工程概论

第3章 信息安全与隐私

授课教师：孙运雷

目录

CONTENTS

1

信息安全的内涵与系统观

为什么信息安全需要系统思维?

- **案例：某医院因勒索软件攻击导致患者数据加密，急救系统瘫痪48小时**
- **提问：**
  - 攻击暴露了哪些安全问题？（技术漏洞？管理缺失？）
    - 技术漏洞
      - 系统漏洞、网络安全配置不足、数据备份不足、身份认证与访问控制薄弱
    - 管理缺失
      - 安全意识培训不足、应急预案缺失、合规性管理不足
  - 单一防火墙能否解决所有风险?
    - 无法防御内部威胁、无法保护应用层漏洞、无法阻止横向移动、无法防御社会工程攻击

CIA三元组——信息安全的基石

- **机密性（Confidentiality）**
  - 定义：确保信息仅被授权者访问
  - 反面案例：2017Equifax数据泄露（1.43亿用户社保号被盗）
- **完整性（Integrity）**
  - 定义：防止数据被未授权篡改
  - 案例：震网Stuxnet病毒篡改伊朗核设施离心机控制指令
- **可用性（Availability）**
  - 定义：确保授权用户及时可靠访问资源
  - 案例：DDoS攻击瘫痪DeepSeek服务

系统安全观的层次架构

层级	防护对象	典型措施
物理安全	硬件设备、机房	门禁系统、防灾设施
数据安全	数据库、文件	加密技术、备份容灾
应用安全	软件系统、API接口	代码审计、渗透测试
管理安全	人员、流程、制度	权限分级、安全培训、应急预案

- **互动讨论：**
  - 以校园一卡通系统为例，分组讨论四层安全如何协同工作

威胁无处不在——攻击者的“工具箱”

- **恶意攻击**
  - APT攻击（国家级黑客组织）
  - 勒索软件（WannaCry全球事件）
- **技术漏洞**
  - 零日漏洞（Log4j漏洞影响全球企业）
  - 配置错误（AWS S3存储桶公开访问泄露数据）
- **人为失误**
  - 弱密码（123456仍是最常用密码）
  - 钓鱼邮件（特斯拉员工误点链接导致工厂数据泄露）

从理论到实践——安全设计的系统性原则

- **设计原则：**
  - **最小权限**原则（如Linux用户权限分级）
  - **失效安全**原则（故障时默认关闭而非开放）
  - **纵深防御**原则（多层防线避免单点失效）
- **技术趋势：零信任架构（Never Trust, Always Verify）**
  - **最小权限**原则：用户、设备、应用仅被授权完成特定任务所需的最小权限
  - **持续验证**原则：访问策略基于实时上下文动态调整，而非一次性认证
  - **假设被入侵：**默认所有形态可能已遭渗透，需限制攻击者横向移动能力

2 隐私保护的技术挑战与伦理边界

我们真的拥有隐私吗？

数据对比：

- 2000年：人均每日产生0.1GB数据
- 2023年：人均每日产生2.5GB数据（来源：IDC报告）

灵魂拷问：

- "当你使用免费导航APP时，是否意识到用**实时位置数据**支付了服务对价？"

隐私定义的演进-从个人秘密到数字身份

阶段	隐私内涵	典型案例
传统隐私	住宅、通信、肖像权	1984年《美国电子通信隐私法》
数字隐私	位置轨迹、行为偏好	2018年Cambridge Analytica数据滥用事件
泛在隐私	生物特征、脑电波等新型数据	2023年马斯克Neuralink脑机接口隐私争议

技术双刃剑——隐私泄露的四大高危场景

- **大数据画像**
  - 案例：某电商通过购物记录推测用户怀孕（比家人更早知晓）
  - 技术机制：协同过滤算法 × 用户行为分析
- **位置追踪**
  - 案例：Uber"上帝之眼"功能实时查看用户位置引发诉讼
  - 技术机制：GPS定位 × 轨迹预测算法
- **生物特征滥用**
  - 案例：国内售楼处用人脸识别区别对待自然访客与渠道客户
  - 技术机制：人脸识别 × 数据关联分
- **元数据泄露**
  - 案例：手机基站数据反推用户社交关系（斯诺登披露NSA监控）
  - 技术机制：通信日志分析 × 图数据库挖掘

- 互动环节：
  - 投票：上述场景中哪个对隐私侵犯最隐蔽？
  - 讨论：为何元数据比内容数据更具危险性？

工程师的抉择——效率与隐私能否兼得?

