物联网信息安全课程教学大纲

【基于机工社第2版】

一、 课程基本信息

课程名称	物联网信息安全		
	Information Security of Internet of Things		
课程编号	COMP。。。。		
课程学分	3	总学时	48
学时分配	理论:40　实验:8　上机:0　课外:18		
课程类型	专业核心课		
开课学期	第 6 或 7 学期		
先修课程	物联网技术导论		
教材、参考书及其他资料	**使用教材：** [1] 桂小林等，物联网信息安全（第 2 版），北京：机械工业出版社，2021. [2] 桂小林等，物联网信息安全，北京：机械工业出版社,2014. **参考教材：** [1] 桂小林编著，物联网安全与隐私保护，北京：人民邮电出版社，2020		

二、课程目标及学生应达到的能力

课程目标 1:掌握物联网信息安全的概念和特征,理解物联网安全体系的重要性，能够在物联网系统设计时综合考虑工程经济、安全和隐私问题。

课程目标 2: 掌握密码学、身份认证和访问控制等信 息安全基础理论，并能够在物联网信息系统中进行应用。

课程目标 3:掌握 RFID 和二维码的安全隐私保护原理与方法，能够利用 HASH、密码学理论、RFID 安全机制与协议来实现物联网的身份识别与保护。

课程目标 4:掌握物联网信息安全中的系统安全方法和数据隐私保护机制,能够利用入侵检测、病毒查杀、k-匿名等技术保护物联网系统安全。

课程目标与专业毕业要求的关联关系

课程目标	毕业要求	毕业要求指标点
1	工程经济法律	
2	工程知识	
3	问题分析	
4	系统设计	

三、教学内容简介

章节	章节名称	知识点	参考学时
1	物联网与信息安全	物联网的概念与特征、物联网的安全威胁、物联网的安全体系结构、物联网的主要安全手段	2-4
2	物联网信息安全基础	物联网的数据安全特征 密码学概念、置换加密、流密码与分组密码、DES 算法、掌握 RSA 算法、散列函数与消息摘要	6-8
3	物联网感知安全	物联网感知层的主要安全问题、RFID 的物理安全机制、RFID 逻辑安全机制、RFID 安全认证协议、无线传感器网络安全技术、二维码支付的工作原理、二维码身份检测方法、二维码的应用	6-8
4	物联网接入安全	信任、信任管理、动态信任管理、信任计算、身份认证、访问控制、PK、VPN	6-8
5	物联网系统安全	恶意攻击、入侵检测、攻击防护技术、病毒攻击、病毒查杀、木马攻击、防火墙、网络安全通讯协议	4-6
6	物联网隐私安全	隐私安全的概念、隐私度量方法、数据库隐私保护技术、位置隐私保护技术、数据共享隐私保护方法、外包数据加密计算	6-8
7	区块链及其应用	区块链概念及其发展、区块链的结构、区块链的工作原理、区块链共识机制、区块链智能合约、区块链典型应用。	4-6

