架构里看安全

互联网企业安全架构之思考

平安科技· 信息安全及内控部

李骁

lixiao484@pingan.com.cn

About Me

- 西北工业大学· 软件工程
- 上海交通大学· 信息安全工程
- 从开发转型安全，从客户端安全转型Web安全
- 台湾骇客年会HITCON 2013 Speaker
- OWASP 2013上海安全论坛Speaker
- 携程旅行网· 高级安全架构师
- 平安科技· 安全产品经理

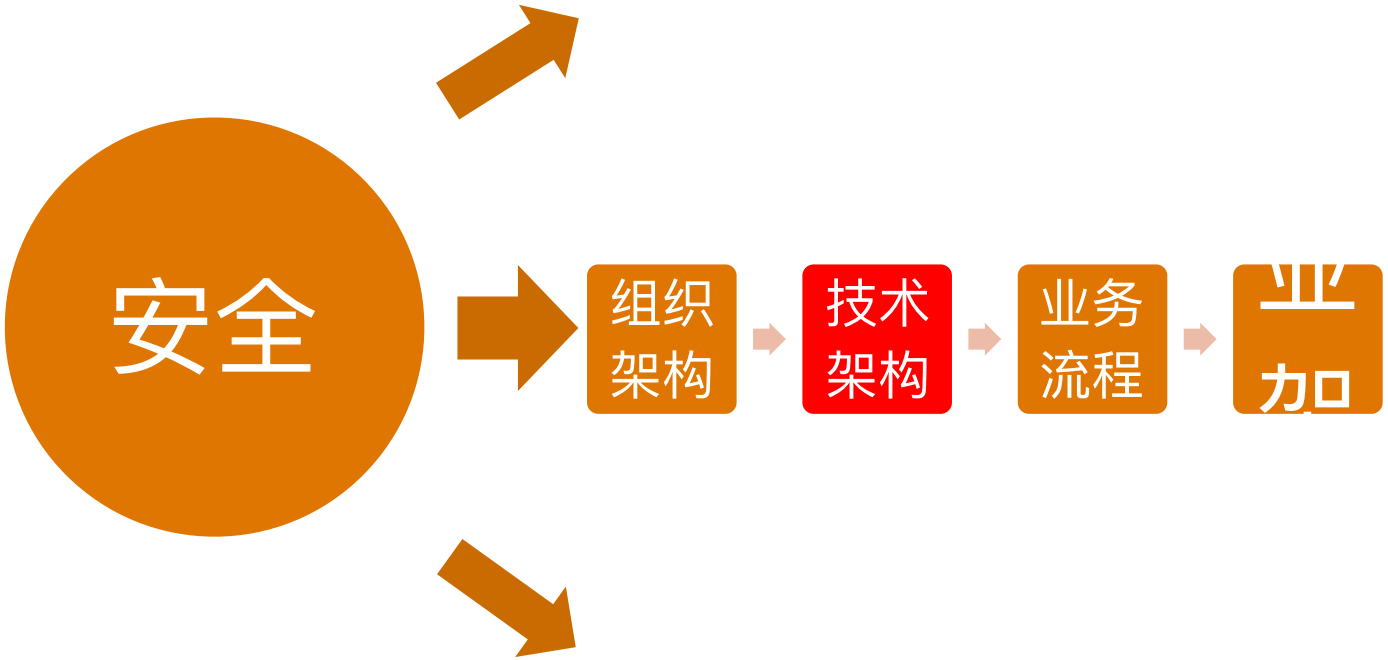
摘要

- 架构中看安全
  - 了解企业的架构
  - 安全与架构之职责
  - 安全与架构之关系
- 在架构中修复安全漏洞
- 安全架构建设实践
- 结语

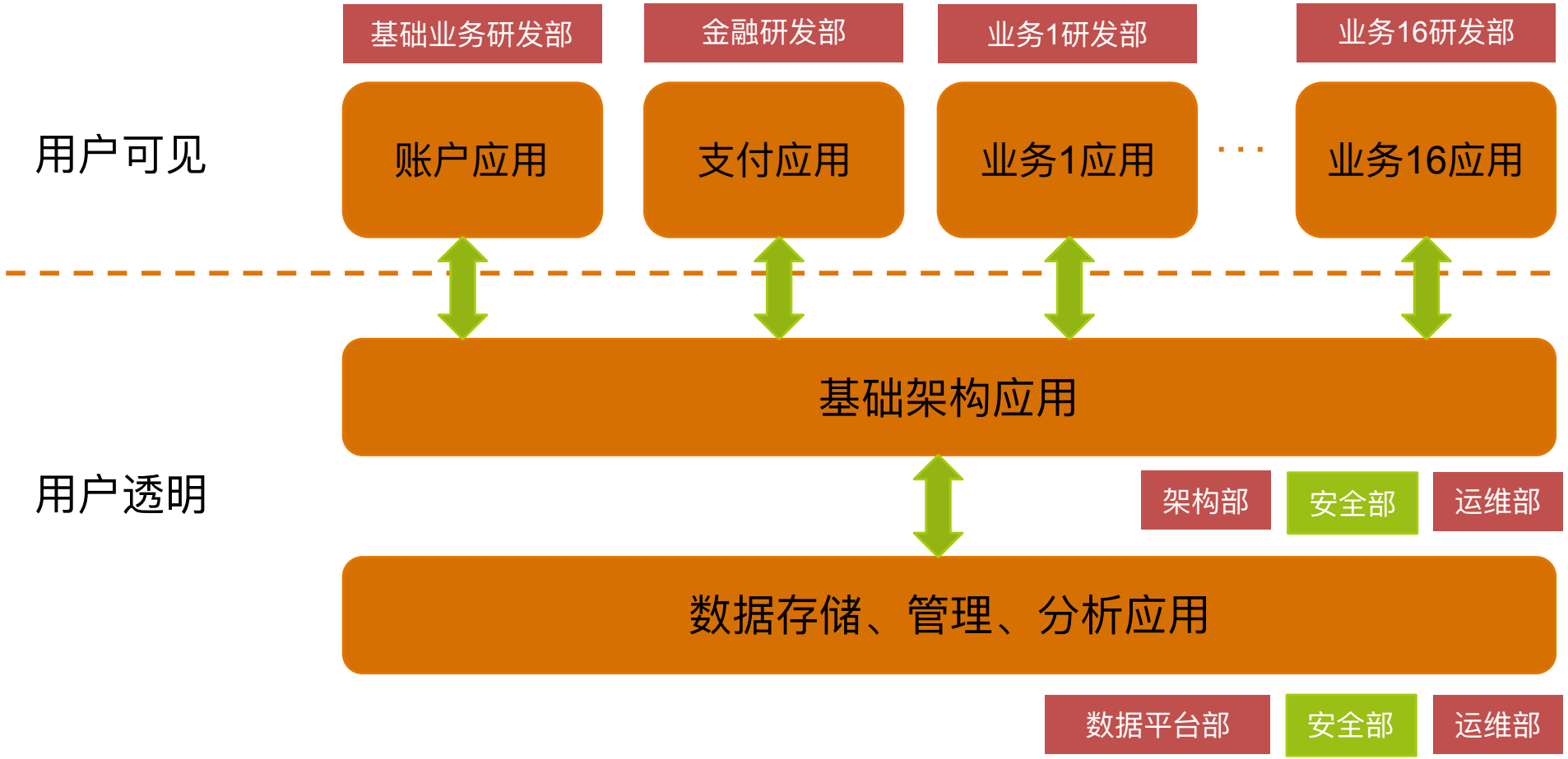
架构里看安全

“授人以鱼，不如授之以渔”

