# 《网络安全与保密》课程教学大纲

**一、课程概述**

|  |  |  |  |
| --- | --- | --- | --- |
| **课程名称** | 网络安全与保密 | **英文名称** | Network Security and Confidentiality |
| **课程性质** | 专业选修课 | **课程代码** | 22122031 |
| **总学时** | 40  理论32学时+实验8学时 | **学分** | 2 |
| **开课学期** | 第六学期 | **先修课程** | 计算机网络 |
| **适用专业** | 通信工程 | **开课单位** | 计算机与电气工程学院 |

**二、课程简介**

网络的普及使非法访问和恶意进入很难控制，从而造成计算机信息资源被篡改、被盗窃和被破坏。利用计算机程序的可复制性和非法读写功能，制造出的各种各样计算机病毒，使全世界成千上万的计算机用户胆战心惊。因此，十分有必要在大学通信工程专业中开设计算机安全与技术这样一门课程，以提高学生在计算机实体与信息安全领域的防范意识和相关的技术水平。

**三、课程目标**

课程目标1：使学生了解网络安全与保密技术的发展过程；掌握网络安全和保密的一般方法和特点，理解安全和保密的基本概念、主要功能和实现安全和保密的基本思想，能够根据实际需要进行计算机安全保密工作，并为今后进一步从事使用各种手段分析、设计、检测网络安全与保密的工作打下基础。。

课程目标2：使学生掌握信息安全及其防范技术的基本方法，学生能自觉运用安全管理的技术与规范；使学生了解信息安全的标准和法律法规，自觉维护信息系统的安全。

课程目标3：学生通过学习该课程后能够运用网络安全与保密技术，针对不同环境与场合，能够制定适当的网络安全解决方案。

课程目标4：使学生掌握信息安全的知识，并为学生进一步从事信息安全工作，做好知识准备。

**四、课程目标对毕业要求指标点的支撑**

**表4-1 课程目标对毕业要求指标点的支撑**

| **毕业要求** | **毕业要求指标点** | **课程目标** | | | |
| --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** |
| **1 应用工程知识** | 1.1（工程问题描述）能将数理工程科学语言工具用于通信工程复杂工程问题的表达。 | H |  |  |  |
| **4 研究工程问题** | 4.4（分析数据 ）能运用恰当的工具，根据通信系统与信息工程领域问题中的具体对象特征对数据进行合理分析。 |  | H |  |  |
| **6工程与社会** | 6.1 （掌握行业规则）知晓通信与信息工程领域的技术标准体系、知识产权、产业政策和法律法规，理解不同社会文化对工程活动的影响。 |  |  | H |  |
| **8恪守职业规范** | 8.2（ 工程素养）理解工程伦理与职业道德的意义，并能在工程实践中自觉遵守。 |  |  |  | H |

注：分别用“H、M、L”对应表示“高、中、低”支撑。

**五、教学内容、进度和实施手段**

**表5-1教学内容与进度要求**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **章节** | **小节内容** | **要求** | **具体要求** | **学生成果** | **课程目标** | **学时** |
| 第一章网络安全概述 | 1、网络拓扑与安全性 | 认知 | 总线网、局域网、网状网、星状网。 | 查找文献做出关于网络安全的概述报告。 | 1 | 2 |
| 2、网络安全的层次结构与基本安全技术 | 认知 | 物理服务、安全服务、加密、身份验证。 | 能理清几种不同的概念。 | 1 | 2 |
| 第二章 数据加密 | 1、密码学基础 | 理解 | 密钥加／解密系统模型 、古典密码。 | 使用密钥／解密系统模型 、古典密码。 | 1 | 2 |
| 2、数据加密标准 | 综合 | DES算法的描述、三重DES。 | DES算法的描述。 | 1 | 2 |
| 第三章 单向散列函数 | 1、MD5算法 | 理解 | MD5算法与举例 | 领会原理与举例 | 2 | 2 |
| 2、安全散列函数（SHA） | 理解 | SHA算法与举例 | 领会原理与举例 | 2 | 2 |
| 3.3 消息认码（MAC） | 理解 | MAC编码 | 能理解MAC | 2 | 3 |
| 第四章 公钥密码系统 | 1、Diffie-Hellman密钥交换 | 理解 | （1）Diffie-Hellman算法 （2）中间人攻击 （3）认证的Diffie-Hellman密钥交换 ⑷三方或多方Diffie-Hellman。 | 能进行三方或多方Diffie-Hellman | 2 | 2 |
| 2、数字签名 | 理解 | 数字签名算法、RSA签名方案。 | 掌握数字签名算法、RSA签名方案 | 2 | 2 |
| 第五章  因特网与TCP／IP安全 | 1、TCP协议 | 理解 | （1）端口号 （2）TCP安全缺陷 （3）IP欺骗攻击 （4）TCP状态转移图（5）网络攻击签名检测 | 掌握TCP协议的特征与缺陷 | 2 | 3 |
| 2、网络服务的安全性 | 理解 | 远程登录、文件传输协议、域名系统（DNS）。 | 掌握远程登录方式、文件传输协议、域名系统（DNS） | 3 | 3 |
| 第六章  VPN与IPSec | 1、VPN数据安全性 | 理解 | 认证、加密、完整性 | 掌握VPN认证、加密、完整性 | 3 | 3 |
| 2、VPN协议 | 知晓 | PPTP、L2TP、 IPSec | 知晓PPTP、L2TP、 IPSec | 3 | 2 |
| 3、IPSec协议 | 理解 | 安全关联、SA参数、安全策略、选择符、IPSec模式 | 理解SA参数、安全策略 | 3 | 2 |