四、教学安排详表

序号	教学内容	学时	教学方式	教学要求 (知识要求及能力要求)	对课程目标的支撑关系
第一章	1 物联网安全特征 2 物联网安全需求 3 物联网安全技术 4. 物联网的安全体系	4	授课、作业和讨论	1. 理解物联网安全需求和特征，能够因素将信息安全技术与物联网系统有机结合。 2. 理解信息安全技术的内涵，并能够在物联网系统设计和实现时考虑工程、经济与安全因素。 3. 掌握物联网安全体系，能够对物联网系统进行安全建模。	课程目标1,4
第二章	1. 古典密码学介绍 2. DES 算法原理和应用 3. RSA 算法原理和应用 4. 新型加密算法	8+4	授课、作业、讨论和实验	1. 掌握密码学模型与数据置换方法，能够分析密码的安全性，理解密码的局限性。 2. 掌握 DES 加密原理和公钥密钥技术原理，能够在数据传输保密中进行应用； 3. 理解椭圆曲线和量子密码技术的作用。	课程目标1,2
第三章	1. 感知层安全威胁 2. 感知层的安全机制 3. RFID 的安全机制 4. RFID 安全协议 5. 摄像头安全与隐私 6. 二维码安全与隐私	8	授课、作业和讨论	1. 理解物联网感知层安全技术，能够将 RFID 安全技术用于身份检测与识别； 2. 掌握二维码支付原理及其安全保障机制，并能够在二维码支付中进行实际应用。 3. 理解摄像头面临的主要安全问题，并能够针对这些问题提出解决方案。	课程目标1,2,3
第四章	1. 物联网接入安全 2. 信任管理 3. 身份认证 4. 访问控制 5. 公钥基础设施	6+4	授课、作业、实验	1. 理解物联网接入原理，能够在物联网系统设计时考虑身份认证和访问控制问题。 2. 理解信任管理模型与机制，能够在身份认证是考虑信任级别，并在公钥基础设施中进行应用。 3. 理解物联网安全和应用层安全技术，能够在手机系统使用时考虑经济和安全因素。 4. 理解访问控制模型与方法，能够针对不同系统要求，采用不同的访问控制模型，并分析各种模型的优缺点。	课程目标1,3,4
第五章	1. 恶意攻击 2. 入侵检测 3. 攻击防护技术	4		1、理解系统安全的概念和主要方法，针对不同需求，能够合理选择系统安全保障方法。	课程目标1,2,4

	4.防火墙 5.病毒查杀 6.网络安全通信协议		授课、讨论、作业	2、理解恶意攻击、蜜罐、蜜网、防火墙技术，能够将这些技术应用到物联网相关系统中。 3、理解病毒和木马的概念和原理，能够针对性应用反病毒技术保护物联网应用系统。	
第六章	1.位置隐私保护体系 2.位置隐私保护技术 3.K-匿名栅格化技术 4.位置隐私攻击模型 5.轨迹隐私保护方法	6	授课、作业和讨论	1. 理解隐私概念，能够在物联网系统应用中考虑隐私保护问题，并进行数据隐私分级保护。 2. 理解数据隐私保护技术和位置隐私保护技术，能够针对不同系统需要，设计不同的隐私保护模型，使用合适的隐私保护方法。 3. 理解隐私攻击、度量技术，理解隐私保护技术的经济性、安全性和局限性。	课程目标1,4
第7章	1.区块链概念与结构 3.区块链的工作原理 4.区块链的共识机制 5.区块链的智能合约 6.区块链的典型应用	4	授课、作业和讨论	1. 理解区块链的概念与结构，能够将区块链用于物联网系统的信任管理。 2. 理解区块链的工作原理，能够在分布式物联网系统中进行身份共识。 3. 理解区块链的智能合约原理并能够在区块链中进行应用。	课程目标1,4

五、实践环节

序号	实验名称	实验内容	教学方法	对课程目标的支撑关系
1	数据安全与隐私保护	（1）设计一个 DES 或 RSA 程序，实现文字和图片的加解密。 （2）设计一个 K-匿名程序，实现位置隐私保护	分小组实验，单人提交。不同方法实现的算法或者对算法功能、流程加 以改进	课程目标 1、2，4
2	信任计算与身份认证	（1）设计一个基于信任计算的身份识别认证程序。 （2）设计一个基于图案锁的身份认证实验。	分小组实验，每小组 3,4 人，每人承担不同内容，提交独立的实验报告。	课程目标 1、3，4

六、课外学时分配

序号	内容	参考学时	对课程目标的支撑关系
1	以小组形式，完成一个手机图案锁的安全应用。充分考虑包括从感知层、接入到应用层的安全技术，分析该设备安全概率或风险。	8	课程目标 1、2、3、4

七、考核方式及成绩构成

平时：30%，

实验：20%；

期末：50%

大纲制定者：桂 XX

大纲审核者：XXX

最后修订时间：2020 年 12 月 20 日