了解企业的架构



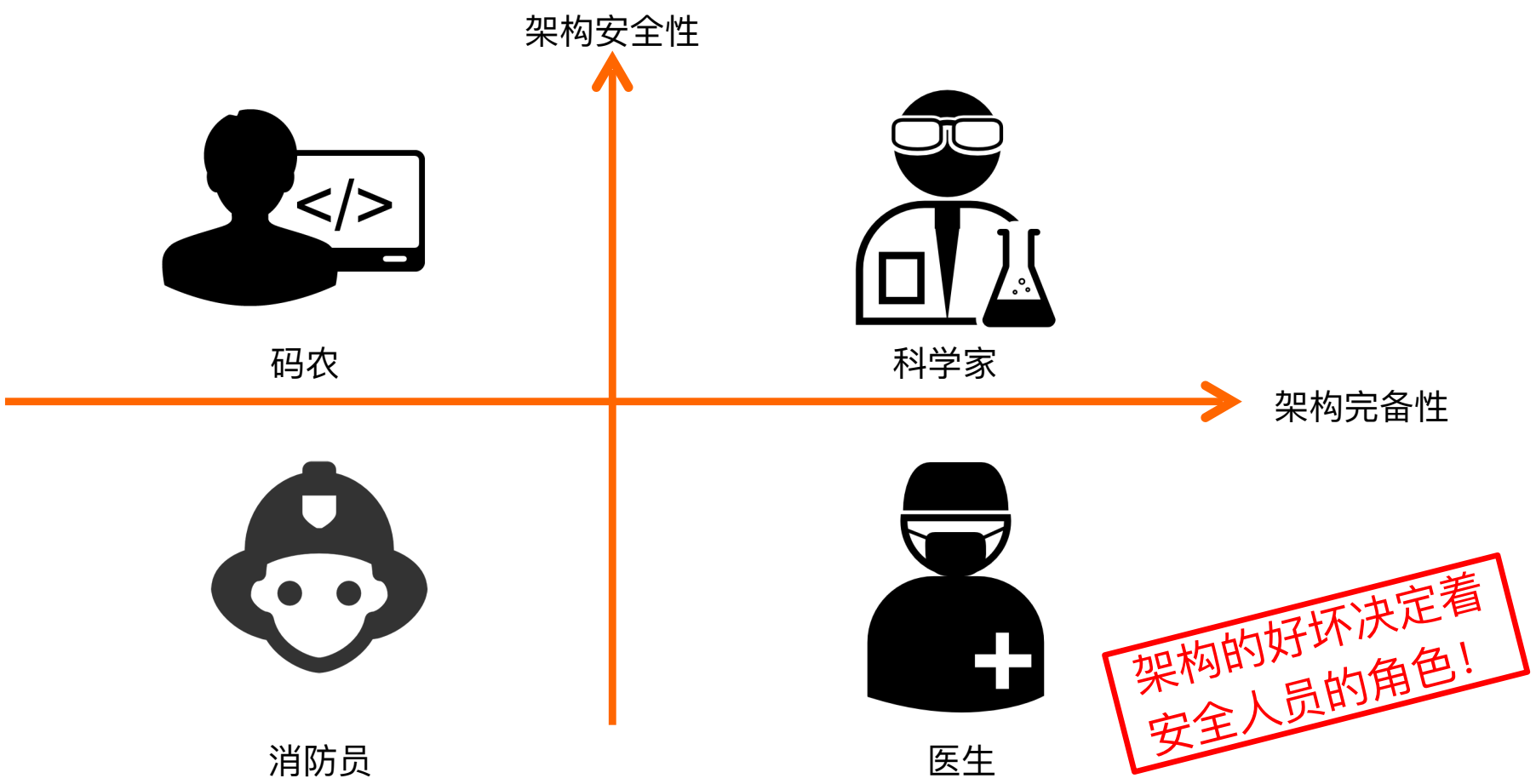
企业架构图


基础业务研发部
金融研发部
业务1研发部
业务16研发部
用户可见
账户应用
支付应用
业务1应用
...
业务16应用
基础架构应用
用户透明
架构部
安全部
运维部
数据存储、管理、分析应用
数据平台部
安全部
运维部

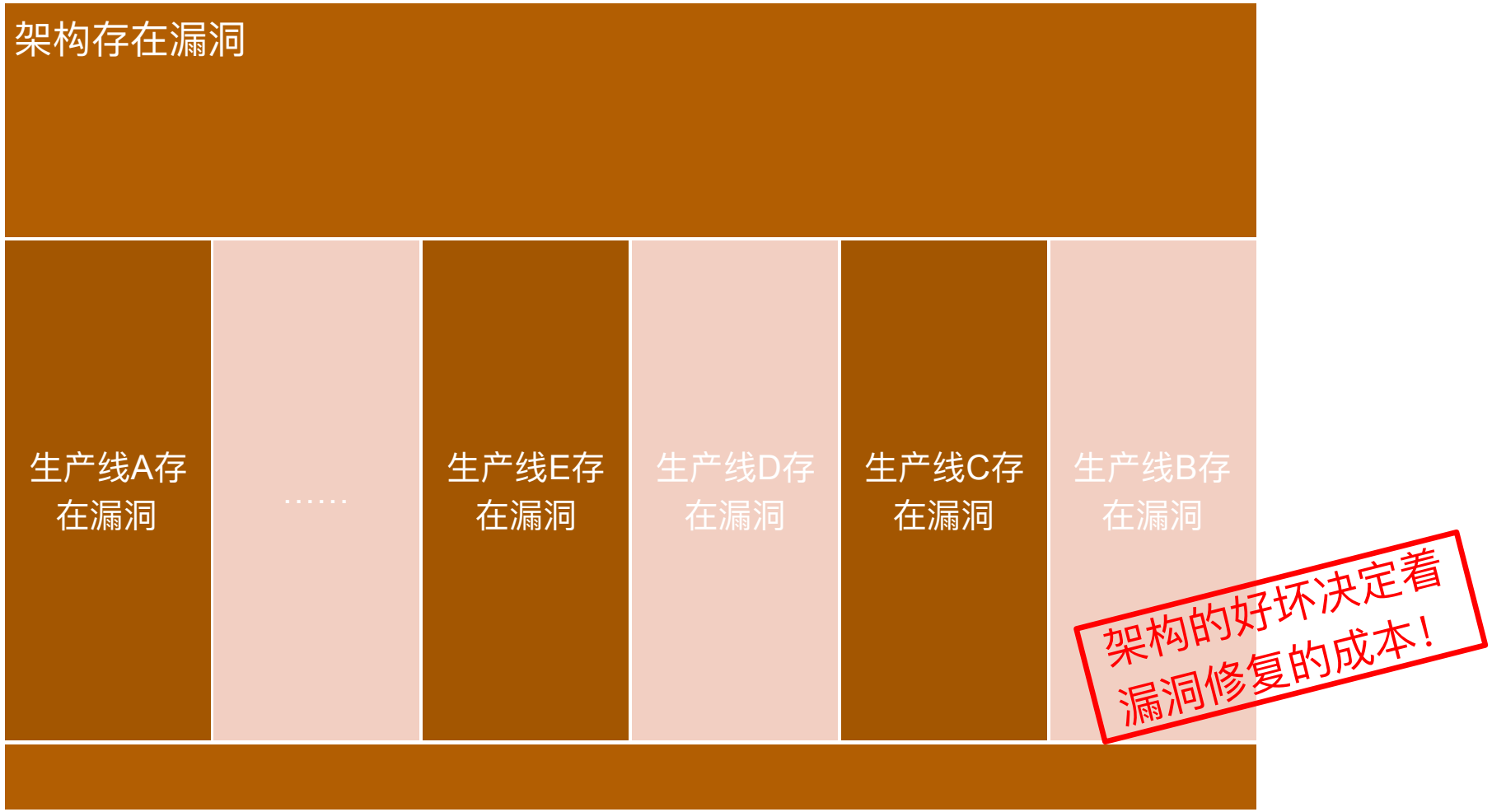
安全与架构之职责

- 安全
  - 漏洞挖掘与修复
  - 防御入侵、攻击
  - 安全审计/评估
  - 业务安全
  - …
- 架构
  - 为业务提供基础技术服务
  - 架构评估
  - 统一管理、统一运维