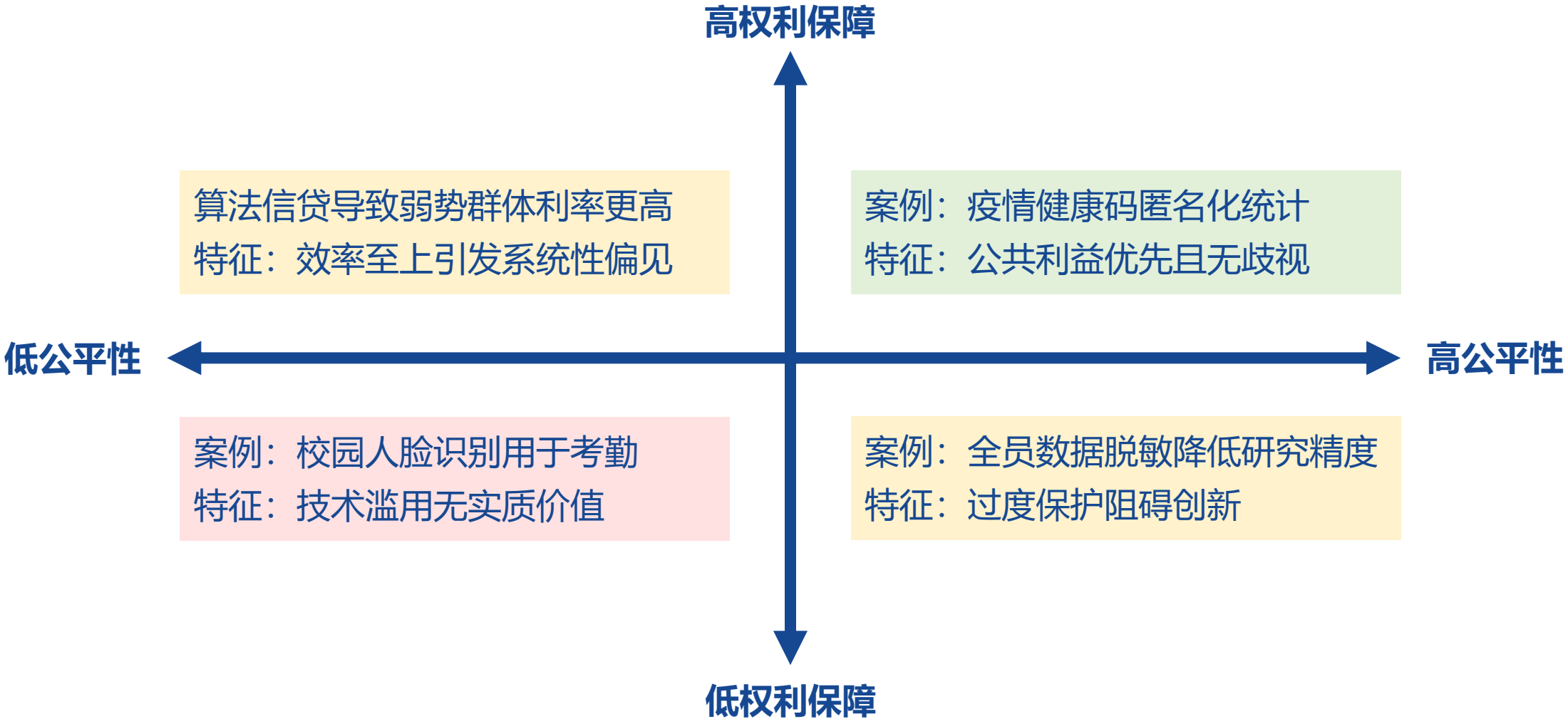
技术需求	隐私风险	伦理困境
精准推荐算法	过度收集用户偏好	商业价值 vs 用户控制权
疫情密接追踪系统	轨迹信息公开导致歧视	公共安全 vs 个人匿名权
AI训练数据采集	包含未脱敏个人信息	技术创新 vs 知情同意原则

