标题：数据安全架构设计与实战

来源：郑云文.数据安全架构与实战.机械工业出版社，2019-09.微信读书

编辑时间：2020.06.09

目录：

正文：

1 安全架构

* 架构的定义：架构 = 元素（组件或逻辑模块） + 关系
* 三层架构：用户，用户接口层，业务逻辑层，数据访问层
* 架构关注的问题：
  + 产品功能：对功能模块、组件进行分割组装，保障模块及组件之间高内聚低耦合
  + 产品质量：性能，安全性，扩展性， 可维护性
* 安全的目标CIA：机密性、完整性、可用性
* 安全概念演变：信息安全、网络安全、数据安全
* 安全架构的概念：架构在安全性上细分的领域
  + 产品安全架构：不依赖外部防御系统的情况下，从源头实现产品安全
  + 安全技术体系架构：包括安全基础设施、安全工具和技术、安全组件与支持系统等，系统性地增强各产品的安全防御能力，构建第二道防线
  + 审计架构：独立的审计部门等提供风险发现能力，审计范围包括安全风险所在内的所有风险，构建第三道防线
* SDL：具备安全开发生命周期流程的企业中，通常会有系统架构师、安全架构师、运维架构师或数据库架构师等
* 安全架构5A方法论：
  + 身份认证：
  + 授权：授予用户主体允许或拒绝访问客体的权限
  + 访问控制
  + 可审计：形成可供追溯的操作日志
  + 资产保护：资产的机密性、完整性、可用性保障
* 主体：用户、员工、合作伙伴、访客等、设备、系统
* 范围：从应用层扩展到空间立体、覆盖物理和环境层、网络和通信层、设备和主机层、应用和数据层
* 数据：即信息资产
  + 结构化数据：数据库、缓存、Key-value存储系统等
  + 非结构化数据：文档、图片、音频、视频等
  + 非存储数据：使用、传输、流转中的数据
* 资源：网络资源、计算资源、存储资源、进程、产品功能、网络服务、系统文件等
* 可审计的范围：
  + 身份认证：用户登录时间、源IP、用户ID、访问的目标应用等
  + 授权：权限申请流程的每个审批环节，IP地址、用户ID、理由、通过或驳回的动作
  + 访问控制：通过或驳回结果、对敏感资产的每一个请求及动作
  + 资产保护：访问资产、查询、添加、修改、删除等操作

2 产品安全架构

* 典型架构：三层架构、BS架构、CS架构、SOA和微服务架构
* 典型框架：.net framework、spring、Django
* 数据访问层：数据库口令只在一个地方出现，且加密存储，通常为配置文件
  + DAL（数据访问层）编码：自定义编码，采用数字证书，并对数字证书私钥进行加密保护
  + ORM框架：将关系数据库中的一行记录，与业务逻辑层中的一个对象建立关联
  + DB Proxy：一种数据库访问中间件，包扩读写分离、分库分表、收敛访问路径（所有访问数据库的流量都经过DB Proxy）、收敛数据库账号（数据库账号只在DP Proxy上加密存储）、参数检查
  + 数据服务简化DAL：将数据库封装为数据服务，基于协议进行通信

3 身份认证

* 身份认证：
  + 对人的身份认证：单点登录
    - 会话机制：一次Token
    - 全程Token机制
* 持续的消息认证机制：每次请求都执行身份认证
  + 后台间身份认证
  + 对设备的身份认证

4 授权

* 授权原则与方式：
  + 基于属性：属性规则表
  + 基于角色：业务管理员、审计员、审批、非自然人账号
  + 基于任务：临时授权
  + 基于ACL（自主访问控制）
  + 动态授权
* 授权的风险：无授权机制、未授权、平行授权或垂直授权、交叉授权、诱导授权、职责未分离
* 授权漏洞的发现与改进：
  + 交叉测试法：用户使用自己的权限访问其他用户的数据
  + 漏洞改进：内建授权模块、外部权限管理系统

6 访问控制

* 访问控制三要素：
  + 主体：用户、管理员、系统调用方法等
  + 客体：资源、数据、文件、功能、设备、终端等
  + 访问控制策略：规则
* 访问控制策略：
  + 基于属性的访问控制
  + 基于角色的访问控制
  + 基于任务的访问控制
  + 基于ACL的访问控制
  + 基于专家知识的访问控制
  + 强制访问控制

