数据安全之威胁建模
Threat modeling for data security

演讲人：樊山

CONTENTS

目录

什么是威胁建模
What is threat modeling

威胁建模是一个结构化的过程，其目标如下：

- 识别安全需求，
- 精确定位安全威胁和潜在漏洞，
- 量化威胁和漏洞的关键性，并优先考虑补救方法。

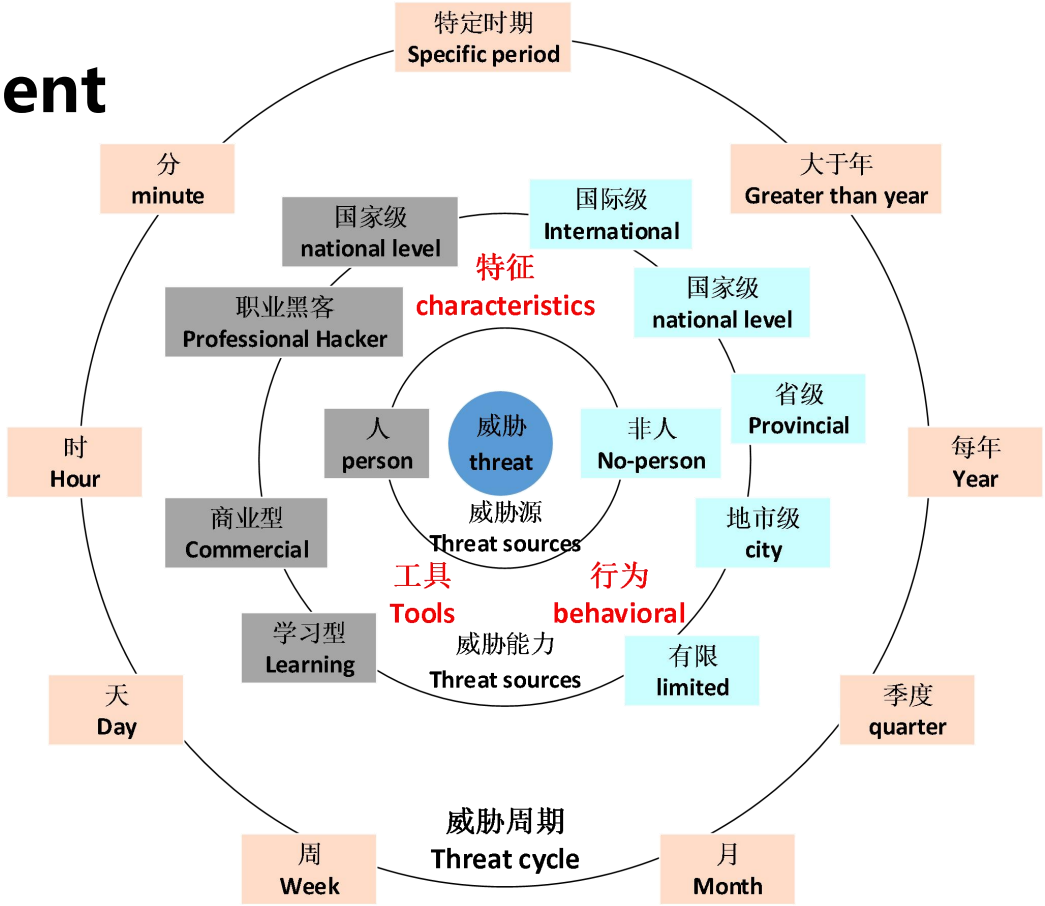
威胁建模方法会创建以下工件：

- 系统的抽象
- 潜在攻击者的简介，
- 包括他们的目标和方法，可能出现的威胁目录

威胁建模特征
Threat modeling characteristics

- 被建模的逻辑实体（数据、软件、系统等）；
- 系统生命周期的阶段（例如，软件初始设计期间的安全建模与已实现的现成软件的安全建模）；
- 威胁建模的目标（减少软件漏洞、阻止特定类别的攻击者、提高整体系统安全性、保护特定类型的数据等）。

威胁元素
Threat element



基于数据的威胁建模场景
Data-based threat modeling scenarios

- 以数据为中心的系统威胁建模允许组织考虑每个需要关注的案例的安全需求，而不是仅仅依赖通用化的“最佳实践”建议。添加以数据为中心的系统威胁建模，在持续监控、安全自动化和安全指标方面具有强大能力的组织应考虑根据本出版物中介绍的原则以补充这些能力，并为特别重要的数据实现明显更好的安全性。
    - *NIST SP 800-154 Guide to Data-Centric System Threat Modeling*

