聚·变

第二届顺丰信息安全峰会分论坛

AI安全与及隐私保护(2)

构建结构化数据安全纵深防护体系

刘玉霞 顺丰信息安全

结构化数据

行数据，存储在数据库里，可以用二维表结构来逻辑表达实现的数据

数据产生-流转-使用过程

业务场景

客户下单

订单处理

售后服务

数据分析

系统维护

数据风险点

用户使用

节点间传输

后端存储

结构化数据安全纵深防护体系架构

应用数据安全

创建	存储	传输	访问	使用
• 数据分类，分级 • 数据识别 • 数据标记	• 字段/列级别加密 • 备份加密	• 受信通道 • 上下游鉴权 • 通道/内容加密	• 用户鉴权 • 功能/数据权控	• 查询脱敏 • 导出脱敏 • 测试脱敏

监控 审计，阻断

应用系统安全

源代码检测 | 自动化漏洞检测 | 人工渗透测试 | 顺丰SRC | ……

基础设施安全

网络设施安全 | 存储设施安全 | 计算设施安全 | 终端安全 | ……

物理与环境设施安全

创建	存储	传输	访问	使用
• 数据分类，分级 • 数据识别 • 数据标记	• 字段/列级别加密 • 备份加密	• 受信通道 • 上下游鉴权 • 通道/内容加密	• 用户鉴权 • 功能/数据权控	• 查询脱敏 • 导出脱敏 • 测试脱敏

监控 审计，阻断

创建-数据分类，分级

数据分类

在大类下划分中类，在中类下划分小类；按业务或组织分类

员工信息

- 联系电话 **
- 地址 **
- 身份证号码 ***
- 银行卡号 **
- 薪酬 ***
- ……

客户信息

- 姓名 *
- 地址 **
- 联系方式 ***
- 金额 ***
- 商品 *
- ……

数据分级

绝密、机密、内部、公开

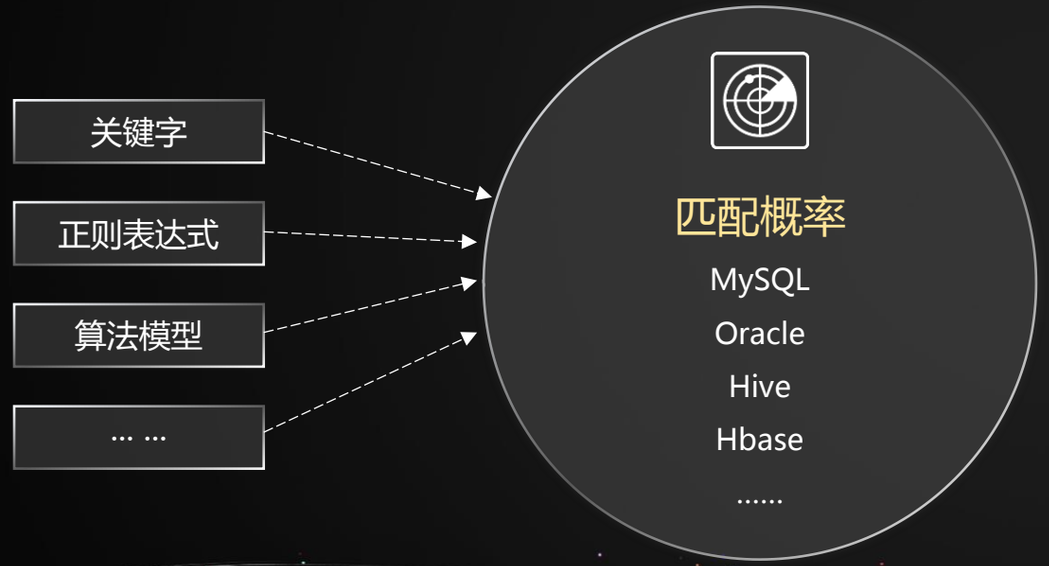
财务信息

- 预算 ***
- 报表 ***
- 结算信息 ***
- 纳税信息 **
- 薪酬福利 **
- ……

…… ……

创建-敏感数据发现，标记

你无法保护你找不到的东西，如何识别敏感数据并实施针对性的保护，是进行数据保护的重要基础工作



- 从数据库中发现敏感数据
- 按行数或比例匹配
- 精确到数据库名，表名，字段名
- 按字段进行标记

创建-数据识别，标记

- 姓名
- 电话
- 地址
- 英文地址
- 邮箱
- 银行卡号
- 企业名称
- 营业执照号码
- 组织机构代码
- 纳税人识别码
- ……

创建	存储	传输	访问	使用
• 数据分类，分级 • 数据识别 • 数据标记	• 字段/列级别加密 • 备份加密	• 受信通道 • 上下游鉴权 • 通道/内容加密	• 用户鉴权 • 功能/数据权控	• 查询脱敏 • 导出脱敏 • 测试脱敏

