《网络安全程序设计》课程教学大纲

一、课程名称（中英文）

中文名称：网络安全程序设计

英文名称：Network Security Programming

二、课程代码及性质

专业方向课　选修

三、学时与学分

总学时：32（理论学时：24 学时；实践学时：8 学时）

学　分：2

四、先修课程

C 语言程序设计，计算机通信与网络，计算机网络安全，密码学基础

五、授课对象

本课程面向信息安全专业|网络空间安全专业学生开设

六、课程教学目的

1、 通过课程学习，使学生以 Linux 操作系统为对象，从整体上认识网络通信从应用层 API 到内核协议栈的层次结构、工作原理和运行机制，了解网络通信面临的安全威胁，建立网络安全程序设计的思想；(K1)

2、 通过实践，让学生了解主要的网络安全程序设计技术及解决安全威胁的技术思路，使学生能够将安全理论应用于实践，培养相应的程序设计能力，提升工程实践能力；(K2)

3、 通过课堂讲授与课外文献检索阅读，使学生了解与本课程相关的计算机领域的前沿发展；(K3)

4、 通过规范化的文献阅读报告以及课外实践报告，培养学生良好的文档习惯以及撰写规范文档的能力。(K4)

表 1 对毕业要求的支撑关系

毕业要求及其指标点	本 K 对毕业要

毕业要求	指标点	求的支撑关系
毕业要求 1：人文素质与社会责任	1.1 掌握马列主义、毛泽东思想与中国特色社会主义基本理论	
	1.2 掌握基本的人文社会科学知识	
	1.3 具有健全的人格，身心健康	
	1.4 具有社会责任感	
毕业要求 2：数理基础、自然科学、工程知识	2.1 掌握本学科所需的数学理基础、自然科学和工程知识	
	2.2 能应用数学、物理及自然科学知识描述本学科复杂工程问题	
	2.3 能从数学、物理及自然科学的角度对本学科的复杂工程问题进行分析	
	2.4 能理解工程活动中涉及的经济与管理因素	
毕业要求 3：掌握计算机科学与技术学科基本理论和专业知识，具有一定的系统能力	3.1 理解计算机软/硬件系统的基本架构与工作原理	K1、
	3.2 掌握程序设计的基本方法、算法设计与分析的基本方法	K2
	3.3 熟悉一种硬件开发工具，掌握硬件系统开发的基本方法和技术	
	3.4 具有软件与硬件协同的系统能力	
毕业要求 4：分析本学科复杂工程问题的能力	4.1 能综合应用数学物理知识、自然科学知识、工程知识，发现、识别、表达本学科的复杂工程问题	
	4.2 能综合应用数学物理知识、自然科学知识、工程知识，并通过文献分析和研究，对本学科的复杂工程问题进行建模、分析，并得出有效结论	K1
	4.3 能综合应用数学物理知识、自然科学知识、工程知识，并通过文献分析和研究，对本学科的复杂工程问题提出解决问题的思路	K2
毕业要求 5：复杂工程问题设计/开发解决方案	5.1 熟悉需求分析、设计、实现、评审、测试、维护以及过程与管理的方法和技术	
	5.2 了解计算机科学与技术工程问题特征，掌握解决本学科复杂工程问题的基本方法	
	5.3 具备选择合适的开发工具，设计（开发）满足特定功能要求的软/硬件系统、单元（部件）或工艺流程的能力	K2
	5.4 在考虑法律、健康、安全、文化、社会以及环境等制约因素的前提下，能够设计（开发）针对复杂硬件系统、软件系统或应用系统的解决方案	K2
毕业要求 6：调查研究能力	6.1 熟悉本学科复杂工程问题的调查研究方法	K2
	6.2 能正确选择工具，采用科学方法和本学科的专业知识，对本学科的复杂工程问题设计研究方案	**K2**
	6.3 能正确使用和处理实验或研究数据，通过信息综合处理，对本学科的复杂工程问题进行预测或提出优化方案	
毕业要求 7：具有良好的	7.1 了解与信息产业相关的政策和法律法规	