以数据为中心的系统威胁建模
Data-Centric System Threat Modeling

步骤 1：识别和描述需要关注的系统和数据

识别系统内数据的授权位置

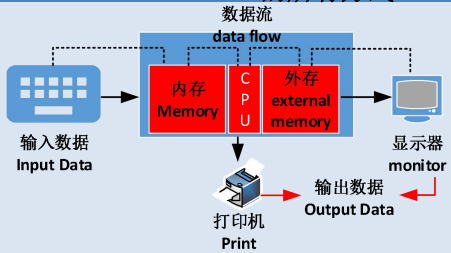
所有静态数据所在位置

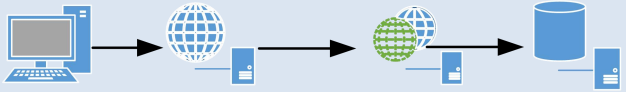
数据在系统组件之间和跨越系统边界的网络上传输的所有方式

运行时保存在本地内存中的数据，虚拟 CPU 处理的数据

使用键盘输入数据/打印到物理连接的打印机的数据、笔记本电脑屏幕上显示数据

识别数据如何在系统内授权位置之间移动





识别数据的安全目标

- 抗抵赖性（Non repudiation）
- 可靠性（Reliability）
- 真实性（Authenticity）
- 数据质量（Data quality）

