计算机安全（2021 年春季）

程绍银 sycheng@ustc.edu.cn

介绍	**绪论**	信息安全的概念和属性 等级保护、风险评估和安全测评的相互关系 风险评估的基本方法，攻击树
安全基础	**计算机安全基础**	计算机安全的定义及其内涵，CIA 模型含义 计算机系统的保护措施 计算机安全的五个设计原则 隐蔽通道（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三种威胁
	访问控制	主角、主体、客体（对象）、访问操作 自主访问控制 DAC、强制访问控制 MAC、基于角色的访问控制 RBAC 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 格适用于描述安全性、完整性等级别
	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	引用验证机制（访问监控器）的三个核心要求 受控调用/门、可信路径 访问监控器、安全内核、可信计算基
	计算机实体安全	可信计算 环境对计算机的安全威胁 计算机工作的环境温度和湿度范围
系统安全	**Unix/Linux 安全**	Unix 的自主访问控制，粒度 主角（UID、GID、group、root） 主体（pid、ppid、real/effective UID/GID） 客体（文件许可位） SUID/SGID 受控调用 Unix 安全机制（基于用户名和口令的身份识别和认证、文件系统安全）
	Android 安全	Android 系统架构（Dalvik/ART） Android 的主要安全机制(沙箱/权限)
	Windows 安全	WinLogon/LSA/SAM/注册表/域/活动目录 主角&域/主体/令牌/对象/安全描述符/访问掩码/受限上下文 DACL/SACL 安全管理

系统安全	BLP 模型	状态集 V=B×M×F ss-property, *-property, ds-property 基本安全定理
	Biba 模型	简单完整性，完整性*-property 主体低水印性，客体低水印性 调用性，环属性
	中国墙模型	公司数据集，利益冲突类，安全标签 ss-property, *-property
	信息流控制模型	强信息流、弱信息流 隐式信息流的信息量/条件熵计算 隐信道、隐存储信道、隐定时信道
	安全评估	安全评估框架（评估对象/评估目标/评估方法） TCSEC（级别定义和内涵） ITSEC（级别定义和内涵/TOE） CC（级别定义和内涵/保护框架 PP/安全目标 ST/评估类型）
	网络安全等级保护	等级保护制度的主要内容 等级保护的主要工作/测评流程 等级保护 2.0 与 1.0 的区别，等保 2.0 的十大安全类 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）
	数据库安全	关系数据库/视图/快照/存储过程/触发器 自主访问控制/特权 聚集/推断/跟踪攻击/差分隐私 数据备份/数据容灾/全备份/增量备份/差分备份
网络系统安全	基于代码的访问控制	与代码相关的安全属性（可作为访问控制的证据） 调用链/堆栈游走 Java 安全模型/.NET 安全框架
	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）
	入侵检测	PDR/PDRR 模型 入侵检测方法（异常检测/误用检测） 入侵检测系统的分类（基于主机/基于网络/混合型） IDS/IPS/DPI/DFI/态势感知
	网络侦查	社会工程学 网络扫描/Nmap 网络监听/Wireshark
	拒绝服务攻击	DoS/DDoS/DRDoS