计算机安全（2024 年春季）

绪论	信息安全的概念和 CIA 三要素 系统研究的方法（还原论、整体论）、系统安全工程、系统安全思维 风险分析基本方法(资产×漏洞×威胁) 攻击面、攻击树、社会工程学
计算机安全基础	计算机安全的内涵，CIA 三要素，PDRR/PDR/PPDRR 模型 计算机安全的五个设计原则 隐蔽信道（隐信道）、旁道攻击（侧信道攻击）
身份识别与认证	口令空间的计算，蛮力攻击的时间（平均、至多） 用户身份认证可以基于哪些信息 口令认证机制面临的威胁（猜测、欺骗、文件泄露、遗忘） 口令认证机制的缺点
访问控制	主角、主体、客体/对象/目标、访问操作 自主访问控制 DAC、强制访问控制 MAC 访问控制矩阵、能力、访问控制列表 中间控制，如组、否定许可、角色、特权 安全级别的偏序关系、安全标签的格 基于角色的访问控制 RBAC（角色继承、角色限制） 基于任务的访问控制 TBAC（上下文环境、动态授权）
使用控制	ABC 模型的三个基本元素和三个授权相关元素 UCON 的 16 种基本模型（preA0/preA1/preB0/onC0/...） 会用使用控制模型描述 DAC/MAC/RBAC
访问监控器	访问验证机制（访问监控器实现）的三个核心要求 访问监控器、安全内核、可信计算基 受控调用/门、可信路径
计算机实体安全	可信计算，TPM，软件狗
Unix/Linux 安全	Unix 的自主访问控制，粒度 主角（UID、GID、group、root）；主体（pid、EUID/EGID/RUID/RGID） 客体（文件许可位及其二进制表示、八进制表示） SUID/SGID 受控调用；强制访问控制（SELinux 优点、类型、域、域切换）
Android 安全	Android 系统架构（Dalvik/ART），主要安全机制(沙箱、权限)
Windows 安全	WinLogon、LSA、SAM、注册表、域、活动目录 主角、主体、令牌、安全描述符、受限上下文 DACL、SACL、DEP
数据库安全	关系数据库、视图、快照、存储过程、函数、触发器 委托授权、递归回收、否定式授权、解决授权冲突的原则 视图的优势，用户发放授权和角色发放授权的区别 三元组安全标签、基于标签的访问判定 统计数据库的推理、跟踪攻击、差分隐私 完全备份、差异备份、增量备份

系统可信检查机制	系统可信引导和系统安全引导的异同 进程完整性体现在哪些方面（初始状态、中断过程、片上 Cache/片外存储、输出结果）
BLP 模型	状态集 V=B×M×F；ss-property，*-property，ds-property 基本安全定理；隐蔽信道、隐蔽存储信道、隐蔽定时信道
安全模型	Biba 模型：简单完整性，完整性*-property，动态完整性级别，信息传递路径，调用性，环属性 Chinese Wall 模型：公司数据集，利益冲突类，安全标签，ss-property，*-property 信息流模型：强(显示)信息流、弱(隐式)信息流、信息量/条件熵计算、赋值语句/条件语句的信息流分析和安全必要条件
安全评估	安全评估框架（评估对象、评估目标、评估方法） TCSEC/ITSEC/CC 的级别和内涵；TCSEC 各个级别的特点
网络安全等级保护	等级保护的内涵、等保 2.0 的十大安全类 等级保护制度的主要内容(从信息、信息系统、安全产品、安全服务资质、安全事件等方面) 等级保护的主要工作(定级、备案、建设/整改、定期等级测评、定期监督检查) 等级保护对象的定级方法（业务信息/系统服务/受侵害客体/侵害程度） 等级测评流程(测评准备、方案编制、现场测评、报告编制)
密码应用安全性评估	密码应用安全性评估的含义（合规性、正确性、有效性） 密码应用基本要求的八大安全类 技术标准中“应”、“宜”、“可”的区别 等保和密评的区别（方案评估）
云计算安全	云计算的主要特性（按需自助服务、泛在接入、资源池化、快速伸缩性、服务可计量） 云计算的服务模式（SaaS、PaaS、IaaS） 云计算的部署模式（公有云、私有云、社区云、混合云） 云服务商和客户之间的安全责任划分（设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台、应用软件）
基于代码的访问控制	堆栈遍历、惰性计算、热情计算 许可断言
入侵检测	IDS、IPS、DPI、DFI、态势感知 入侵检测方法（异常检测、误用检测） 入侵检测系统分类（按照数据来源，基于主机、基于网络、混合型）
应急响应与灾备恢复	IATF：一个核心思想、三个核心要素、四个焦点领域 应急响应的概念、应急响应过程、风险评估过程 灾难恢复的概念、容灾备份的概念 RAID 0、RAID 1、RAID 10 和 RAID 5