- 决策工具:
  - 隐私影响评估（PIA）流程
  - 伦理审查四象限法（效用/风险/权利/公平）

隐私影响评估（PIA）流程

1. **确定评估范围与目标**：界定项目边界、明确评估目标
2. **组建 PIA 团队**：跨部门协作、明确职责分工
3. **开展数据映射与收集**：绘制数据流程图、识别数据类别、收集信息
4. **风险识别与分析**：识别潜在风险、评估风险可能性、评估影响程度
5. **制定风险缓解措施**：技术措施、管理措施、应急响应措施
6. **合规性审查**：法律法规对标、行业标准与最佳实践对照
7. **撰写 PIA 报告，明确给出评估结论。**
8. **持续监控与更新**：建立监控机制、及时更新 PIA

伦理审查四象限法


高权利保障
低公平性
高公平性
低权利保障
算法信贷导致弱势群体利率更高
特征：效率至上引发系统性偏见
案例：疫情健康码匿名化统计
特征：公共利益优先且无歧视
案例：校园人脸识别用于考勤
特征：技术滥用无实质价值
案例：全员数据脱敏降低研究精度
特征：过度保护阻碍创新

隐私增强技术（PETs）破局

- **数据最小化**技术
  - 联邦学习：数据不动模型动（医疗联合科研案例）
  - 差分隐私：添加噪声保护个体（苹果iOS数据收集方案）
- **用户赋权**技术
  - 隐私计算沙盒：数据可用不可见（蚂蚁摩斯安全计算平台）
  - 数据代理机器人：自动执行用户隐私偏好（MyData架构）
- **合规验证**技术
  - 区块链存证： GDPR"被遗忘权"实施追踪
  - 自动化审计工具：检测算法歧视性（IBM AI Fairness 360）
- **三重认知升级**
  - 隐私已从道德议题变为技术可实现目标
  - 工程师需在架构设计阶段植入隐私保护（Privacy by Design）
  - 没有完美的方案，只有动态的平衡

3

信息安全法律法规体系

技术自由 vs 法律边界——工程师如何抉择?

冲突案例：某AI公司未经用户授权使用社交媒体数据训练模型，面临欧盟GDPR天价罚款

提问：

- 工程师是否应承担合规责任?
- 法律如何影响技术架构设计?

中国网络安全治理的"三驾马车"

法律	管控对象	工程师义务
《网络安全法》	关键信息基础设施	▶ 等保2.0实施（三级以上系统） ▶ 日志留存≥6个月
《数据安全法》	数据分类分级	▶ 重要数据目录标识 ▶ 跨境数据传输安全评估
《个人信息保护法》	个人信息处理	▶ 最小必要原则落地 ▶ 单独同意机制（如人脸信息采集）

全球化的合规拼图——工程师必备知识

- **GDPR**（欧盟）
  - 核心要求：数据主体权利（访问/删除/携带）
  - 工程影响：设计默认隐私保护（如Cookie同意管理界面）
- **CCPA**（美国加州）
  - 特色条款：用户可拒绝数据出售（“Do Not Sell”按钮）
  - 技术实现：数据标签化追踪与响应
- ISO/IEC **27001**
  - 实施要点：PDCA循环（计划-执行-检查-改进）
  - 文档体系：风险处置计划→安全运行记录

行业规范实践

- **金融行业**
  - 央行《金融数据安全分级指南》
  - 案例：支付系统必须满足PCI DSS标准（加密存储+双因素认证）
- **医疗健康**
  - HIPAA（美国）与《健康医疗数据安全指南》（中国）
  - 技术约束：去标识化处理后方可用于AI训练
- **开源合规**
  - GPL传染性条款对代码引用的限制
  - 供应链安全：Log4j漏洞暴露的开源组件管理缺失

法律合规的工程实现路径

- **把法条翻译成代码——合规驱动的系统设计**
  - 1 **需求分析**阶段
    - 法律条文→ 功能需求（如《个保法》第17条→ 隐私政策弹窗开发）
  - 2 **架构设计**阶段
    - 合规性设计模式（如数据主权架构支持区域隔离）
  - 3 **测试验证**阶段
    - 自动化合规测试工具（如GDPR合规扫描插件）
  - 4 **运维监控**阶段
    - 实时审计追踪（区块链存证不可篡改）