**表5-2 实验教学内容与进度要求**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序**  **号** | **实验名称** | **实验内容与方法** | **实验**  **要求** | **实验**  **类型** | **实验**  **学时** | **课程目标** |
| 1 | 数据加密技术 | 凯撒密码实现、维吉尼亚表加密、DES。 | 必做 | 验证 | 2 | 4 |
| 2 | 计算机容错存储实现 | 学习使用Wireshark抓取发送邮件的包。 | 必做 | 设计 | 2 | 4 |
| 3 | PGP加密软件文的使用 | 对E-MAIL进行加密和数字签名对E-MAIL进行解密和验证。 | 必做 | 设计 | 2 | 4 |
| 4 | 路由器模拟防火墙实验 | 配置路由器使用路由器的功能模拟防火墙的包过滤。 | 必做 | 设计 | 2 | 4 |

**六、课程思政**

**表6-1 课程思政内容**

|  |  |
| --- | --- |
| **课程思政教学内容** | ①诚信：认真付出，努力做事，坚持科学观和实事求是精神。 |
| ②友善：保持平和、宽容的心去对人做事，团结协作，尊长爱幼。 |
| ③爱岗：富有不断学习和探索进取的工作态度，热爱本专业。 |
| ④敬业：做事可以吃苦耐劳，工作能够精益求精。 |
| ⑤其它：科学发展观及积极向上的人生观。 |

**表6-2 课程思政具体案例**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **所属章节/**  **案例名称** | **案例教学目标** | **思政元素** |
| 1 | 第2章第2讲  DES算法实现 | 通过DES算法实现，掌握一种数字加密手段。 | 诚信、爱岗：布置学习任务，要求学生诚实守信完成；培养学生对数字加密的兴趣和爱好，鼓励学生在该领域探索进取，热爱本专业。 |
| 2 | 第3章第3讲  三方Diffie-Hellman密钥交换 | 通过演示三方Diffie-Hellman密钥交换过程，掌握三方Diffie-Hellman密钥交换方法。 | 友善、敬业：通过三方Diffie-Hellman密钥的讲解，培养学生友爱、宽容的心；让学生工程中领会并形成精益求精的态度。 |
| 3 | 第3章第4讲  RSA签名 | 通过举例RSA签名认证，了解网络安全数字签名机制，实现对安全防范。 | 友善、爱岗：通过RSA让学生领会团结协作、友善爱岗的精神。 |
| 4 | 第4章第2讲  IP欺骗攻击 | 演示发起IP欺骗攻击，介绍防御手段，应对措施。 | 科学发展观：培养学生考虑工程与环境因素：通过发动欺骗攻击，让学生清楚IP攻击的特征，能够针对性防范，并意识到网络加密安全的必要性。 |

注：课程思政案例每门课程根据课程内容实际情况加设，每门课程至少3-6个。

**七、考核及成绩评定**

1、考核方法

本课程考核采用平时成绩+实验成绩+期末考试的综合考核方式，即：

**总成绩=平时成绩\*27%+实验成绩\*13%+期末考试成绩\*60%**

**表7-1 考核环节及权重表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **项目名称**    **课程目标** | **考核环节及成绩占比（%）** | | | | | **课程目标权重**  **（%）** |
| **课堂**  **测试**  **（1）** | **课后**  **作业**  **（2）** | **课程**  **调研**  **（3）** | **实验**  **成绩**  **（4）** | **期末**  **成绩**  **（5）** |
| 课程目标1 | 3 | 3 | 3 | 2- | 18 | 29 |
| 课程目标2 | 5 | 3 | 1 | 4 | 16 | 29 |
| 课程目标3 | 4 | 1 | 3 | 4 | 10 | 22 |
| 课程目标4 | 5 | 3 | 3 | 3 | 16 | 30 |
| 合计 | 17 | 10 | 10 | 13 | 50 | 100 |

2、考核内容及评价标准

① 实验成绩：占总成绩的10%。分为4次实验；每次评分施行百分制，评分内容包括实际操作和实验报告，评分标准如表7-2所示。

**表7-2 实验考核方案及评价标准**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **课程目标** | **考核内容** | **优秀** | **良好** | **中等** | **及格** | **不及格** |
| 课程目标3 | 数据加密技术 | 实验操作步骤熟练正确，实验报告完整详实。 | 实验操作步骤较正确、实验报告较完整较详实。 | 实验操作步骤基本正确、实验报告较完整 | 实验操作步骤不够正确，实验报告不够完整 | 不做实验、不交实验报告 |
| 计算机容错存储实现 |
| PGP加密软件文的使用 |
| 路由器模拟防火墙实验 |