毕业要求及其指标点		本K对毕业要求的支撑关系
毕业要求	指标点	
工程素质与职业道德	7.2 正确认识信息化工程对于客观世界和社会的影响；理解用技术手段降低其负面影响的作用与局限性	
	7.3 在工程实践中，理解工程师的职业性质、职业责任,具备工程师的职业道德	K2
毕业要求 8： 组织管理能力与团队协作精神	8.1 能够通过口头或书面方式表达自己的想法并与相关人员沟通	
	8.2 能够理解多学科团队中各角色的划分及其作用，具有组织管理能力	
	8.3 能够在多学科团队中做好自己所承担的角色，具有良好的团队合作意识	
	8.4 具备良好的团队协作精神，善于和团队其它成员协作、互补、交往	K2
毕业要求 9：具有较强的交流与沟通能力	9.1 较好地掌握了一门外语，了解不同文化的差异，具有一定的跨文化交流能力	
	9.2 了解本专业领域及其相关行业的国内外的技术现状，具有较强的业务沟通能力	K3
	9.3 能够就复杂工程问题与业界同行及社会公众通过撰写报告、设计文稿、陈述发言等方式进行有效沟通与交流	K4
毕业要求 10：终身学习意识与能力	10.1 对终身学习的重要性，有自觉的意识和正确的认识	
	10.2 能够采用合适的方法，自我学习、提高的能力	
	10.3 能运用现代化教育手段学习新技术、新知识	K3

七、教学重点与难点：

课程重点：

1. 网络安全威胁
2. 网络安全技术
3. TCP socket 通信程序设计方法；
4. 通信加密机制及应用；
5. raw socket 原理及使用；
6. openssl 原理及使用；
7. Linux 网络协议栈；
8. netfilter 框架原理及使用；

课程难点：

1. 通信加密中的密钥分发和管理机制的演进；

2. socket 通信的并行机制和异步机制；
3. 网络报文的封装与解析；
4. ssl 协商的双向认证；
5. Linux 网络协议栈中报文发送和接收流程；
6. netfilter 在协议栈中 HOOK 点的作用。

八、教学方法与手段：

本课程偏重于实践，教学过程中将主要采取原理讲解、实例解读、效果演示等方法，充分调动学生的学习积极性，实施课内和课外相结合的学习方式，体现研究性学习，提高学习效果。同时结合网络安全发展，开展文献阅读与讨论，让学生了解相关的前沿发展趋势。主要的教学环节包括课堂授课、课堂讨论、课程项目、项目报告等环节。

本课程的教学适当的贯穿 PBL 方法，以项目开发的形式，从网络通信面临的安全问题出发，设定问题场景，提出安全解决方案，进而介绍相关程序开发技术，通过程序流程图、源代码的讲解和程序的运行演示，使学生对所介绍的安全程序设计技术有感性认识。本课程还采用逐步深入的方式，对已经完成的项目，通过设问，进一步分析其在安全性上存在不足，从而提出改进方案，形成一个新的项目，进一步引入更深一层的技术，力争提高学生的兴趣，使其能在思维上主动参与问题的分析和解决的过程，提高学习的效果。

九、教学内容与学时安排

(一) 概述

本章的主要知识点包括网络安全技术的特点；网络安全形势的演变；网络安全技术研究的基本内容。

本章课堂教学学时 2 学时，建议学生课后学习 2 学时。

(二) 加密聊天程序

本章的主要知识点包括基本网络通信程序、对称密钥加密的实现及缺点、RSA 安全性、其他公钥密码体系、RSA 与对称密钥算法结合、使用 Select 机制进行并行通信、使用异步 I/O 进行通信优化等。