识别影响安全目标的方式访问数据的人员和流程

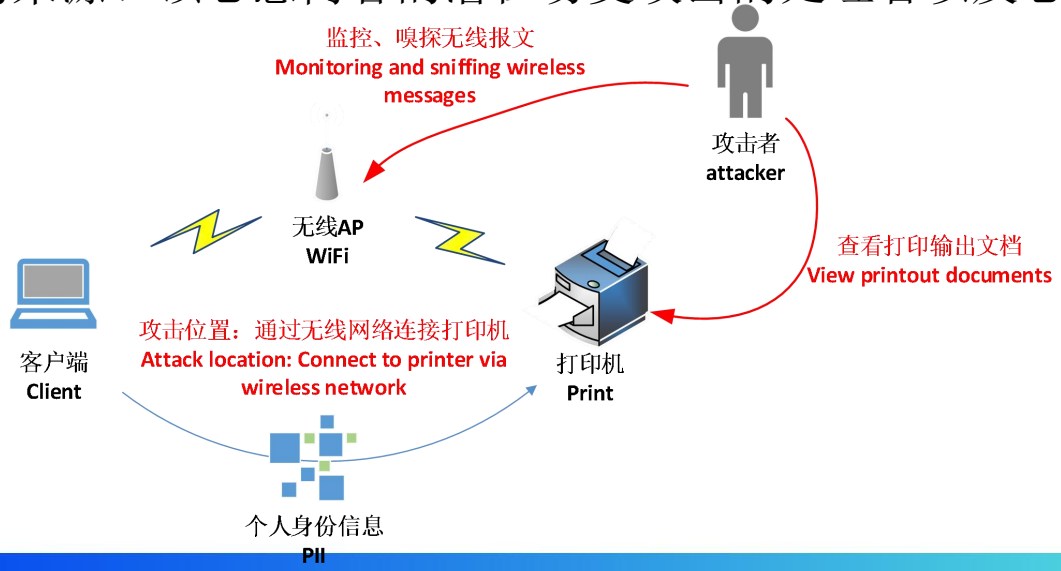
人员
personnel

流程
process

以数据为中心的系统威胁建模
Data-Centric System Threat Modeling

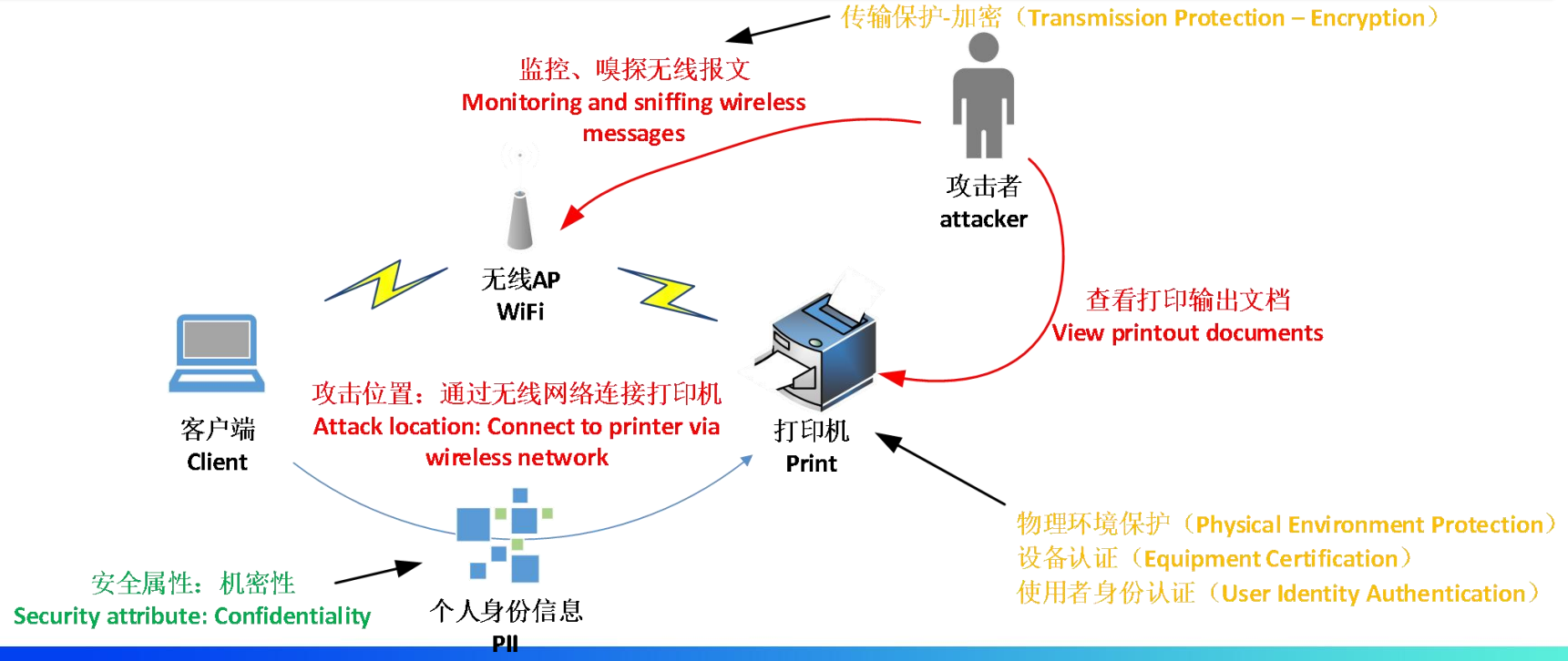
步骤 2：识别和选择要包含在模型中的攻击向量

- 攻击向量是攻击用来访问漏洞的整个路径的一部分。可以将每个攻击向量视为包含恶意内容的来源、该恶意内容的潜在易受攻击的处理者以及恶意内容本身的性质。



以数据为中心的系统威胁建模
Data-Centric System Threat Modeling

步骤3：描述用于减轻攻击向量的安全控制



以数据为中心的系统威胁建模
Data-Centric System Threat Modeling

步骤 4：分析威胁模型

设定以下分数并平均权衡：

- 无安全控制有效性 = 0
- 安全控制有效性低 = 1
- 安全控制效果中等 = 2
- 安全控制有效性高 = 3
- 负面值高 = 1
- 中等的负面含义 = 2
- 低的负面含义 = 3