安全与架构之关系



安全与架构之关系


架构存在漏洞
生产线A存在漏洞
……
生产线E存在漏洞
生产线D存在漏洞
生产线C存在漏洞
生产线B存在漏洞
架构的好坏决定着漏洞修复的成本！

安全与架构之关系

好的架构使得安全建设事半功倍！

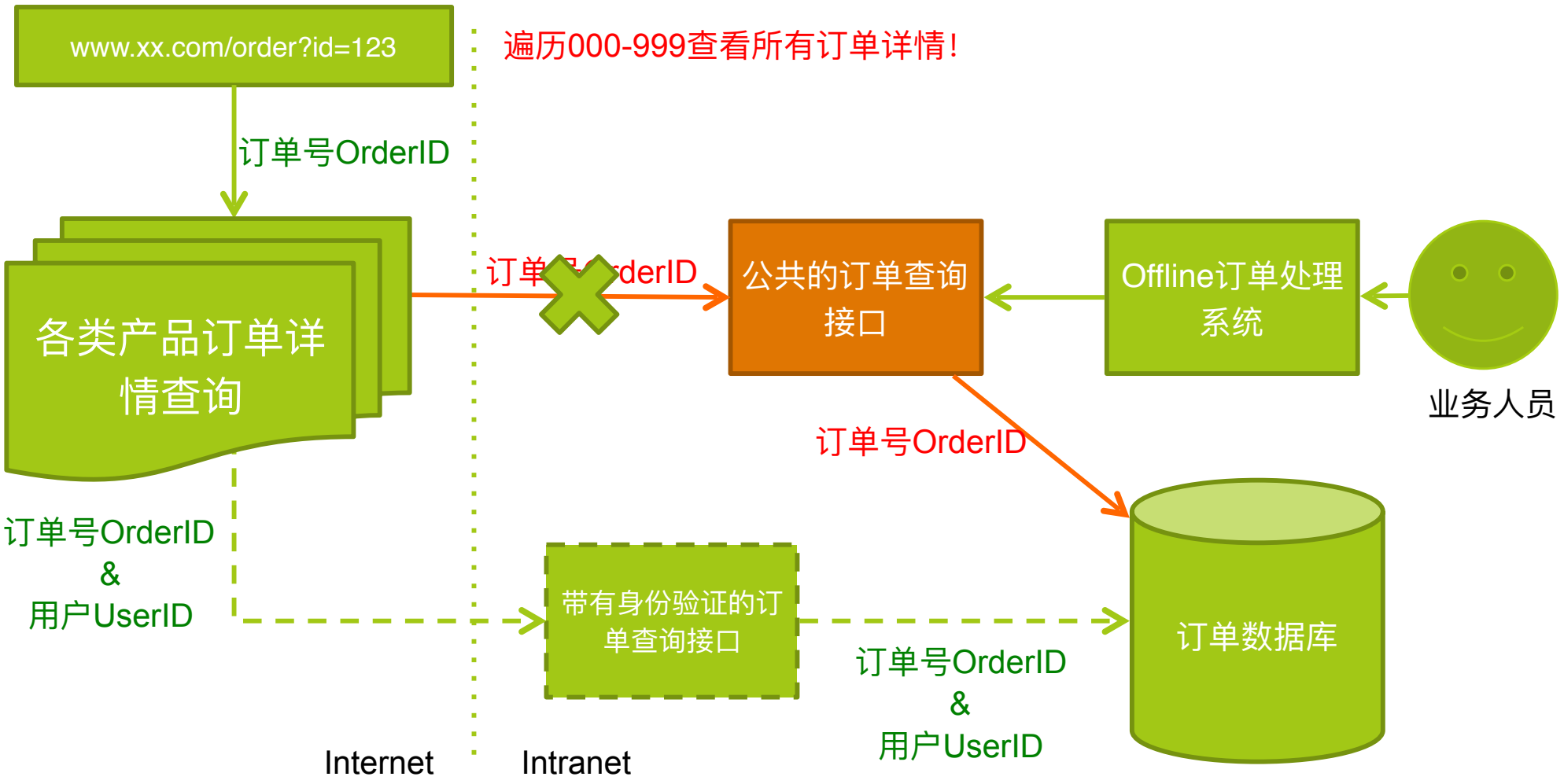
在架构中修复安全漏洞

“君有疾在腠理，不治将恐深”

