Privacy threat modeling using linddun

Privacy

- Obtaining privacy means controlling the consequences of exposing personal information in a given context
- Limiting personal data
- Providing data subjects: to be informed about and intervene in the processing operation of personal info.

Privacy threat category (LINDDUN)

- Likability 可链接性
- Identifiability 可识别性
- Non-repudiation 不可否认性
- Detectability 可检测性
- Disclosure of information 信息泄露性
- Unawareness 不了解性
- Non-compliance 不遵守规定性

GDPR key concepts

- Key subject rights (unawareness)
    - Right to information, object, access, rectification, be forgotten, data portability, object to profiling

- Processing principles (non-compliance)
    - Lawfulness
    - Storage limitation
    - Purpose limitation
    - Accuracy
    - Data minimization
    - Integrity and confidentiality

Threat modeling (fix the what can go wrong before actually happens)

- Tackled proactively
- Systematically analyzed
- Integrated in the development lifecycle
- Have an impact on design decisions

威胁建模 (threat modeling)

- 识别体系化的结构缺陷， 指导安全测试， 降低因安全漏洞造成的顺财或财产损失等可能性
- 节约组织安全成本： 在设计阶段建立安全性需求， 降低安全设计缺陷导致的修复成本
- DevSecOps： 通过威胁建模和安全工具的流程， 把风险管理潜入产品的完整生命周期
- 满足合规要求：通过向管理层和监管机构提供产品的风险管理活动的完整记录， 帮助遵守法规要求

Privacy threat modeling

- Model the system, create a relationship schema to represent the system work flow, describe all data
- Elicit threats, map threats to the schema, identify threats using LINDDUN methods
- Manage threats, prioritize/assess and mitigate to provide solution
- Reflect and repeat the above procedure again

数据流关系图元素

- 过程（圆圈）： 接收， 修改输入， 将输入定向到输出， 可以用于数据存储， 外部实体， 过程元素之间
- 数据存储（平行线）： 永久/临时存储，
- 外部实体（正方形）： 直接控制之外的任务，实体，数据的储存
- 数据流（箭头）： 进程，数据存储和外部实体之间的数据移动
- 信任边界（虚线）： 信任区域在数据流经系统是更改

数据流关系图深度层

- 0: 对于所有系统都是必须的， 包含主要系统部分 （系统层）
    - 创建每个系统都需要系统层
    - 帮助了解其工作原理， 交互方式

- 风险： 新系统会给环境带来哪些风险，新的分析程序与协议， 新的身份验证与授权条例， 新的机密储存和加密方法， 第三方身份验证， 所需的未加密信道， 功能所需的权限等

- 1: 对于大多数系统是必须的， 包含每个系统部分和其他关系图 （过程层）
  - 对于每个系统， 处理敏感数据时使用过程层
  - 用于找出威胁， 降低风险

- 2: 对于高敏感的系统是必须的， 包含系统子部分和其他关系图 （子过程层）
  - 系统中子过程层漏洞可能会导致系统， 客户等面临风险
  - 在安全环境中使用/处理敏感数据/有高风险评分的系统

- 3:对于关键级别系统/内核级别系统是必须的， 包含每个过程的其他关系图 （较低级别层）
  - 表示低级别系统子部分
  - 进行威胁建模
  - 为一个子过层进行多轮安全检查

处理数据流关系图与威胁建模， 威胁建模 4 步骤

1. 设计

- 了解系统工作原理
- 列出系统的每个服务
- 列举有关环境和磨人安全配置的所有假设
- 创建数据关系流程图：
- 提出有关系统的问题： 功能？ 业务流程加定义？ 系统如何建构？ 用户如何使用系统？ 是否需要数据/硬件访问要求？ 运营商？ 默认安全配置？ 操作系统如何影响系统本身？ 第三方和第一方默认安全配置， 如何影响系统要求？ 系统账户类型和需要那些访问权限？系统如何保护账户？ 系统如何监视异常和备份数据 如何加密？ 系统创建/处理数据的类型/如何分析数据/如何对数据进行加密？

2. 中断

- 以了解攻击者， 保护系统为内容 用 LUDDUN 框架识别常见威胁， 发现用户与系统的未加密链接/哪些流程可以暴露用户信息， 攻击者可能会对这些信息采取什么行动， 分类数据处理确定关键资产加以保护

3. 修复

- 衡量每个威胁的优先级： 威胁的影响， 严重性， 风险
- 在 bug 管理服务中对每个 威胁进行跟踪
- 提出对应 LUDDUN 威胁的安全控制建议
- 选择相对应功能对威胁采取解决

4. 验证

- 确认系统满足所提出的安全要求：是否满足 网络安全， 机密管理， 安全控制， 访问控制等
- 确保正确的安全系统控制解决所有问题
- 在实行前手动/自动验证：是否可以处理机密数据， 要遵守什么规定，有什么其他安全保护功能， 对隐私和运营开发是否有风险

使用框架识别威胁， 找到减少风险的方法

谁问题优先级， 应用安全控制措施

- 确定问题的优先级
  - 每个问题的风险因素
  - 攻击者带来的风险影响
- 安全控制类型与功能
  - 物理控制 （摄像头， 围栏等）
  - 技术 （加密， 防火墙， 杀毒软件）
  - 管理 （策略， 法规要求）
  - 对于潜在威胁进行系统保护
  - 安全控制的预防， 检测， 纠正， 恢复， 阻碍
  - 运用物理， 技术， 管理控制对安全控制每个部分提出解决方法
  -

https://tari.moe/2021/04/04/thread-modeling/