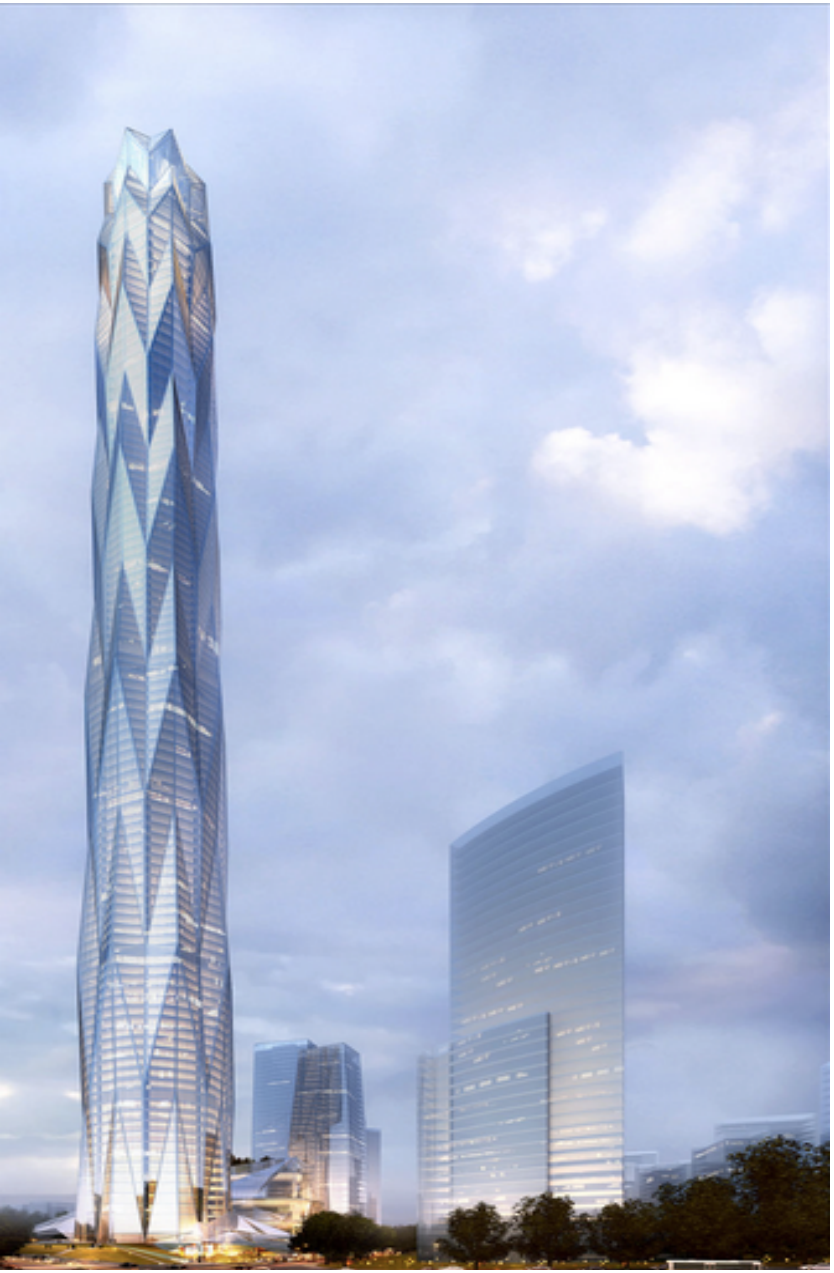


新环境下的电商业务安全

刘明 岂安科技 Chief Products Officer

业务安全 反欺诈 安全感

网易 一号店 携程

数据分析 业务审计 产品

Java js Sql Ai Ps Axure Charles Linux …

创业

网名

风花

为什么会产生业务风险

由业务逻辑本身导致的风险，使用者不按套路出牌

问题：
桶上开这个口是方便添加猫粮，使用者是人，但没能区分进来的是猫粮还是猫脑袋

结果：
猫的饮食没有节制了，随便吃

问题影响：
猫粮开销增大，猫主人遭受了损失

亡羊补牢：
换个自动喂食机（前一个白买了）
每次只给一顿的量（自动喂食的意义不存在了）
加个盖子（猫可能会自己开）
加个带锁的盖子（钥匙怎么保管，每次开锁麻烦）

业务安全类问题影响

12306信息泄露数据被下载传播 12306网站被撞库

论坛出处： 作者： 时间： 2014-12-26

僵尸遍地 互联网过半访问量来自爬虫

2014年12月26日 08:58 转载：快科技 作者:陈骋 编辑:陈骋 0 分享

聚美活动被刷，陈欧微博怒斥黑客

作者： 站内编辑 2015年08月10日 08:08:34 7367 次阅读 来源： TSRC

P2P揽客进入烧钱季 羊毛党每月薅万元不是事儿

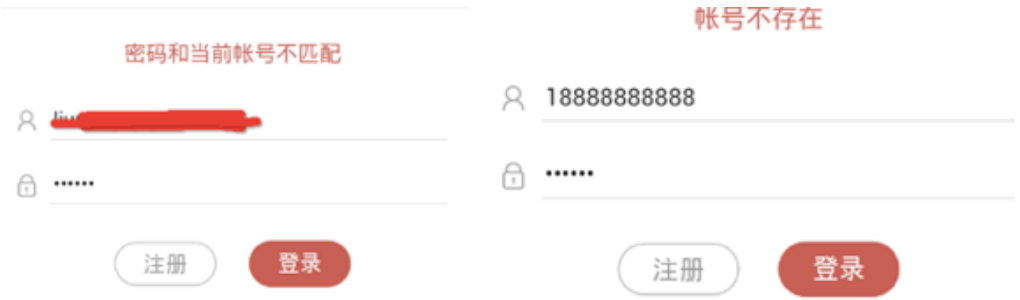
2015-09-26 02:35:37 来源: 证券日报-资本证券网(北京)