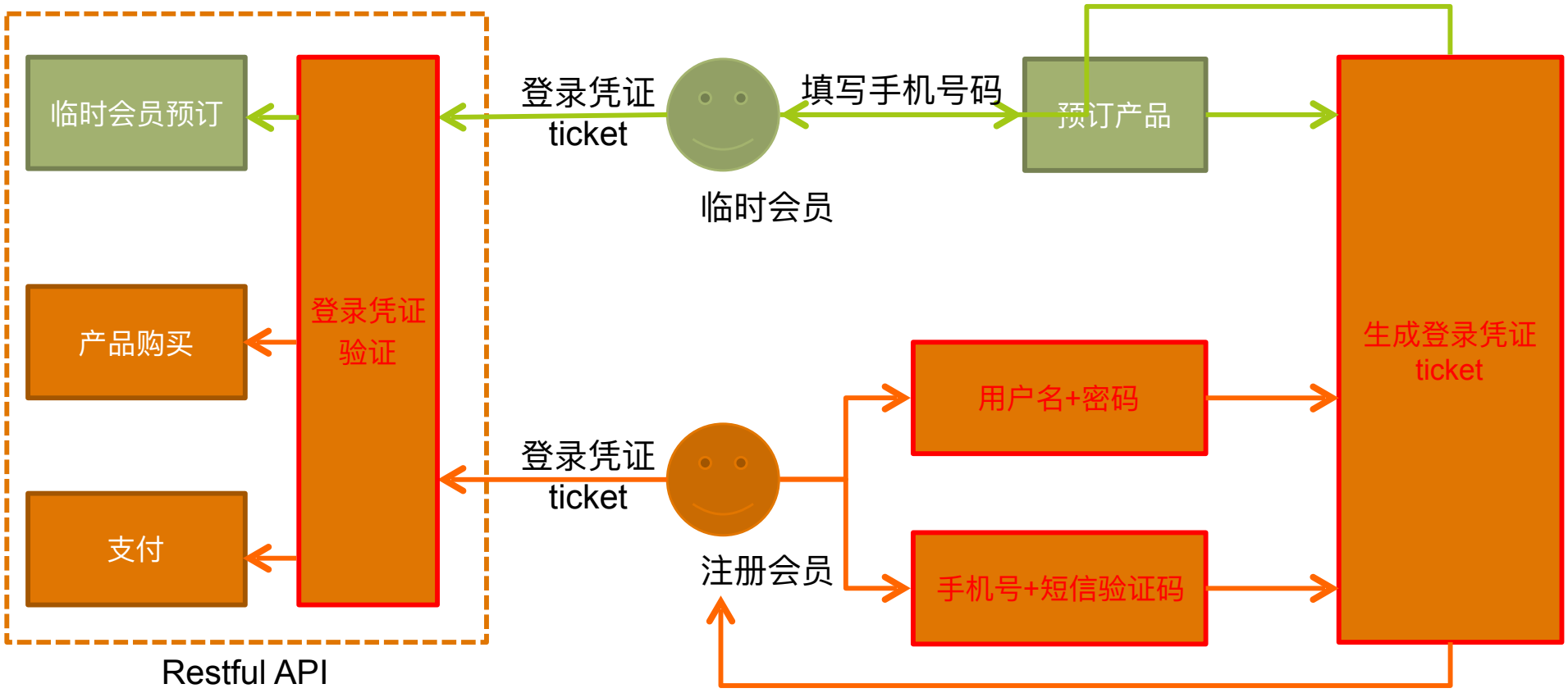
违反安全原则的架构设计

- 耦合性过高
  - 计算资源分配不均
  - 木桶原理，短板效应
- 用户权限未隔离
  - 水平权限: 同级别用户之间
  - 垂直权限: 不同级别用户之间
- 案例分析
  - Case1: 订单查询越权漏洞
  - Case2: 临时用户访问越权漏洞

