软件的技术思路，在此一并致谢。

由于编者水平有限，再加上国内的信息安全开发实践课程和教材建设尚处于探索阶段，以及信息安全技术的快速发展，书中难免会存在一些错误和不足，恳请各位学者及读者批评指正，编者不胜感激。

编　者

2011 年 5 月

目　录

上篇　技术解析篇

下篇　开发实践篇