一些零碎的问题

隐私泄漏

你注册过哪些网站，通过注册用户效验接口进行批量效验

没确认用户身份前，就告知结果

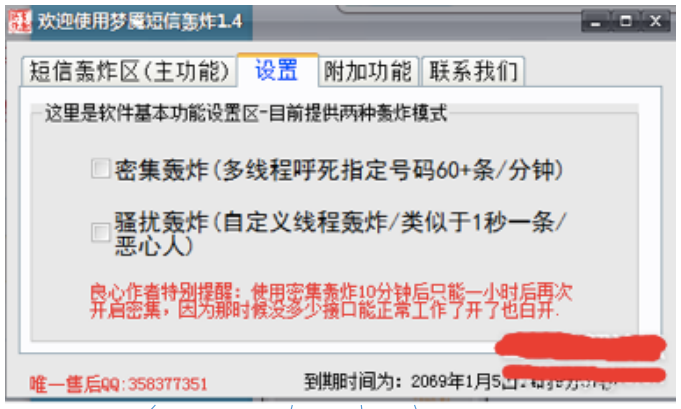


登陆 / 注册 / 密码找回的功能一般都有类似问题

接口滥用

短信资费损失，正常短信发不出去
导致短信渠道异常被关闭

不仅单手机短信应该有疲劳设定
单IP也应当考虑较大阀值的疲劳设定



淘宝
网易
人人贷
其他

手机注册验证码
活动验证码
找回密码验证码
语音验证码

撞库

Ip / Ip段 频度限定

不同账号数 / 密码错误次数 / 不存在账号次数

验证码！验证码！验证码！　　（粘连 / 扭曲 / 空心 / 干扰线 / 多字体）

移动端！移动端！移动端！　　（WEB端基本都做的很好了，但大部分的移动端还是裸的）

羊毛党

怎么去看一个活动做的安不安全？会不会被刷

活动1: 填写手机号码送电影券

活动2: 绑定银行卡送账户20现金

身份真实性 / 次数限定（按身份）

奖品能快速变现吗？身份伪造成本高不高？

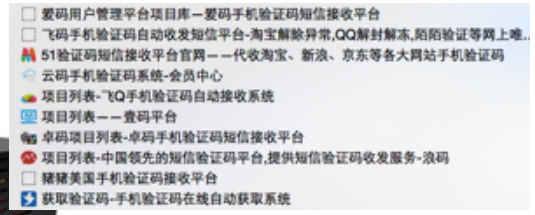