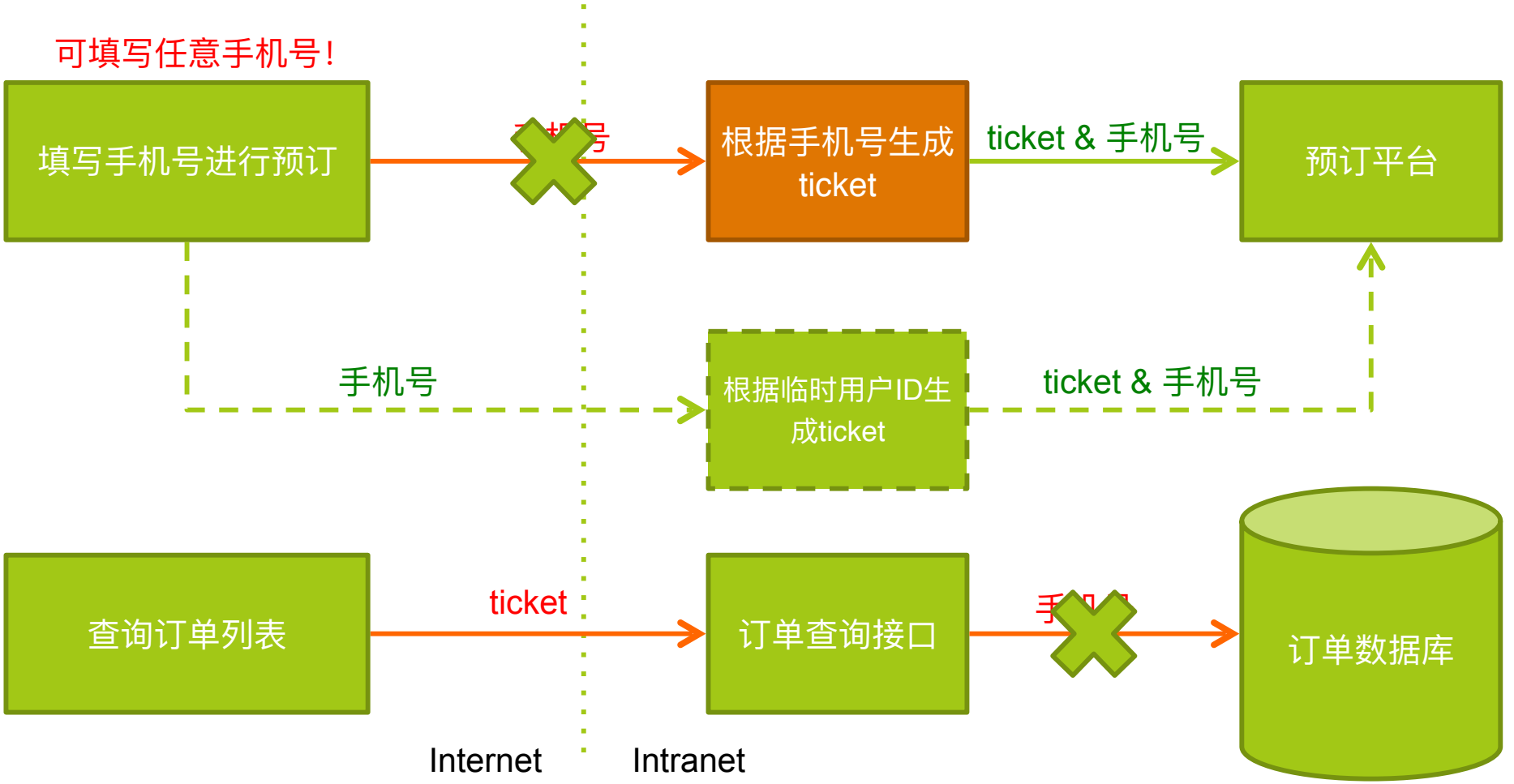
Case1示意图


www.xx.com/order?id=123
遍历000-999查看所有订单详情!
订单号OrderID
各类产品订单详情查询
公共的订单查询接口
Offline订单处理系统
业务人员
订单号OrderID
订单号OrderID
&
用户UserID
带有身份验证的订单查询接口
订单数据库
订单号OrderID
&
用户UserID
Internet
Intranet

Case2示意图一：登录流程