7 可审计

* 审计的目的：
  + 发现产品自身的安全缺陷，改进安全特性，消除安全隐患
  + 为安全防御体系的改进提供支持
  + 为诉讼或其他法律行动提供证据
  + 满足监管或外部认证的合规要求
* 操作日志的内容：
  + 记叙文四要素：时间、地点、任务、事件
  + 日志记录：时间、IP地址、用户ID、操作、操作对象
* 常见的操作和操作对象：
  + 对数据：新增、删除、修改、查询
  + 对资源：申请、释放、扩容、授权
  + 对流程：审批通过、驳回、转移
  + 对交易：发起、支付、撤销
  + 对人员授权、吊销授权
* 日志的存储位置
  + 应用之外的日志管理系统，且无法从应用自身删除
* 日志保存期限：各种监管要求，一般至少保留六个月的操作日志；日志过期后自动清理

8 资产保护

* 数据安全存储：
  + 加密存储：敏感个人信息、个人隐私数据、用户生产内容；口令、加解密密钥、私钥；有明确检索、排序、求和等运算需求的业务数据
* 同态加密
* 数据安全传输：
  + HTTPS证书：DV证书（域名验证）、OV证书（组织验证）、EV证书（扩展验证）-用于在线交易、支付、金融等场景
  + 单域名或多域名证书：通过“使用者”字段指定域名
  + 通配型证书：\*表示任意子域名
* 数据展示与脱敏：密码：\*\*\*\*\*\*
  + 《个人信息保护法（草案）》：个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。
* 数据完整性校验：
  + 单向哈希、HMAC、AES-GCM、数字签名

9 业务安全（业务逻辑安全）

* 业务场景：
  + 交易支付：生成订单，付款时更改数据，然后上传付款凭据
  + 账号安全
    - 防弱口令撞库：不同业务中使用相同的口令；可通过频率限制、总量限制、IP锁定、验证码等技术手段
    - 防账号数据库泄露
    - 防垃圾账号：借助实名认证、邮件认证、手机认证、验证码认证等
    - 防账号找回逻辑缺陷：验证码
  + B2B交易安全：
    - 确认双方身份
    - 确认交易数据
    - 不可抵赖（甲方乙方）
  + 产品攻防能力：CC攻击（挑战黑洞），为绕过防DDOS的攻击形式，模拟大并发用户量
    - 网页静态化与缓存机制
    - 消息队列与异步机制：降低业务模块间的耦合、削峰平谷、提高并发能力
    - 负载均衡：CDN

10 安全技术体系架构简介

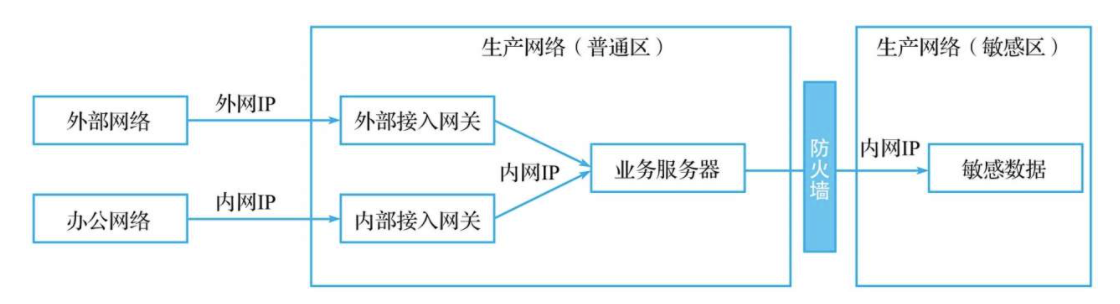
* 安全产品老三样：防病毒（主机层资产保护）、入侵检测（主机层入侵检测）、防火墙（网络层访问控制）
* 网络层延伸：网络接入认证、NAC（网络准入控制）、DDOS
* 主机层延伸：跳板机、自动化运维、大数据传输、HIDS
* 应用层延伸：统一接入网关、SSO、授权管理、WAF与接入网关集成（拦截SQL注入、XSS、上传）、KMS（密钥管理系统）
* 安全架构5要素的维度：
  + 应用和数据层
  + 设备和主机层
  + 网络和通信层
  + 物理和环境层