案例分析：通过隐私计算中间件同时满足精准推荐与数据最小化原则

- **背景**
  - 某电商平台希望为用户提供个性化推荐，同时遵守《通用数据保护条例》(GDPR)中的数据最小化原则，即仅收集和处理必要的数据。
- **解决方案：隐私计算中间件的作用**
  - 隐私计算中间件是一种技术架构，能够在数据不出本地或加密状态下进行计算，确保用户隐私得到保护。
  - **1. 数据本地化处理**
    - 技术实现：用户行为数据（如浏览、点击、购买记录）在用户设备本地进行处理，而不是上传到中心服务器。
    - 合规性：数据最小化原则得到满足，因为平台仅获取处理后的结果，而非原始数据。
    - 示例：用户在浏览商品时，中间件在本地分析其偏好，生成兴趣标签，仅将标签上传至平台。

案例分析：通过隐私计算中间件同时满足精准推荐与数据最小化原则

- 2. **联邦学习**（Federated Learning）
  - 技术实现：平台通过联邦学习技术，在用户设备本地训练推荐模型，模型参数（而非原始数据）被上传至服务器进行聚合和优化。
  - 合规性：原始数据始终保留在用户设备上，符合数据最小化原则。
  - 示例：用户A和用户B的本地模型分别学习其偏好，平台将两个模型的参数聚合，生成全局推荐模型，而不直接访问用户A和用户B的数据。
- 3. **差分隐私**（Differential Privacy）
  - 技术实现：在数据上传或模型训练过程中，加入随机噪声，确保无法通过计算结果反推个体用户信息。
  - 合规性：保护用户隐私，同时允许平台进行宏观分析。
  - 示例：平台分析用户群体的购买趋势时，使用差分隐私技术，确保无法识别具体用户的购买记录。

案例分析：通过隐私计算中间件同时满足精准推荐与数据最小化原则

- 4. **安全多方计算**（Secure Multi-Party Computation, MPC）
  - 技术实现：多个参与方（如用户、商家、平台）在不泄露各自数据的情况下，共同计算推荐结果。
  - 合规性：数据在加密状态下进行计算，避免泄露用户隐私。
  - 示例：平台与商家合作推荐商品时，通过MPC技术计算用户偏好与商品匹配度，而不泄露用户的具体行为数据。
- 5. **用户控制与透明性**
  - 技术实现：中间件提供用户控制面板，允许用户查看和管理其数据的处理方式。
  - 合规性：满足GDPR的透明性要求，增强用户信任。
  - 示例：用户可通过控制面板选择是否参与联邦学习或差分隐私计算，并随时撤回同意。
- **总结**
  - 通过引入隐私计算中间件，电商平台在满足数据最小化原则的同时，实现了精准推荐。

4

工程实践中的安全与隐私管理

安全防护体系设计

■传统分层防御模型

- □网络层：防火墙/IPS
- □主机层：HIDS/EDR
- □应用层：WAF/代码签名
- □数据层：加密/脱敏

■零信任架构实践

- □核心原则：持续验证，永不信任（Never Trust, Always Verify）
- □实现路径：
  - ➢ 微隔离（如Kubernetes网络策略）
  - ➢ 动态访问控制（基于用户行为风险评估）

隐私增强技术（PETs）

技术	适用场景	工程实现	局限性
同态加密	云端密文计算	Microsoft SEAL库集成	性能损耗高（100-1000倍）
联邦学习	跨机构数据协作	PySyft框架分布式训练	通信成本剧增
差分隐私	统计发布	Google DP开源工具集	数据效用下降
安全多方计算	金融联合风控	隐私计算中间件（如蚂蚁摩斯）	开发复杂度高

全生命周期管理框架

- **开发阶段**
  - 威胁建模（STRIDE方法）
  - 安全编码规范（如OWASP Top 10防护）
- **测试阶段**
  - DAST/SAST工具链（如ZAP+Snyk）
  - 模糊测试（AFL框架）
- **运维阶段**
  - 漏洞赏金计划（如HackerOne平台）
  - 红蓝对抗演练

合规驱动的隐私工程

原则	技术实现	管理措施
主动预防而非事后补救	隐私影响评估工具集成到需求管理系统	设立隐私保护官（DPO）岗位
隐私默认设置	用户首次登录默认关闭非必要数据收集	定期隐私设置复查机制
隐私嵌入设计	架构设计文档包含隐私保护模块接口	跨部门隐私评审会议
全生命周期保护	数据自动过期删除功能	供应商隐私管理协议（DPA）

本章案例分析作业

在第一章的复杂工程问题基础上，分析其可能存在的数据泄露风险，结合《个人信息保护法》要求设计技术与管理结合的解决方案。

中国石油大学（华东）
CHINA UNIVERSITY OF PETROLEUM

谢谢大家！