**《信息安全基础》课程教学大纲**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 英文课程名 | Foundation of Information Security | | 总 学 时 | | 32 | 学 分 | 2 |
| 课程编码 | G126125 | | 理论教学学时 | | 24 | 适用专业 | 计算机科学与技术、软件工程、物联网工程 |
| 课程类别（请在课程所属类别栏注明选修或必修） | 通识课程 |  | 实践  教学  学时 | 实验学时 | 0 | 先修课程 | 计算机组成原理、数字电路与数字逻辑、  汇编语言程序设计 |
| 大类基础课程 |  | 上机学时 | 8 | 开课学院（部） | 计算机科学与技术学院、软件学院 |
| 专业课程 | 选修 | 其它 | 0 | 基层教学组织 | 计算机网络系列课程教学团队 |

**一、课程简介**

课程简介（正文：宋体、五号、行距：20磅，下同）：

《信息安全基础》课程是计算机科学与技术等相关专业的一门专业选修课，为学生职业素养养成和职业能力培养起着主要支撑作用。本课程从信息安全管理、信息安全技术和信息安全法律法规三个方面培养学生的职业道德和职业技能。引入大量案例和故事，帮助学生全面、清晰了解信息及信息安全概念；课程内容涉及信息安全领域的基本概念、基础理论和主要技术，并对信息安全管理和信息安全标准进行了简要的介绍，应用领域涉及网络安全领域中的信息获取、存储、传输和信息处理领域中的信息安全保障等问题，属于计算机领域的交叉内容。

**二、教学目标**

**2.1 课程教学目标**

本课程的授课对象为计算机学院计算机科学与技术、软件工程以及物联网工程等专业的本科生；通过学习，使学生了解信息安全领域的知识体系，掌握关键的安全技术和安全机制，熟悉信息保密技术、信息认证技术、信息隐藏技术、操作系统与数据库安全、访问控制技术、网络安全技术、信息安全管理、信息安全标准与法律法规等密码技术、防火墙、软件安全、操作系统安全等，并具有在应用领域和应用系统中予以实施的基本实践技能。学生通过课程教学和实验操作，可以加强实践能力、文档协作能力、汇报演讲能力等，培养信息安全视角的社会责任感、通过小组作业提升团队协作意识、面向实际需求的创新实验设计能力等。

**2.2 课程目标与毕业要求（指标点）对应关系**

【毕业要求1】工程知识：能够将数学、自然科学、工程基础和专业知识用于解决计算机安全领域的复杂工程问题。

【毕业要求2】问题分析：能够应用数学、自然科学和计算机工程科学的基本原理，识别、表达、并通过文献研究分析复杂计算机安全工程问题。

**三、课程教学内容及学时分配**

**1．理论教学安排**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 章节或知识点(模块) | 教学内容 | 学时分配 | 教学要求  (应明确教学重点、难点和教学方法) | 学生任务 | |
| 作业要求 | 其他要求(自学/讨论） |
| 1 | 绪论 | 信息安全含义、信息安全典型应用 | 2 | 通过剖析典型安全案例使学生从安全视角理解计算机计算机网络以及系统应用等，重点理解密码学发展过程。 | 分析当前网络安全现状 | 对网络安全现状进行调研 |
| 2 | 密码学基础 | 经典加密技术、分组加密、流密码、公开密钥加密、哈希函数 | 6 | 通过理论讲解、方案分析以及应用举例等手段培养学生古典密码学的分析能力、现代密码技术的运用能力。教学重点在古典密码技术和现代密码技术思想的融合及演化，难点在密码学的思想及其处理方式的理解。 | 课外自主分组进行密码学讨论 | 理解选题含义，准备实验选题 |
| 3 | 访问控制 | 口令认证、生物特征认证、双因素认证、授权、安全模型、防火墙、入侵检测 | 6 | 通过理论讲解、实践测试和典型案例分析使得学生理解典型的认证技术及不同应用场景、对防火墙、入侵检测等常规防御技术有较深入的理解和掌握，重难点在于认证技术和相关安全模型的工作机制及其想过分析。 | 设计相关访问控制方案，完成个人基础实验 | 自学典型攻防工具操作 |
| 4 | 安全协议 | 认证协议、会话协议、SSL/IPSec协议、Kerberos协议、WEP协议、GSM等 | 6 | 通过理论讲解和实验实践使学生理解并掌握安全协议应用开发能力，重点在于安全协议的工作机制，难点在于安全协议效果的分析。 | 完成小组综合实验；提交个人基础实验报告 | 自学基于不同环境的认证协议开发技术 |
| 5 | 软件安全 | 病毒与恶意软件、逆向工程、版权保护管理、OS安全 | 2 | 通过讲解及典型案例分析使得学生理解病毒与恶意软件及逆向工程初级实践的过程 | 小组综合实验报告 | 分析病毒原理及查杀机制 |
| 6 | 信息安全标准与法律法规 | 国际、国内安全标准、相关国家标准目录、信息安全法律法规 | 2 | 通过对安全法律、标准的讲解、分析使得学生了解信息安全标准和文档的制定 | 尝试制定信息安全标准 | 熟悉信息安全相关法律法规 |

2．实践教学安排

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 学时 | 类型 | 每组人数 | 教学要求  (应明确教学重点、难点和教学方法) | 学生任务 | |
| 作业要求 | 其他要求(自学/讨论） |
| 1 | 基于工具的攻防基础实验（如网络扫描、嗅探、DOS攻击、信息隐藏、口令破译、加解密等） | 4 | 设计、操作 | 3 | 每组自愿选择2个实验、完成实验的设计和操作过程，并提交实验报告，重点是各工具的使用，难点在于理解相关软件安全防御功能实现机制 | 实现相关方案 | 编程、测试 |
| 2 | 小组综合实验及汇报  （读书报告、BCP计划、攻防综合实验及开发等） | 4 | 设计、编程等 | 3 | 各组在期末前课外自学为主、结合教师指导完成小组综合实验，期末前课内进行PPT演讲，并提交报告和展示材料 | 实现相关方案 | 编程、测试 |

**四、考核方式及成绩评定方式**

考核方式：考查

成绩评定：期末成绩=平时成绩50%（平时作业15%+个人实验报告15%+小组实验汇报20%）+期末报告50%

**五、教材、课程网址及参考书目**

教 材： 信息安全原理与实践，斯坦普著，张戈译，清华大学出版社，2013年6月，第二版

参考书：【1】信息安全工程，Ross Anderson著，齐宁、韩智文、刘国萍译，清华出版社，2012年1月，第二版

【2】信息安全概论，张雪锋，人民邮电出版社，2014年3月，第一版

**执笔者：程宏兵**

**审核者：**

**课程教学团队成员：**