监控 审计，阻断

存储-敏感加密

存储加密是数据安全保护的最后一道防线，也是防止拖库等批量泄密的最有效措施

加密层次

硬盘加密

文件加密

数据库全库加密

数据库字段加密

加密方式

软加密

硬件加密

密码体制

密码体制	特点	安全目标	常用算法
对称密码	• 加密和解密的密码相同 • 加密速度较快 • 长文本的加密	机密性	国密SM1/SM4 通用DES/3DES/AES
非对称密码	• 加密和解密的密码不相同 • 加密速度较慢 • 对称密码保护和数字签名	机密性 不可抵赖性	国密SM2 通用RSA
杂凑密码	• HASH密码 • 计算消息摘要值 • 不可逆	完整性	国密SM3 通用MD5/SHA1/SHA256/SHA384/SHA512

存储-敏感加密

加密存储的落地，需要有一个适合的加密方案，我们以快递中的客户电话为例

创建	存储	传输	访问	使用
• 数据分类，分级 • 数据识别 • 数据标记	• 字段/列级别加密 • 备份加密	• 受信通道 • 上下游鉴权 • 通道/内容加密	• 用户鉴权 • 功能/数据权控	• 查询脱敏 • 导出脱敏 • 测试脱敏

监控 审计，阻断

传输-鉴权，加密

数据传输包括节点之间及客户端与服务器之间的数据传输，不同场景采取不同的保护策略。

授信通道

网络专线

- 端到端的物理链路
- 价格贵

VPN专线

- 虚拟专线
- 隧道技术、加解密技术、密钥管理技术和使用者与设备身份认证技术

上下游鉴权

OAuth2.0

- 第三方授权

Token

- 可扩展
- 适用于移动应用
- 基于标准化

Cookie-session

- 扩展受限
- 跨站请求伪造攻击

加密

通道加密

- 防止传输过程中参数被篡改
- HTTPS

内容加密

- 重要的数据传输
- 通过加密内容达到双层保证
- 加密方式，可根据接口的重要程度来选择
- 如哈希算法md5、对称加密的DES、非对称的RSA、加盐加密

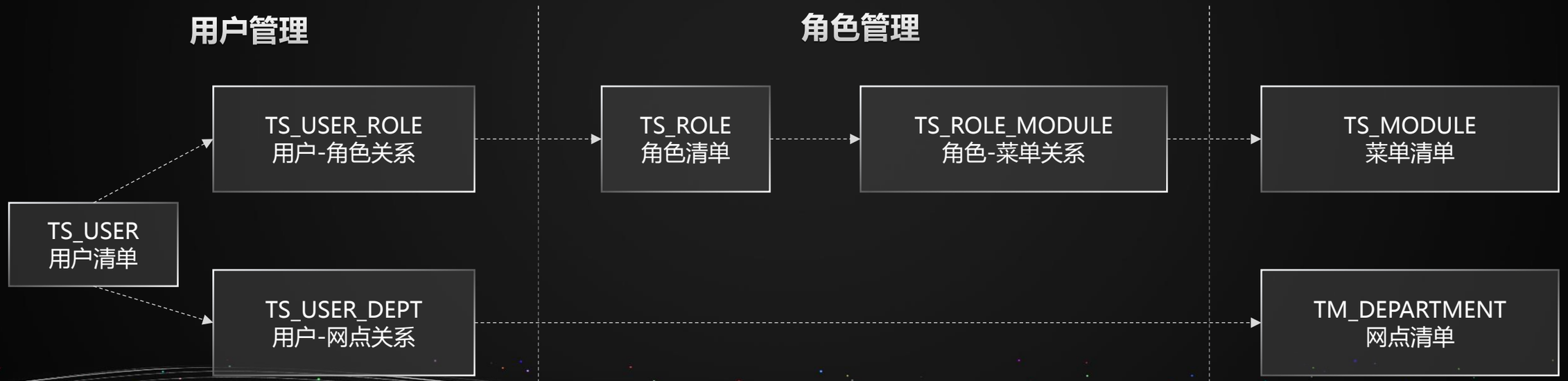
创建	存储	传输	访问	使用
• 数据分类，分级 • 数据识别 • 数据标记	• 字段/列级别加密 • 备份加密	• 受信通道 • 上下游鉴权 • 通道/内容加密	• 用户鉴权 • 功能/数据权控	• 查询脱敏 • 导出脱敏 • 测试脱敏