虚假的用户身份

手机号、身份证、银行卡

2000W开房数据

身份证在线生成器

猫池



短信收码平台

银行开借记卡　买银行卡

手机号码
一条短信1元左右
批发短信卡25一张

身份证 0元

借记卡　自办0元 黑卡300~500一张

虚假的用户身份

IP、邮箱、客户端

临时邮箱 / 10分钟邮箱

VPN　星巴克WI-FI　云服务器

IP

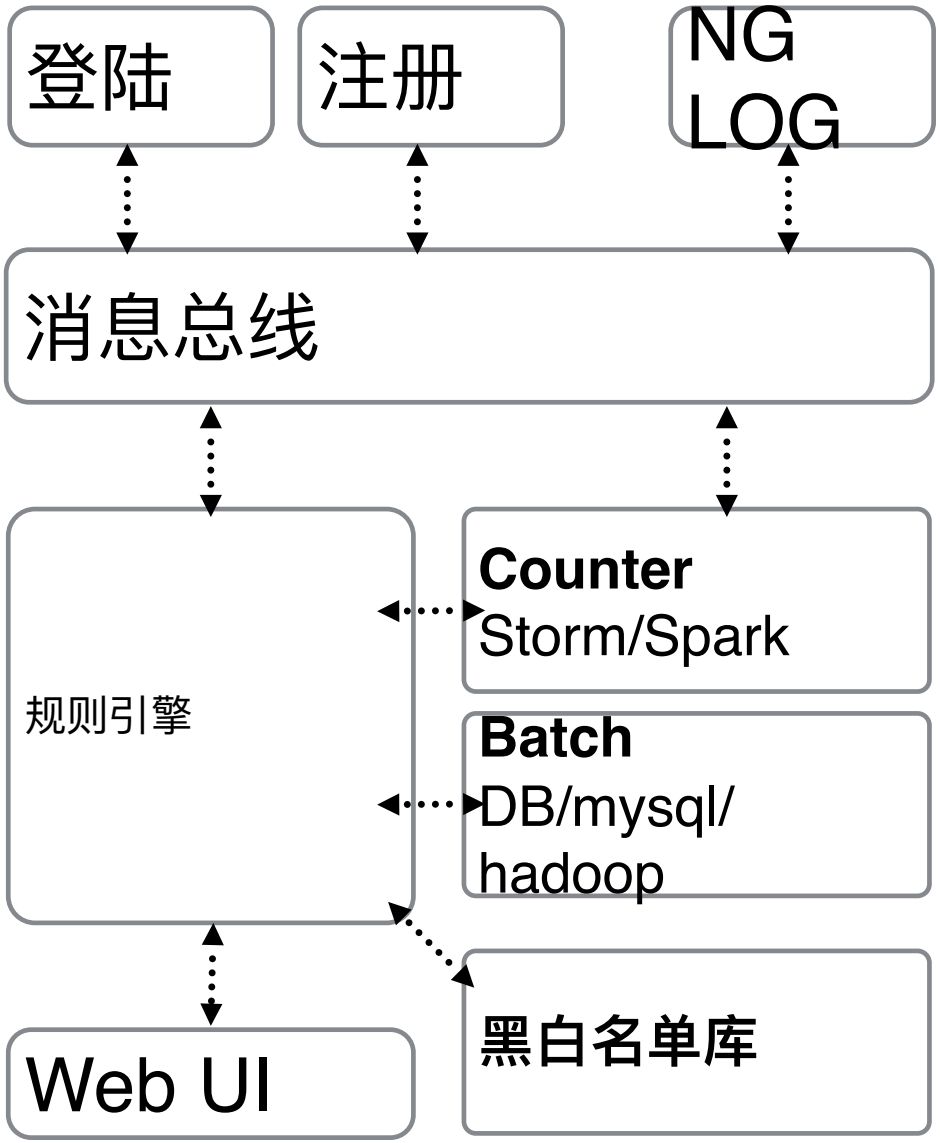
20～60 块钱一个月

模拟器　定制安卓手机

临时邮箱 0元

定制安卓手机，160元，模拟器 0元

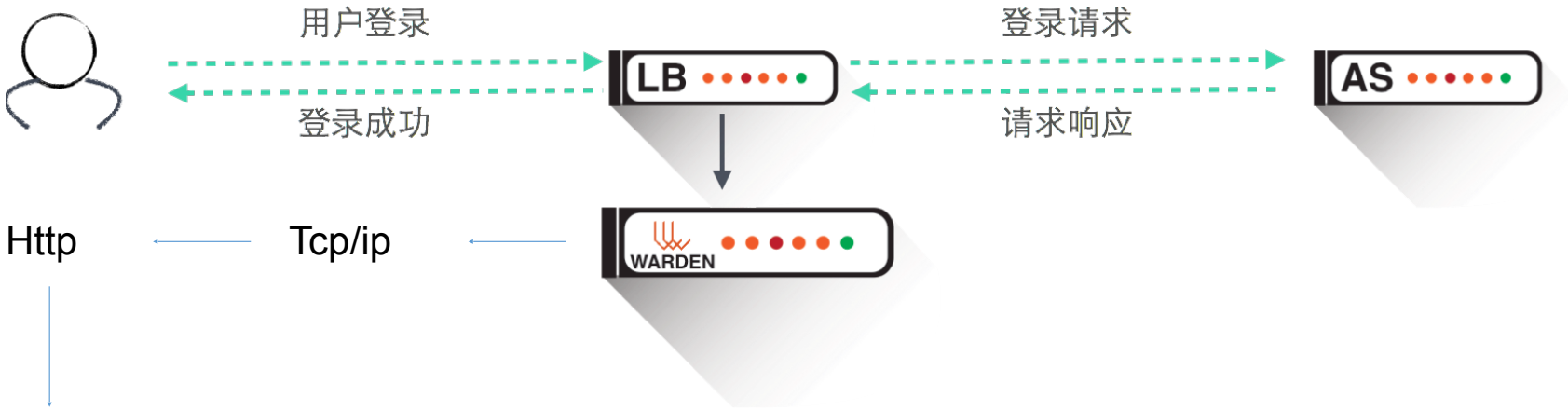
传统风控体系



80% 的精力都放在了

接入埋点的规范定义，宣讲，接入，联调测试，数据质量维护

新环境下的业务安全风控体系



- request: {

  url: /login

  payload: ….username=xxx&pw=xxx&captcha=xxx

  }

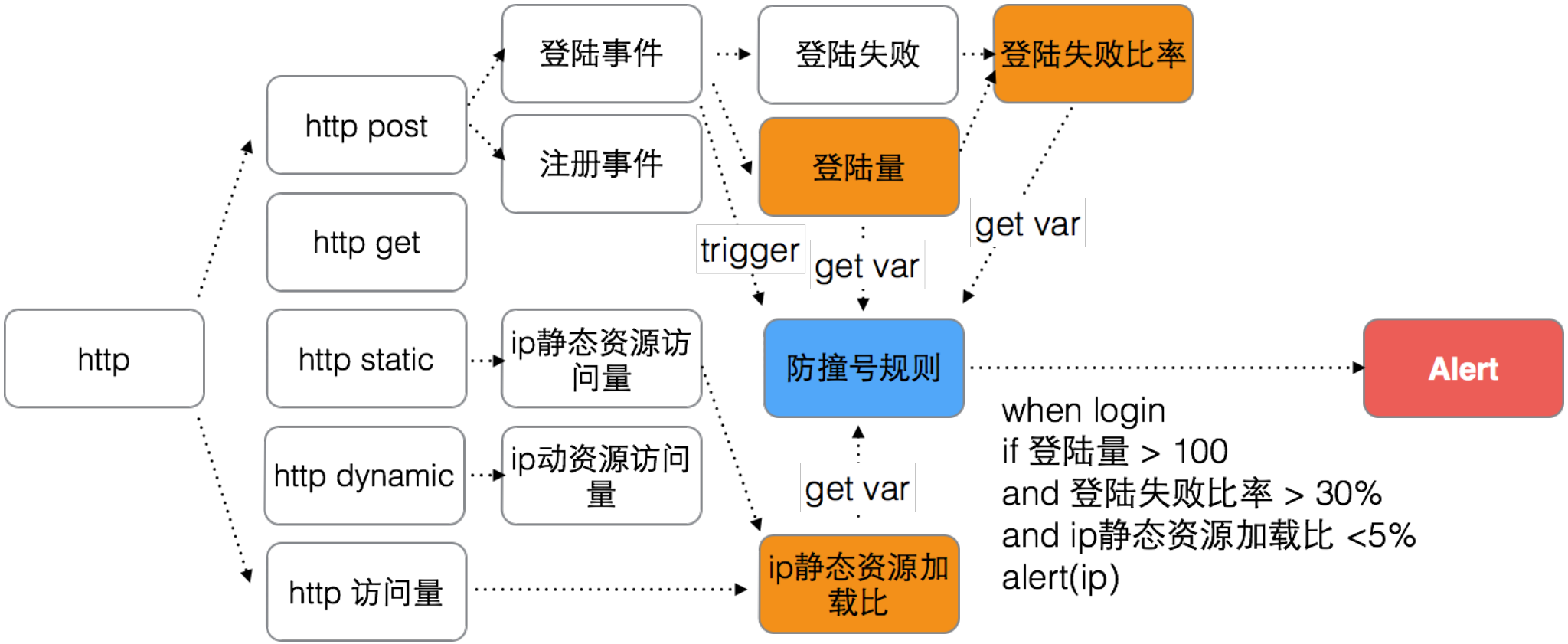