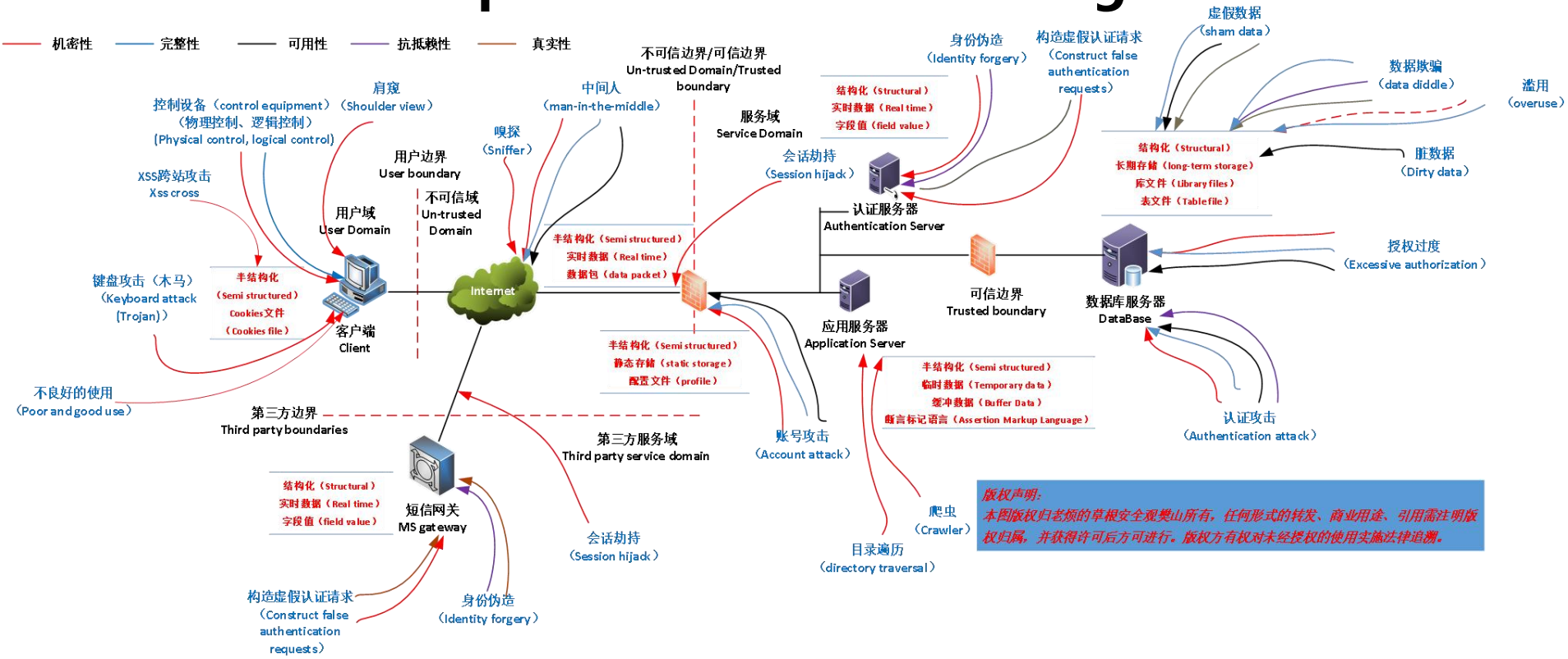
组织计算每个安全控制的负面影响分数的总和，然后将这些总和乘以每个攻击向量的安全控制有效性的分数以获得每个攻击向量的分数 /security（安全）控制对。分数越高，安全控制针对相应攻击向量提供的“资金回报”就越多。

以数据为中心的系统威胁建模
Data-Centric System Threat Modeling

步骤 4：分析威胁模型

可能的安全控制	采购和实施成本	年度管理/维护成本	对功能的影响	对可用性的影响	对性能的影响	安全控制总计
需要强密码和强加密密码散列	3	3	3	3	3	15
需要多因素身份验证	2	2	3	2	3	12
使用杀毒软件、垃圾邮件过滤、实时黑名单、用户感知、网络信誉软件等	2	2	2	2	2	10
补丁漏洞	2	2	2	3	2	11