② 期末考试：占总成绩60%。开卷考试，考试时间120分钟，成绩采用百分制，卷面成绩总分100分，考试范围包括1,2,3,4课程目标。具体考试时间与教务办公室联系协商通知进行。

**表7-3作业评价标准**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **考核内容** | **优秀（90-100分）** | **良好（80-89分）** | **中等（70-79分）** | **及格（60-69分）** | **不及格**  **（60分以下）** |
| 作业 | 按时足量提交，90%以上的概念与计算正确，方案合理，书写清晰且文本规范。 | 按时足量提交，80%以上的概念与计算正确，方案较合理，书写比较清晰、规范。 | 缺量提交，70%以上的概念与计算正确，方案基本合理，书写基本清晰、规范。 | 补交，60%以上的概念与计算正确，方案不够合理，书写不够清晰、规范。 | 提交作业错误过多，书写混乱潦草。（不交作业、抄袭记零分）。 |

③ 课堂测试：占总成绩的17%。每次课程结束后通过雨课堂进行线上小测试。同时结合随机课间考勤和互动，每名学生不少于5次，每缺一次扣2%，扣完17%为止，无故缺勤5次以上者取消本门课程的考核资格。

④ 课后作业：占总成绩的10%。本门课程每章均布置作业，布置次数不低于4次，每次作业的占比均分，根据学生作业是否按时上交、是否独立完成以及作业完成准确性与可读性评分。作业具体评分标准如表7-3所示。

⑤ 课程报告：报告主题由任课老师针对课程目标根据教学内容与实践应用的热点和难点进行拟定布置。

3、按照工程教育认证标准和学校人才培养要求，考核以学生能力是否有效达成为基准。为保障学生课程培养能力的达成，规定期末考试卷面成绩应高于一定分数。

4、考核周期为一个学年。为使评价结果尽快反馈给各个教学环节，促使各个教学环节尽快改进，保证教学效果的快速提升，课程考核成绩评价每学年进行1次。

5、考核依据《计算机与电气工程学院课程目标达成评价实施办法》文件进行。

**八、课程质量评价和持续改进**

课程结束后由课程责任人以定量和定性评价方法，针对具体课程目标形成文字或图表形式的报告，针对学生个体和整体的学习成果评价并对相关问题进行分析；课程目标达成与课程在培养学生解决复杂工程问题能力的具体环节任务的达成相关性分析；对以上各薄弱环节进行原因分析，提供持续改进建议，并由学院教学指导委员会进行审核。针对学生个体和整体的课程目标评价方法如下：

1、课程考核成绩算分评价法：

课程目标达成度算分评价法是以参加课程学习的所有学生获得课程成绩为样本，对支撑毕业要求中各个指标点对应的课程目标进行达成情况评价，要由任课教师、课程负责人进行评价。

课程目标达成情况评价值计算按下面公式进行：

课程目标达成评价值 



上式中k是该课程目标评价环节数，评价环节有平时过程考核、课后作业、大作业、实验、期末考试等（具体的依据考核审核表确定）; z𝑖 是第𝑖个评价方式的总分值，𝐷𝑖 是为学生在第𝑖个评价方式上的得分，𝑃𝑖 是第𝑖个评价方式在该课程目标评价中的占比。

2、针对学生课程目标未达成者，通过优秀学生与其沟通交流及任课教师进一步专题辅导改进；整体达成度较差部分，任课教师通过抽查与学生交流、分析问题，作进一步教学内容及方法的改善。

**九、教材与主要参考资料**

**1. 教材：**刘建伟主编，《网络安全技术与实践》，清华大学出版社，2017.1

**2. 教学参考书目：**

[1] 施峰主编，《信息安全保密基础教程》，北京理工大学出版社，2019.6

[2] 葛秀慧[等](http://www.china-pub.com/search/power_search/power_search.asp?key1=%d6%a7%b3%a4%d2%e5+%b3%cc%d6%be%c6%bd+%b3%c2%ca%e9%c1%a2+%c1%f5%cf%fe%c0%bc)编，《计算机网络安全管理》，清华大学出版社，2018.8

[3] 卢开澄等编，《计算机密码学》，清华大学出版社，2018.4

**十、教学团队**

|  |  |  |
| --- | --- | --- |
| **姓名** | **职称** | **承担的教学工作** |
| 杨峰 | 讲师 | 课程负责人、主讲教师 |
| 朱明旱 | 副教授 | 主讲教师 |
| 谭明涛 | 副教授 | 主讲教师 |
| 黄建春 | 副教授 | 主讲教师 |

执笔人：杨峰

系（室）审核机构：通信工程教学大纲审核小组

组长：邵湘怡

审核执行人（签字） 王立 2022年11月15日

教学院审核机构：计电学院教学大纲审核小组

组长：李建英

审核执行人（签字）: 孙树亮 2022年12月30日