<<信息安全实验教程>>

图书基本信息

书名：<<信息安全实验教程>>

13位ISBN编号：9787121189722

10位ISBN编号：7121189720

出版时间：2013-1

出版时间：电子工业出版社

作者：周亚建

页数：231

字数：384000

前言

信息安全的重要性不言而喻。
随着电子政务、电子商务的进一步普及，政府、企业以及各种社会机构对信息安全专业人才的需求逐渐从数量向质量过渡，以适应日益复杂的网络应用环境。
高等院校作为人才培养的基地，有义务向国家和社会输送一批又一批既掌握扎实理论基础、又具有较强动手能力的高素质专业人才。
截至2009年，教育部共批准了70所高校设置信息安全类本科专业，其中的15所在2007年年底被教育部批准为“国家特色专业建设点”，从而能够把信息安全专业作为国家特色专业来建设。
但信息安全专业人才的培养绝非易事，原因在于信息安全涉及密码学、数学、计算机科学、通信工程和信息工程等多门学科的交叉，一方面知识体系庞杂、难于掌握，另一方面实践性很强。
在长期的教学实践过程中，多数学校基本上形成一种共识：合理、完善的实验课程体系是帮助学生掌握理论体系、培养动手能力的有效途径，并纷纷加大了对实验室建设的投入，加强了实验课程体系的建设。
于是，各种各样的实验教材如雨后春笋般地涌现出来。
毋庸置疑，每本教材都是对其编著者教学理念和教学经验的总结，反映了不同学校对人才培养的侧重点和不同诉求。
本书几位编著者所在的北京邮电大学信息安全中心承担着本校信息安全本科专业建设和教学的任务，并有幸入选教育部的“国家特色专业建设点”。
在多年信息安全实验教学过程中，几位编著者根据社会需求和学生特点的变化不断调整实验内容和实验教学方法，体会到实验教学的难点在于如何实现理论基础和动手操作的平衡：要么是学生的动手能力达不到用人单位的要求；要么是动手能力虽强，但只知其然、不知其所以然，缺乏创新能力。
学生在走上工作岗位之后遇到的问题不可能都在上学期间由老师讲授过，需要自己发挥主观能动性，开展创新性思维寻求解决方案。
要想具备这种能力，学生必须深刻理解各种信息安全技术和算法的基本原理，光靠“啃书本”不可能实现这一点，必须动手编程、调试程序和跟踪程序运行过程，才能了解每一种算法背后的真正机制。
基于上述考虑，本教程重新梳理了信息安全实验教学内容，结合源代码和详细的注释讲解算法（或技术）原理，引导学生深入到算法的实现过程中去理解其原理。
由于篇幅的限制，不可能对所有的技术、理论和算法均进行深入的剖析，只能选择一些典型的、影响较大的算法来分析，关键是对方法论的讲解。
这本质上是一种以点带面的方法：学生只要深入理解了书中所讲授的方法，同样能够举一反三，自己去研究、理解其他可能遇到的问题。
作为实现编著者教学理念的载体，本教程有以下几个鲜明的特色：　①把攻、防统一起来考虑问题。
信息安全问题往往涉及攻击和防御这样两个矛盾的对立面：攻击方考虑的是如何把自己的攻击之矛打磨得无坚不摧，防御方则竭力去铸造坚不可摧的盾。
本教程在讲解攻击的时候，引导学生思考防御之策；而在讲解防御的时候，也不得不思考攻击之法。
例如，对于古典密码算法和DES密码算法，不但要求学生掌握密码编码的算法，还要求他们能够编程实现密码分析的算法。
②结合源代码讲解原理。
以最经典的密码算法DES为例，按照算法的原理把从明文输入到密文输出之间的加密流程分解为一系列关键步骤，每一步的原理结合相应的C语言源代码（含详细的注释）予以讲解。
这样做的好处是，学生既理解了原理，又掌握了实现的方法。
一旦遇到不同的应用需求，只需对现有的代码做或多或少的修改即可。
③采用软件或者开源软件构件实验环境。
学生们朝气蓬勃、思维活跃，随时随地可能产生新的想法，实验为他们提供了验证自己想法的测试环境。

本教程涉及的实验仅依赖开源软件，甚至多数情况下要求学生自己编写程序，并不需要昂贵的设备作为支撑。
这实际上也是在训练学生掌握自己创造实验条件的方法和技巧。

本教材在编写过程中引用了来自互联网的一些原理描述、源代码及注释，目的是服务于教学，为学生提供更优秀、更便于理解的教学素材和资源，作为正式出版物的参考文献（书籍、学术论文及学位论文）在每一实验的最后都做了标注。

本教材的编写得到了所在灵创团队的老师和研究生们的大力支持和协助，在此一并致谢！
同时，由于编著者的水平有限，书中肯定存在这样或那样的问题，欢迎读者在使用过程中予以批评指正。

编著者　　2012年10月21日于北京

<<信息安全实验教程>>

内容概要

本书选择信息安全实验教学中最基本、最重要的内容作为切入点，深入到源代码层面讲解几种典型密码算法的原理，剖析各种信息安全技术实现的真实方式，旨在帮助读者深入探究算法与技术的原理，掌握运用所学知识解决各种具体问题的基本方法，提高其编程能力。
本书分为密码学实验和网络安全实验两大部分，密码学实验部分包括实验1到实验6，内容覆盖古典密码的加密与密码分析、DES算法的加／解密原理及其差分分析和公钥密码算法的加／解密及信息隐藏等内容；网络安全实验部分由实验7到实验14组成，主要涉及常见的网络攻击技术（扫描、口令破解和嗅探DoS/DDoS攻击等）内容。

<<信息安全实验教程>>

书籍目录

编辑推荐

周亚建、郑康锋、武斌、杨义先编著的《信息安全实验教程(通信网络精品图书)》重新梳理了信息安全实验教学内容，结合源代码和详细的注释讲解算法（或技术）原理，引导学生深入到算法的实现过程中去理解其原理。
以最经典的密码算法DES为例，按照算法的原理把从明文输入到密文输出之间的加密流程分解为一系列关键步骤，每一步的原理结合相应的C语言源代码（含详细的注释）予以讲解。
这样做的好处是，学生既理解了原理，又掌握了实现的方法。
一旦遇到不同的应用需求，只需对现有的代码做或多或少的修改即可。

<<信息安全实验教程>>

版权说明