Case2示意图二：问题描述



经验与教训

Case1
- 涉及18个部门
- 花费40天修复

Case2
- 涉及3个部门
- 花费20天修复

- 架构缺陷带来的问题：漏洞修复成本极高
- 对于旧的系统，要进行排查、审计
- 对于新的系统，要做好架构评审工作
- 面对特殊业务，评估是否基础架构先行

收益
- 降低风险

成本
- 运维成本
- 研发成本
- 沟通成本

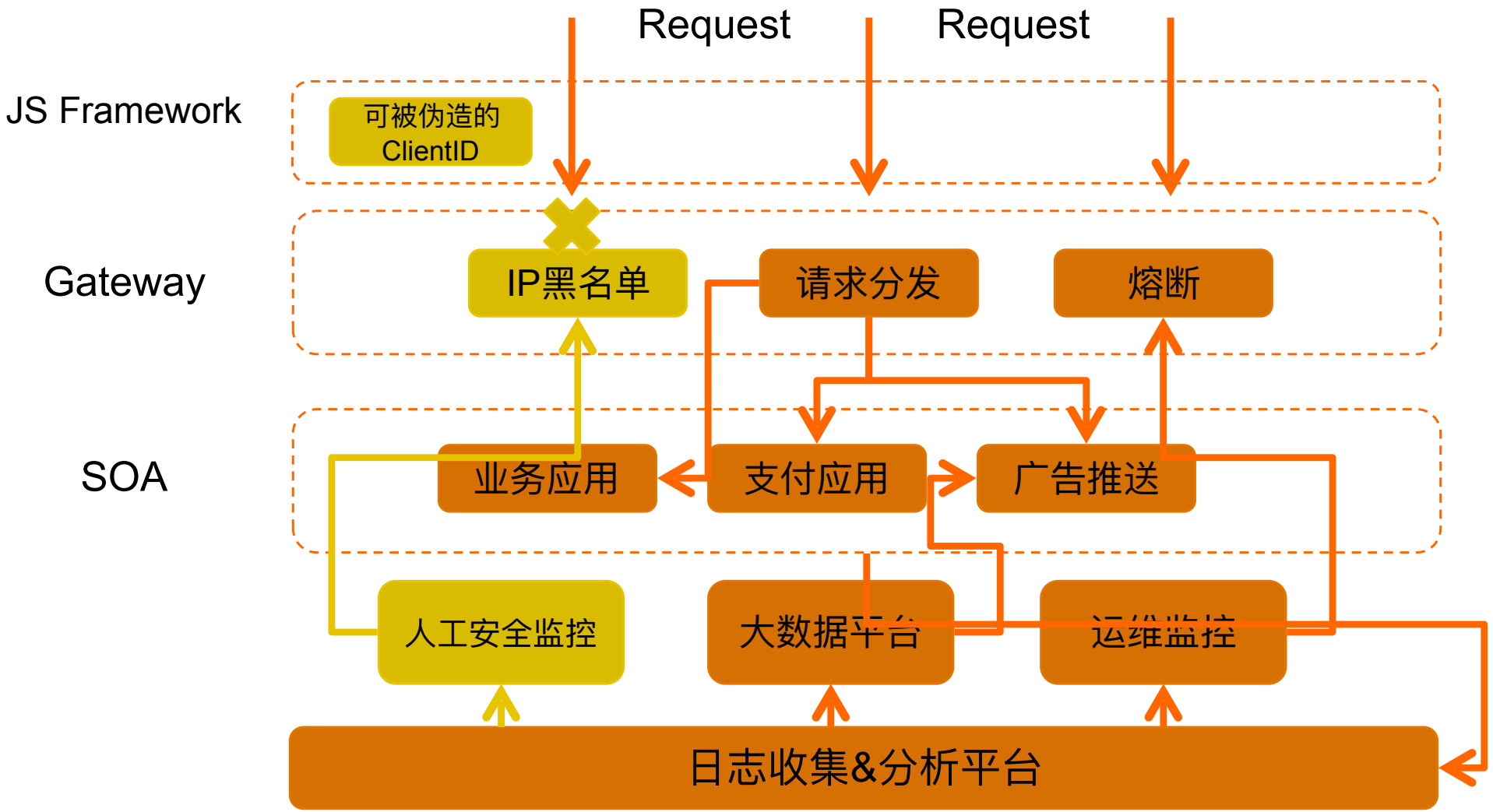
安全架构建设实践

“无他，唯手熟尔”