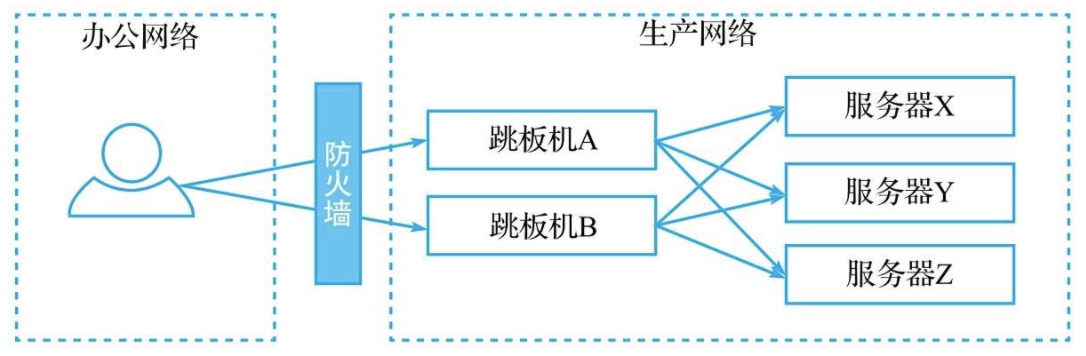


* 安全体系结构范围：
  + 安全基础设施：IT通用基础设施、安全防御基础设施（抗DDOS、HIDS、WAF等）、安全运维基础设施
  + 安全工具和技术：扫描、检测工具、加密、脱敏、HTTP等技术
  + 安全组件与支持系统：SSO、KMS、运维平台、第三方日志系统
* 风险管理的三道防线：
  + 业务部门：风险管理，从源头控制风险
  + 风险管理部门：数据安全管理部门、数据安全与隐私保护部等、安全技术架构
  + 独立的审计：识别前两者战略、管理政策、流程、人员、技术等；包括业务风险、管理文件、技术规范、控制措施覆盖等
* 数据安全技术团队的工作：
  + 建立和完善数据安全政策文件体系（在第四部分讲述）。制定其所在领域内的政策总纲、管理规定、标准、规范，供各业务遵循，提供专业性风险评估与指导，并对各业务的风险现状进行度量和监督，整体把控风险
  + 管理内外安全合规、认证测评、渗透测试
  + 协助建立/完善通用的基础设施，包括但不限于：较少的网络安全域划分与简洁的访问控制策略（借鉴无边界网络理念）、CMDB、统一接入网关等
  + 建立并完善安全相关的安全防御基础设施（抗DDoS/HIDS/WAF等）、安全运维基础设施（跳板机/运维平台/数据传输平台等）、安全支撑系统（SSO/日志/应用网关）、风险识别工具（如扫描器）、运营工具（风险度量等）
  + 建立并完善安全组件与支持系统，包括但不限于：SSO、权限管理、KMS、日志系统等
  + 完善各种安全工具和技术，包括但不限于：扫描、大数据分析（网关可作为流量输入）等
  + 考虑建设数据中台，将数据作为生产力，并统一执行安全管理
  + 例行开展扫描、检测活动，为风险数据化运营提供数据，执行风险规避措施。
  + 风险管理、事件管理与应急响应
* 网络部署架构：网络安全域、接入基础设施、访问控制策略
* 主机层安全：端口和服务、统一接入网关与WAF集成
* 应用层安全：身份认证、SSO单点登录、授权、访问控制、审计
* 数据层安全：加密存储、加密传输、脱敏

11 网络和通信层安全架构

* 网络和通信层基础设施：
  + 网络安全域：由路由器、交换机ACL、防火墙等封闭管理，逻辑上的区域
    - 不同组安全域之间存在访问规则，n个安全域之间需要n(n-1)套安全规则
    - 简单的安全域划分为办公网络和生产网络
    - 推荐的网络安全域





* + 网络接入身份认证：配合网络准入控制NAC机制使用
  + 网络接入授权
  + 防火墙及配套的防火墙策略管理系统
    - 网络准入控制
    - 生产网络主动连接外网的访问控制
  + 四层网关（NAT）
* 防御基础设施
  + 抗DDoS
  + 网络准入控制NAC
* 其他
  + 运维通道
  + 网络流量审计
* 备注：由于加密传输的普及，基于明文协议工作的产品，如IPS使用范围已大大受限