本章课堂教学学时 6 学时，建议学生课后学习 8 学时。

(三) 基于 Raw Socket 的网络嗅探器程序

本章的主要知识点包括原始套接字、TCP/IP 网络协议栈结构、数据的封装与解析、使用 libpcap 捕获数据报、使用 tcpdump 捕获数据报。

本章课堂教学学时 4 学时，建议学生课后学习 4 学时。

(四) 基于 OpenSSL 的安全 Web 服务器程序

本章的主要知识点包括 SSL 协议介绍、OpenSSL 库、相关数据结构分析、客户端证书校验的实现、基于 IPSec 的安全通信分析等。

本章课堂教学学时 2 学时，建议学生课后学习 4 学时。

(五) Linux 网络协议栈简介

本章的主要知识点包括 Linux 网络协议栈概述、Linux 网络协议栈中报文发送和接收流程。

本章课堂教学学时 4 学时，建议学生课后学习 8 学时。

(六) 基于 Netfilter 防火墙的设计与实现

本章的主要知识点包括防火墙相关知识介绍、Netfilter、IPTables、Netfilter 内核模块扩充、iptables 命令及参数详解、设计防火墙等。

本章课堂教学学时 4 学时，建议学生课后学习 8 学时。

(七) Linux 内核网络协议栈加固

本章的主要知识点包括拒绝服务式攻击、Linux 内核网络协议栈相关代码分析、其他拒绝服务式攻击方式的讨论、基于 TCP SYN Cookie 的 SYN Flood 防御策略等。

本章课堂教学学时 2 学时，建议学生课后学习 4 学时。

十、实验内容与学时安排

(一) 选题一：基于 OpenSSL 的安全聊天系统

实验内容	在 Windows 或 Linux 平台下设计实现一套聊天软件，采取点到点模式，基于 OpenSSL 实现加密的安全套接字通信，启用客户端服务器双向认证，对聊天记录本地加密存储，输入正确口令可查看。
实验类型	综合性、设计型实验
实验目的与要求	(1)掌握基本的客户端与服务器的套接字通信编程方法； (2)掌握 OpenSSL 安全套接字通信编程方法； (3)理解公钥密钥算法与对称密钥算法在通信过程中的作用； (4)掌握基本的文件加密保护方法；
实验形式	(1)独立完成。 (2)课内 8 学时，课内检查，其余为课外学时。
实验考核	(1)现场验收并对实验内容进行提问。

	(2)根据设计方案、实验结果、附加功能、操作熟练程度、现场检查和回答情况及实验报告质量综合评定成绩。

(二) 选题二：基于 Netfilter 的网络嗅探器

实验内容	在 Linux 平台下设计实现一套网络嗅探器程序，使用内核模块通过 Netfilter 机制截获网络报文，支持过滤器设置，包括 IP 地址、协议、端口参数，过滤器通过一定技术写入内核模块生效，符合过滤器条件的报文复制后通过一定技术传递给应用层进程，应用层进程进行协议分析并显示分析结果。
实验类型	综合性、设计型实验
实验目的与要求	(1)掌握 Linux 内核模块编程方法； (2)掌握 Netfilter 机制截获报文技术； (3)掌握 Linux 用户空间与内核空间通信技术； (4)了解常见的网络协议报文格式；
实验形式	(1)独立完成。 (2)课内 8 学时，课内检查，其余为课外学时。
实验考核	(1)现场验收并对实验内容进行提问。 (2)根据设计方案、实验结果、附加功能、操作熟练程度、现场检查和回答情况及实验报告质量综合评定成绩。

教学参考书及文献

教学参考书：

1. 网络安全高级软件编程技术．吴功宜．清华大学出版社，2010
2. 网络安全编程技术与实例．刘文涛．机械工业出版社，2008
3. 网络安全编程与实践．陈卓，阮鸥，沈剑．国防工业出版社，2008
4. （美）Jonathan Corbet,Alessandro Rubini, Greg Kroah-Hartman．Linux 设备驱动程序（第三版）．魏永明，耿岳，钟书毅译．中国电力出版社，2006

课外文献阅读 (动态更新)：

1.

十一、课程成绩评定与记载

课程成绩=课堂考勤（10%）+课堂讨论（10%）+终结性考试（80%）

终结性考试形式：报告

大纲制定：《网络安全程序设计》课程组

审核：网络空间安全学院教学指导委员会