复旦大学研究生课程教学大纲

课程名称/Course Title:　网络和计算机安全

课程代码/Course Code:　SOFT620009

任课教师/Instructor(s):　曾剑平

开课院系/School/Department:　201 软件学院

1.课程概要/Course Summary

课程名称（中文 Course Title (Chinese)	网络和计算机安全		
课程名称（英文) Course Title (English)	Network and Computer Security		
课程代码 Course Code	SOFT620009	任课教师 Instructor(s)	曾剑平
开课院系 School/Department	201 软件学院	开课学期 semester	2023-2024学年 第一学期
授课语言 Teaching Language	中文	适用学科专业 Discipline/ Specialization	
学分数 Course Credit(s)	3	教学周数 Weeks	共16周
总学时 Teaching Hours in Total	共54学时	实验/实践学时 Hours for Experiments/ Practice	共0学时
预修课程要求 Pre-requisite Course(s)	高等数学、离散数学		
课程简介 Course Introduction	本课程主要基于网络安全、大数据与AI安全的密切联系，讲述相关原理、模型、方法与实现技术。课程内容包括网络典型结构和常见协议及漏洞、新型网络结构及安全挑战、大数据与AI安全技术体系、AI安全的共性数据处理方法、对抗样本理论与方法以及典型的大数据AI安全技术，如入侵检测\异常检测、口令大数据安全、大数据隐私安全、聚类算法的攻击与风险等。		

2.教学目标/Course Objective

理解大数据安全、网络安全和AI安全技术之间的联系;掌握网络安全解决思路和防御方法；掌握大数据技术用于解决传统安全的思路和方法;理解并掌握大数据驱动的机器学习模型算法所存在的安全问题、攻击方法、防御方法;理解大数据隐私安全及保护方法;掌握大数据AI安全中数据处理的三个共性方法。

3.教学内容及进度安排/Course Content & Schedule

课次/模块	教学周	教学内容及预期效果	作业/练习
1	1	网络安全概述	
	3	新型网络结构及安全挑战1	
	2	典型网络结构和常见协议漏洞	
	4	新型网络结构及安全挑战2	

1	5	新型网络结构及安全挑战3（文献汇报交流1）	
2	6	大数据与AI安全概述	
	7	AI安全的共性数据处理方法	
	8	入侵检测\异常检测技术	
	9	对抗样本攻击的理论与方法	
	11	大数据隐私安全	
	12	聚类算法的攻击与风险	
	10	口令安全的大数据方法	
	13	大数据与AI安全技术交流	
3	17	考试周	

4.课程考核及成绩评定/Course Assessment & Grading

考核形式 Assessment Criteria	权重 Percentage	评定标准 Assessment Standard
出勤/Attendance	10	考勤记录
课堂表现/Participation		
作业/实验/实践/ Assignment(s)	20	课程报告与交流情况
课程论文/Course Paper	70	论文的工作量、创新性和规范性等
开卷考试/Open-book exam		
闭卷考试/Close-book exam		
其他/Other(s)		

5.教材/Textbook(s)

序号 No.	名称 Title	编著者 Author(s)	标准书号 ISBN	出版机构 Publisher	出版年月 Publication Date
1	人工智能安全	曾剑平	9787302611509	清华大学出版社	202208

6.教学参考资料/Reading Materials and References

7.任课教师简介/Profile of Instructor(s)

刘森，青年副研究员，ACM SIGCOMM China专委会委员，从事新型网络架构、分布式系统互联和应用性能优化研究。近五年共在SIGCOMM、TON、JSAC、INFOCOM等国际顶级学术期刊和会议上发表学术论文30篇余，申请专利8项。2022年ACM SIGCOMM中国新星奖获得者，2020 年上海市“超级博士后”激励计划获得者。现担任多项国家项目、省部级重点项目课题负责人，担任包括TON、INFOCOM在内的多项国际国内顶级期刊及会议审稿人。

曾剑平，副教授，从事互联网大数据与安全方面的研究。主持国家自然科学基金、上海市自然科学基金等课题，研究方向是互联网社交媒体分析挖掘、大数据安全、人工智能安全、主动防御。在IEEE TIFS、Computers & Security、SCN、KBS等信息安全和人工智能有影响力的期刊上发表100多篇论文，获得大数据处理、大数据安全相关方面的技术发明专利9项。出版《互联网大数据处理技术与应用》、《Python爬虫大数据采集与挖掘》、《人工智能安全》三本著作。

办公地址	江湾X2 A6027	办公时间	周1-5

办公地址 Office Add	江湾X2 A6027	办公时间 Office Hour	周1-5
联系邮箱 Email Add	zjp@fudan.edu.cn	联系电话 Contact phone	