  respond:{

  HTTP/1.1 301 Moved Permanently

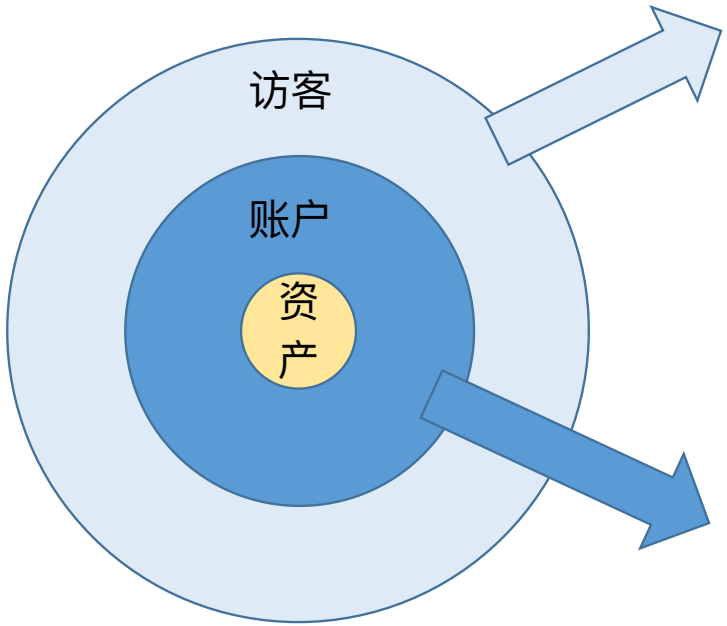
  }

http req/res
登陆
注册
预定
市场活动页面
一切你能想到的业务行为

抓住运维的人帮你搞定就结束了


http
http post
http get
http static
http dynamic
http 访问量
登陆事件
注册事件
ip静态资源访问量
ip动资源访问量
登陆失败
登陆量
ip静态资源加载比
登陆失败比率
trigger
get var
get var
get var
防撞号规则
Alert
when login
if 登陆量 > 100
and 登陆失败比率 > 30%
and ip静态资源加载比 <5%
alert(ip)

铡刀


访客
账户
资产


为防黄牛，请您输入下面的数字
在防黄牛的路上，我们一直在努力，也知道做的还不够。
所以，这次劳烦您多输一次验证码，我们一起防黄牛。
唐僧有A个徒弟（算白龙马）？武大郎在家里排行第B? A + B = ?
提示
您还在使用这个手机号码?
137×××6392
不，早换号了
没错！还在使用
安全验证
无法通过验证? 获取解决方案
验证方式:
手机宝令/手机密令
验证码:
一键校验等待放行中
确定
取消

辅助我们做好业务安全的东西

设备指纹

成熟技术并未出现

设备指纹

需要部署js 或者sdk
跨浏览器的不准确性
客户端的不可信任性

设备行为轨迹

特征难提取
复杂性差，难以区分不同的人
可以区别机器人

协议栈指纹

要探测客户端
实现相对复杂

情报服务

本地分析瓶颈的有效补充

192.168.0.1
188 8888 8888

黑名单联盟

交换信任问题
不能完全定性

成本低廉

IP/手机情报

云服务器 / 机房IP
组织出口
代理服务器
收码平台手机
欺诈电话平台数据
颗粒度大，需要结合使用

失信情报

法院传票
欠款逾期
不良记录

局限性(初犯)

心得

安全感是一种口碑，不是口号

安全收益量化难，业务安全还是可以抓住有钱的地方死磕

做让客户和同事都喜欢的安全

欢迎指正！

我的微信

bigsec

in bigsec . we trust