安全需求分析

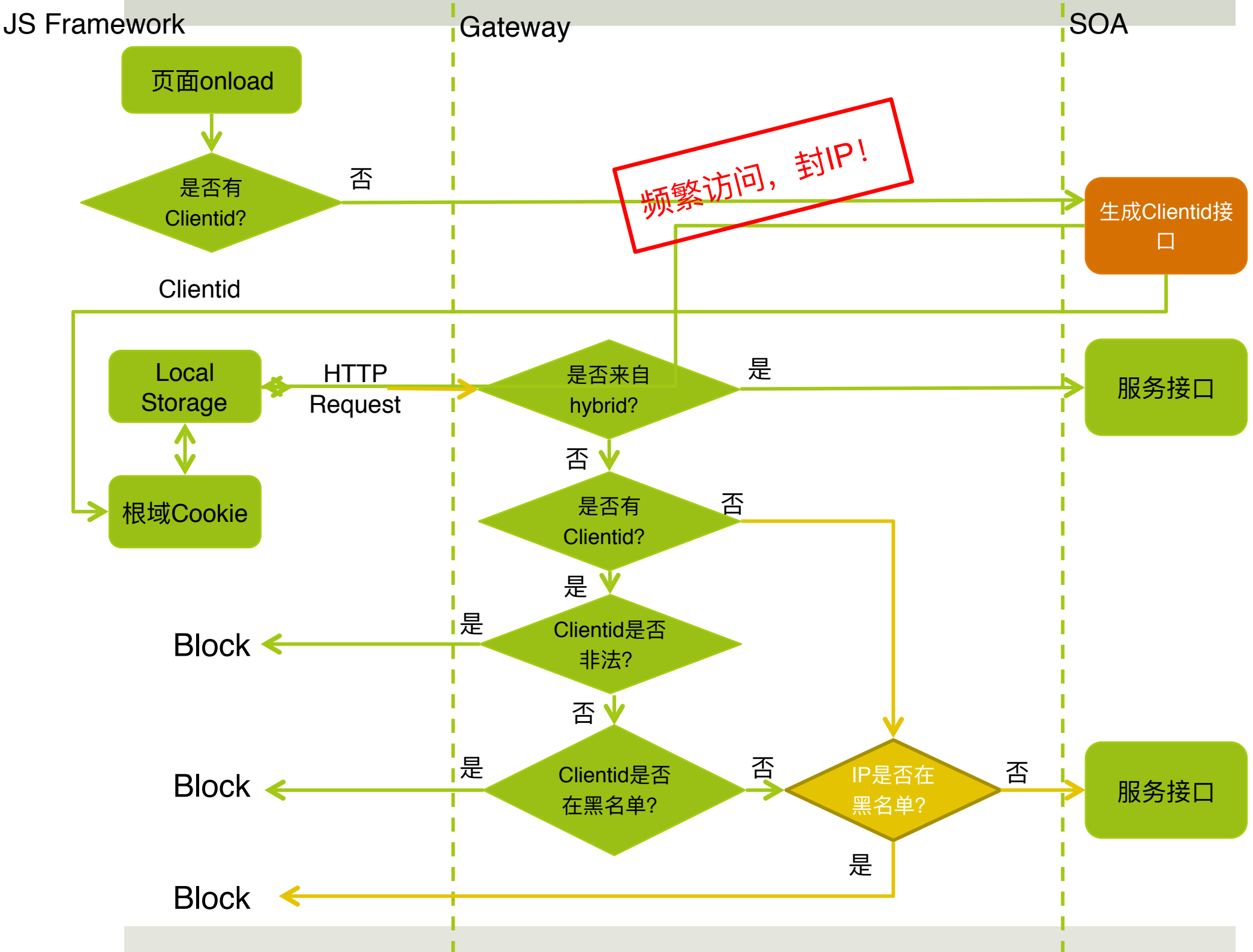
- 爬虫
  - 爬取公司独家的商品、价格信息
  - 批量刷单/刷活动/刷评论/刷优惠券…
  - 移动端H5站点是重灾区
- 旧有架构是否满足?
  - 前端风险：ClientID可被伪造
  - 风险识别效率低：依赖人工
  - 响应方式落后：网络设备上封锁IP地址
- 为旧有架构添加安全Feature
  - 规则引擎
  - 响应模块