监控 审计，阻断

访问-鉴权，权控

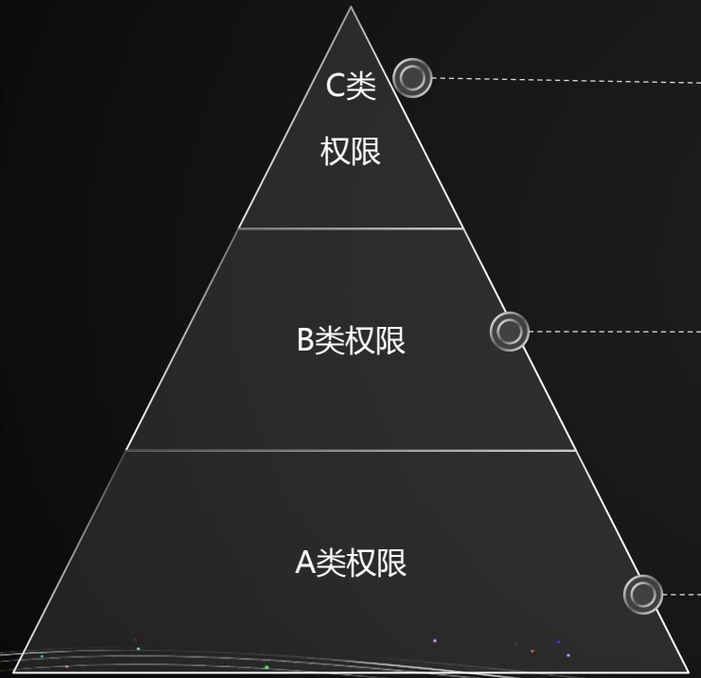
鉴权是防护数据安全的第一道关卡，通过鉴权确保访问者安全。权控是防止系统敏感资源滥用或非法使用。

RBAC基于角色的权限访问控制，权限与角色相关联，用户通过成为适当角色的成员而得到这些角色的权限。



访问-鉴权，权控

对于每个职位/岗位，权限都被划分为A、B、C三个级别进行管理。



- **含义**：非A、B类的即为C类，存在较高风险的权限（严控）
- **管理模式**：用户无法自行申请，需要由流程审批人员代用户提交申请，审批节点不变

- **含义**： 在满足内控要求的前提下，因特殊工作安排所需（受限）
- **管理模式**：用户自行提交申请，直属上级和流程审批人审批

- **含义**：符合岗位职责内的工作需要（合规）
- **管理模式**：无需申请，入职后自动开通

创建	存储	传输	访问	使用
• 数据分类，分级 • 数据识别 • 数据标记	• 字段/列级别加密 • 备份加密	• 受信通道 • 上下游鉴权 • 通道/内容加密	• 用户鉴权 • 功能/数据权控	• 查询脱敏 • 导出脱敏 • 测试脱敏

监控 审计，阻断

使用-脱敏

数据脱敏又称数据去隐私化或数据匿名化或数据变形，是在保留数据原始特征的条件下

脱敏类型

静态脱敏

非生产环境

开发、测试、培训、分析等场景

动态脱敏

生产环境

用户访问敏感数据即时进行脱敏

脱敏方式

可逆

置换，置换规则或映射表

加密，公开加密算法

不可逆

遮挡，隐藏部分

乱序，打乱顺序

浮动，向上或向下浮动

偏移，范围内偏移

截断，截断部分信息

清空，直接清空

考虑因素

保持数据业务属性

保留数据有效性，银行卡、身份证等

保持数据完整性

保留数据字段长度、格式，11位手机号

可逆性

可恢复原始数据

完备性

防止使用非敏感数据重构敏感数据

使用-脱敏

数据脱敏实现，需要理清两个问题：1）明确哪些数据需要脱敏 2）根据数据使用场景、使用目的，选择合适的脱敏方法

非生产环境场景，静态脱敏方案

使用-脱敏

生产环境场景，静态脱敏方案

用户

下单　　订单查询

售后服务人员

身份确认　　联系客户　　查询检索

创建	存储	传输	访问	使用
• 数据分类，分级 • 数据识别 • 数据标记	• 字段/列级别加密 • 备份加密	• 受信通道 • 上下游鉴权 • 通道/内容加密	• 用户鉴权 • 功能/数据权控	• 查询脱敏 • 导出脱敏 • 测试脱敏

监控 审计，阻断

总结

Q 哪些是敏感数据？	A 数据分类，分级
Q 敏感数据在哪里？	A 数据发现，标识
Q 数据保存安全吗？	A 数据存储加密
Q 数据怎么流转？流转过程安全吗？	A 可信通道传输，鉴权，加密
Q 哪些人在使用这些数据？这些人合法吗？使用是合规吗？	A 数据访问鉴权，权控，脱敏
Q 异常访问怎么发现？发现了，能阻断吗？	A 安全审计，阻断

数据安全是一项综合工程，需要全路径，全生命周期去保护

THANK YOU