威胁建模下的数据威胁地图
Data threat map under threat modeling



以数据为中心的系统威胁建模
Data-Centric System Threat Modeling

域	组件	位置	存储形式	数据类型	安全属性	攻击向量描述	对抗手段
用户域	PC终端	外存	Cookies文件	★半结构化 ★临时数据	★机密性 ★完整性	★设备被控制 ★滥用 ★肩窥 ★Xss跨站导致cookies文件泄露 ★键盘攻击（木马） ★不良好的使用	★终端认证（双因素认证） ★防病毒/恶意代码 ★Cookies保护（开发侧） ★安全意识
服务域	通信	通信介质	数据包	★半结构化 ★实时数据	★机密性 ★完整性 ★可用性	★嗅探 ★中间人	★传输加密
	边界防火墙	外存	配置文件	★半结构化 ★静态存储	★机密性 ★完整性 ★可用性	★账号攻击	★强口令设置 ★关闭远程管理端口
	应用服务器	硬盘	断言标记语言	★半结构化 ★临时数据 ★缓冲数据	★机密性	★爬虫 ★目录遍历	★配置管理 ★安全断言标记语言 ★安全开发控制
	认证服务器	外存 内存	字段值	★结构化 ★实时数据	★机密性 ★完整性 ★可用性 ★抗抵赖性 ★真实性	★身份伪造 ★构造虚假认证请求 ★劫持	★零信任机制 ★多因素身份认证 ★签名认证
	数据库服务器	外存	库文件 表文件	★结构化 长期存储	★机密性 ★完整性 ★可用性 ★抗抵赖性 ★真实性 ★数据质量 ★可靠性	★虚假数据 ★数据欺骗 ★脏数据 ★认证攻击 ★授权过度 ★滥用 ★数据损坏 ★非标准数据 ★数据来源不可信 ★数据请求不可信	★密码技术 ★区块链技术（云环境下） ★去标识化 ★数据标准 ★授权管理 ★源认证 ★零信任机制 ★数据验证 ★容灾备份
第三方服务域	短信网关服务器	外存 内存	字段值	★结构化 ★实时数据	★机密性 ★完整性 ★可用性 ★抗抵赖性 ★真实性	★身份伪造 ★构造虚假认证请求 ★劫持 ★响应虚假请）	★零信任机） ★多因素身份认证 ★签名认证

基于数据的威胁建模接口描述

威胁模型视角下的数据安全治理概述

Overview of data security governance from a threat model perspective

1 访问控制	2 意识和培训	3 审计和问责	4 配置管理	5 身份验证
6 事件响应	7 维护	8 介质保护	9 人员安全	10 物理保护
11 风险评估	12 安全评估和监控	13 系统和通信保护	14 系统和信息完整性	15 规划
16 系统和服务采购	17 供应链风险管理			

NIST SP 800-171Ar3 ipd Assessing Security Requirements for Controlled Unclassified Information

威胁模型视角下的数据安全治理概述

Overview of data security governance from a threat model perspective

访问控制	意识和培训	审计和问责	配置管理	身份验证	事件响应	维护	介质保护
账户管理	素养培训和意识	事件日志	基线配置	用户识别、身份验证和重新身份验证	事件响应计划和处理	维护工具	介质存储
访问执行	基于角色的培训	审核记录内容	配置设置	设备识别和认证	事件监测、报告和响应协助	非本地维护	介质访问
信息流执行		审计记录生成	配置变更控制	多因素认证	事件响应测试	维护人员	介质消毒
职责分离		对审计日志记录过程失败的响应	影响分析	防重放认证	事件响应培训		介质标记
最小特权		审计记录审查、分析和报告	变更访问限制	标识符管理			介质传输
最小特权-特权账户		审核记录裁剪和报告生成	功能最少	密码管理			介质使用
最小特权-特权功能		时间戳	授权软件-例外情况下允许	认证反馈			系统备份-密码保护
登录尝试失败		审计信息的保护	系统组件清单	身份验证程序管理			
系统使用通知			信息定位				
设备锁定			高风险区域的系统和组件配置				
会话终止							
远程访问							
无线接入							
移动设备的访问控制							
外部系统的使用							
公众可访问内容							

威胁模型视角下的数据安全治理概述

Overview of data security governance from a threat model perspective

人员安全	物理保护	风险评估	安全评估和监控	系统和通信保护	系统和信息完整性	计划	系统和服务采购	供应链风险管理
人员筛选	物理访问授权	风险评估	安全评估	边界保护	缺陷修复	政策和程序	采购流程	供应链风险管理计划
人员终止和调动	监控物理访问	漏洞监控和扫描	行动计划和里程碑	共享系统资源中的信息	恶意代码保护	系统安全计划	不支持的系统组件	采购策略、工具和方法
	备用场地		持续监测	网络通信-默认拒绝-例外允许	安全警报、咨询和指令	行为规则	外部系统服务	供应链要求和流程
	物理访问控制		信息交流	传输和存储保密	系统监控			
	传输和输出设备的访问控制			网络断开	信息管理和保留			
				机密密钥的建立和管理				
				密码保护				
				协作计算设备和应用程序				
				移动代码				
				会话真实性				

网安加社区

www.cwasp.cn