旧有架构

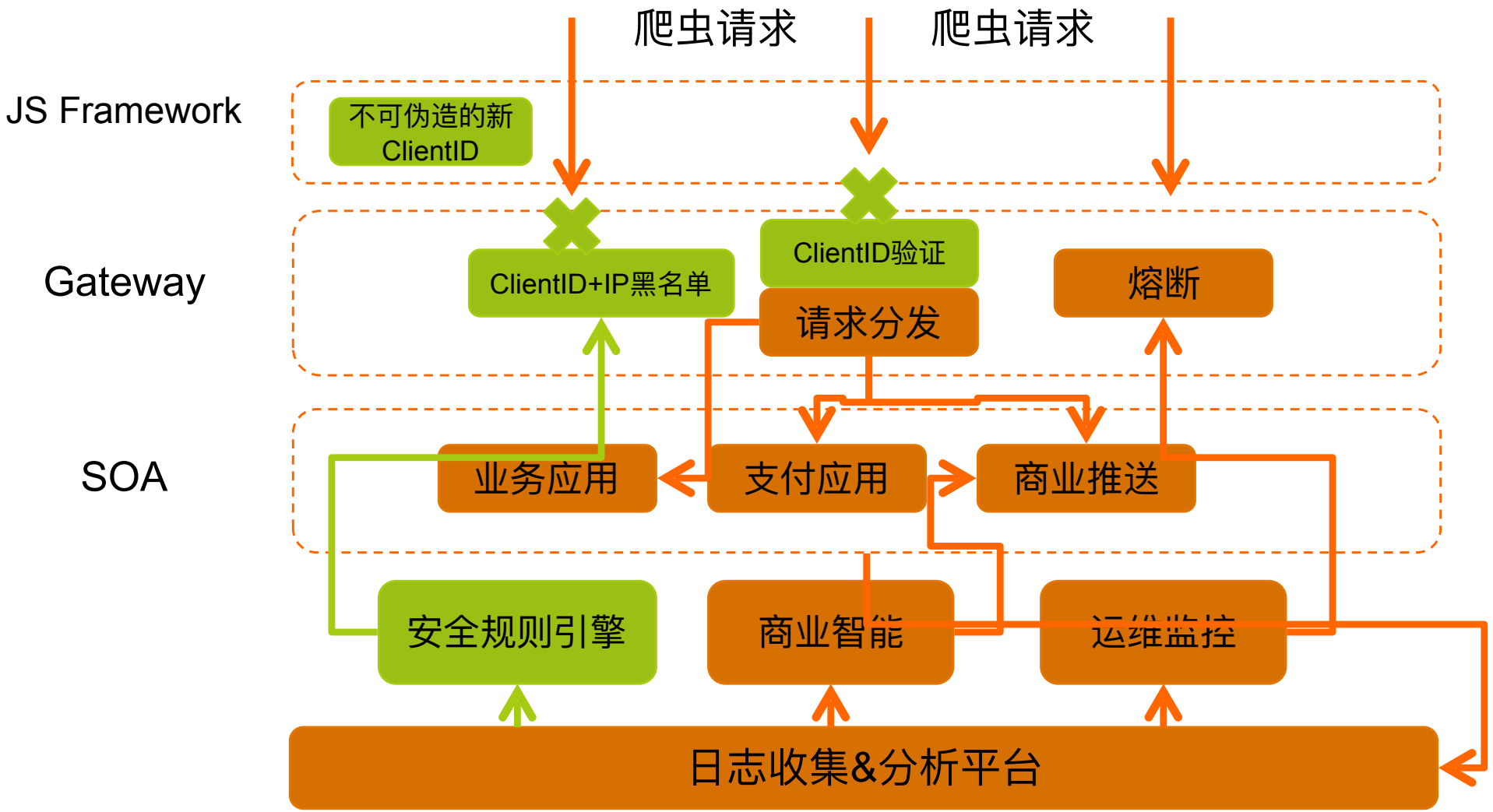

Request
Request
JS Framework
可被伪造的
ClientID
Gateway
IP黑名单
请求分发
熔断
SOA
业务应用
支付应用
广告推送
人工安全监控
大数据平台
运维监控
日志收集&分析平台

新的安全架构方案

- 安全监控模块
  - 规则引擎代替人工
- Gateway改造
  - ClientID合法性验证
  - 两个黑名单：ClientID & IP
- 新增SOA服务
  - 给客户端下发ClientID
  - 提升安全性：ClientID中带有校验位
- JS Framework改造
  - ClientID的获取、存储
  - 访问SOA服务统一携带ClientID


JS Framework
Gateway
SOA
页面onload
是否有Clientid?
否
频繁访问，封IP！
生成Clientid接口
Clientid
Local Storage
HTTP Request
是否来自hybrid?
是
服务接口
否
根域Cookie
是否有Clientid?
否
是
Block
是
Clientid是否非法?
否
Block
是
Clientid是否在黑名单?
否
IP是否在黑名单?
否
服务接口
是
Block

新架构


爬虫请求
爬虫请求
JS Framework
不可伪造的新ClientID
Gateway
ClientID+IP黑名单
ClientID验证
请求分发
熔断
SOA
业务应用
支付应用
商业推送
安全规则引擎
商业智能
运维监控
日志收集&分析平台

数据分析

业务	总访问量	有cid的访问量	无cid的访问量	非法cid	无cid的访问比例
A	4,447,240	1,869,260	2,577,980	0	42.03%
B	3,091,720	1,473,800	1,617,920	26	47.67%

近半数请求疑似爬虫发起!

经验与教训

- 安全的覆盖面取决于底层架构的覆盖面
  - 某产品线一直在使用1.0版本的JS Framework…
  - 无法兼容移动APP中的Hybrid模式
- 架构变更需要充分考虑到对各业务/产品线的影响
  - 三个域名之间同步ClientID
  - 替代旧有ClientID，是否影响业务部门的数据统计?

结语

“知己知彼者，百战不殆”

结语

- 架构里看安全
  - 安全应作为基础架构的一部分
  - 互联网企业需重视基础架构的建设
    - 满足大多数业务的需求
    - 满足安全性需求
  - 建设优秀的架构需要有安全人员的参与
- 安全愿景
  - 降低安全的连带成本
  - 解决安全问题： 改代码 -> 改规则

Thanks

Q&A