物联网安全与隐私保护课程教学大纲

一、课程基本信息

|  |  |  |  |
| --- | --- | --- | --- |
| 课程名称 | 物联网安全与隐私保护 | | |
| Information Security & Privacy of Internet of Things | | |
| 课程编号 |  | | |
| 课程学分 | 2 | 总学时 | 40 |
| 学时分配 | 理论:32 实验:8 上机:0 课外:18  （课外学时不计入总学时） | | |
| 课程类型 | 专业核心课 | | |
| 开课学期 | 3-1或3-2 | | |
| 先修课程 | 物联网技术概论 | | |
| 教材、参考书及 其他资料 | 使用教材：  [1]桂小林.物联网安全与隐私保护. 北京:：人民邮电出版社，2019.  参考教材：  [1]桂小林等.物联网信息安全. 北京： 机械工业出版社，2014.  [2]胡向东等. 物联网安全. 科学出版社，2012. | | |

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2： 掌握RFID安全隐私保护原理与方法，能够将RFID的物理安全机制与逻辑安全机制用来实现物联网RFID 的安全与隐私保护。

课程目标3：掌握物联网信息安全中的系统安全与隐私保护方法，能够利用入侵检测、病毒查杀、k-匿名等技术来保护物联网系统安全。

课程目标4：理解信息安全因素在物联网研究和开发中的作用，并能够在物联网应用系统设计中综合考虑工程、经济和安全因素，为后续研究和工作提供支撑。

课程目标与专业毕业要求的关联关系

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 毕业要求  课程目标 |  |  |  |  |  |  |  |  |  |  |
| 1 |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

三、教学内容简介

|  |  |  |  |
| --- | --- | --- | --- |
| 章节顺序 | 章节名称 | 知识点 | 参考学时 |
| 1 | 第1章  物联网安全体系 | 物联网的概念与特征、物联网的体系结构、物联网安全问题分析、物联网的信息安全体系、 | 讲授4-6 |
| 2 | 第2章  物联网感知安全 | 物联网感知层的安全威胁、物联网感知层的安全机制、物联网的RFID安全分析  RFID的安全机制、RFID安全协议、摄像头的安全与隐私机制、二维码的安全与隐私机制 | 讲授6-8  实践2 |
| 3 | 第3章  物联网数据安全 | 数据安全三原则、数据加密模型、密码攻击方法  置换和替换、DES加解密算法、RSA加解密算法  可计算加密算法、同态加密算法 | 讲授6-8  实践2 |
| 4 | 第4章  物联网接入安全 | 信任与信任管理、身份认证的概念与主要方式、面向手机的身份认证技术、访问控制的概念与原则、BLP访问控制、基于角色的访问控制、基于信任关系的动态访问控制模型、基于于信任关系的动态服务授权 | 讲授6-8  实践2 |
| 5 | 第5章  物联网系统安全 | 网络与系统安全的概念，恶意攻击的概念、原理和方法，入侵检测的概念、原理和方法，攻击防护技术的概念与原理，防火墙原理，病毒查杀原理，网络安全通信协议 | 讲授6-8 |
| 6 | 第6章  物联网隐私保护 | 位置隐私保护体系结构、位置隐私保护技术、  K-匿名栅格化的位置隐私保护、位置隐私攻击模型、轨迹隐私保护分类与度量、轨迹隐私保护方法 | 讲授4-6  实践2 |

四、教学安排详表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 教学内容 | 学时分 配 | 教学方式  （授课、实验、 上机、讨论） | 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 | 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。 | 课程目标1，4 |
| 2．物联网安全需求 |
| 3．物联网安全技术 |
| 第二章 | 1.物联网的安全体系结构  2.物联网感知层安全  3.物联网网络层安全  4.物联网应用层安全 | 6 | 授课、作业和讨论 | 1. 掌握物联网安全体系，能够对物联网系统进行安全建模； 2. 理解物联网感知层安全技术，能够将RFID安全技术应用到实际生活中； 3. 理解物联网网络层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。 | 课程目标 1，2，3 |
| 第三章 | 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 | 6+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 1，2，4 |
| 第四章 | 1．隐私度量  2．数据隐私  3．位置隐私  4．隐私攻击 | 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 |
| 第五章 | 1.物联网接入安全的概念  2.信任管理  3.身份认证  4.访问控制  4.公钥基础设施 | 4+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 |
| 第六章 | 1.恶意攻击  2.病毒、木马  3.入侵检测和安全防护  4.网络安全协议 | 4 | 授课、讨论、作业 | 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；  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。 | 课程目标 1，2,4 |
| 第七章 | 1.无线网络安全协议  2.WIFI，蜂窝网络、蓝牙安 全技术  3.下一代无线网络安全 | 2 | 授课、讨论、实验 | 1.理解无线网络安全协议的原理和作用，能够针对不同的应用系统，进行无线网络安全配置和管理；  2.理解下一代无线网络技术，能够在系统设计时考虑工程和安全因素。 | 课程目标 4 |

五、实践环节

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 实验编号 | 实验名称 | 实验内容 | 教学方法 | 对课程目标的  支撑关系 |
| 1 | 数据安全实验  （DES 或 RSA） | 设计一个 DES 或 RSA 程序， 可参考开源代码实现对文 字、图片的加解密过程 | 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 | 设计一个图像识别的身份认  证程序或参考淘宝的信誉体  系设计一套信用计算方法实  现动态信任管理 | 分小组实验，每小组 3,4  人，每人承担部分内容 | 课程目标  1、3，4 |

六、课外学时分配

|  |  |  |  |
| --- | --- | --- | --- |
| 章节顺序 | 内容 | 参考学时 | 对课程目标的支  撑关系 |
| 1 | 以小组形式，完成一个物联网设备，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：10%；

期末：60%

大纲制定者：桂小林 大纲审核者：桂小林 最后修订时间：年月日