大数据反欺诈十例

OWASP 中国

The Open Web Application Security Project

关于我

www.payegis.com.cn

Dejia Wang

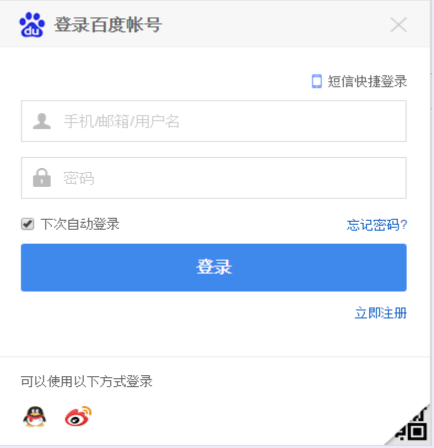
Founder, Chairman and CEO, PAYEGIS

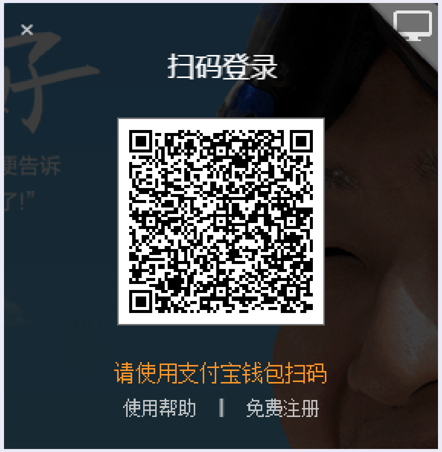
Dejia Wang is the founder of PAYEGIS and has been the Chairman and CEO since 2011. Dejia founded PAYEGIS with the singular vision of empowering consumers and consumer-facing businesses to win the war on mobile, account and transaction fraud. Mr. Wang gained more than a decade of experience working with consumer and transaction data and generating business insights out of big data. From 2001 until 2006, Mr. Wang worked at the leading CRM company Siebel Systems (acquired by Oracle), where he served in various engineering and management positions in US. From 2006 until 2011, Mr. Wang held senior architect and director level positions at Supply Chain Planning, Monetization-As-a -Service and Predictive Marketing Analytics startups: TrueDemand (acquired by Acosta), PlaySpan (acquired by VISA) and M-Factor (acquired by DemandTec, then by IBM).Mr. Wang is also a founding member of Lyris next-generation multi-channel Marketing Optimization Platform. Mr. Wang received PhD in Mathematics from University of Wisconsin-Madison, MS in Computability Theory from Institute of Software, Chinese Academy of Sciences, and BSs in Probability and Statistics, Economical Management from University of Science and Technology of China. Dr. Wang has dozens of patents pertaining to data insightand fraud detection technologies.

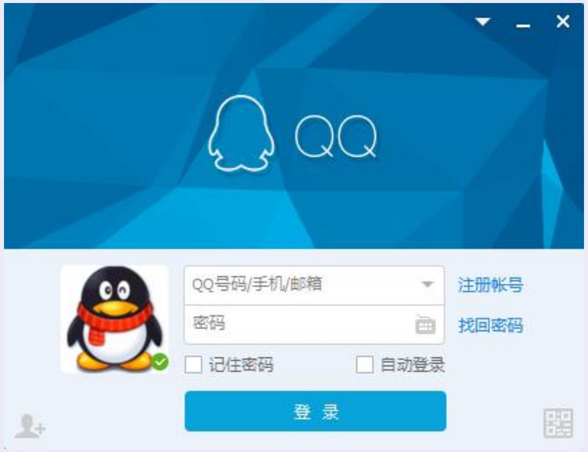
提纲

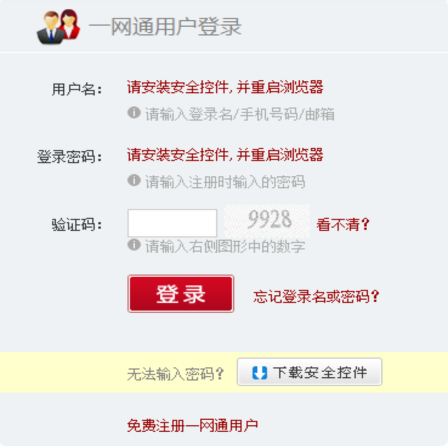
- 场景一:登录(认证问题)
- 场景二:支付(授权问题)
- 场景三:贷款(审核问题)
- 总结

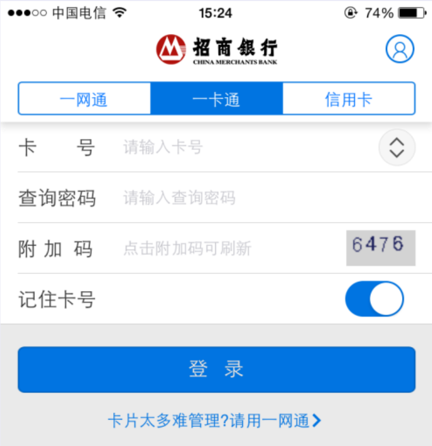
登录场景

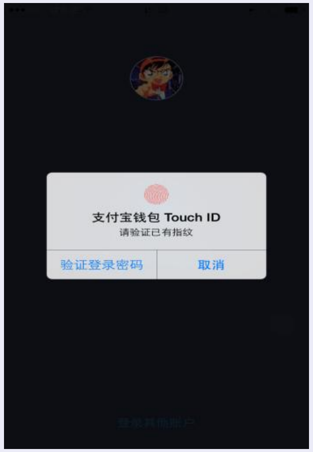

登录百度帐号
短信快捷登录
手机/邮箱/用户名
密码
☑ 下次自动登录
忘记密码?
登录
立即注册
可以使用以下方式登录

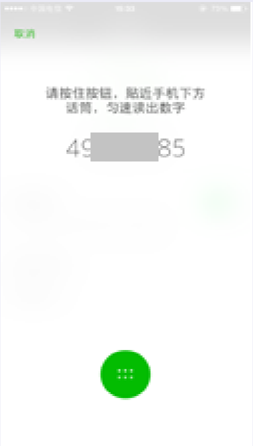

扫码登录
请使用支付宝钱包扫码
使用帮助 | 免费注册


QQ
QQ号码/手机/邮箱
密码
注册帐号
找回密码
□ 记住密码
□ 自动登录
登 录

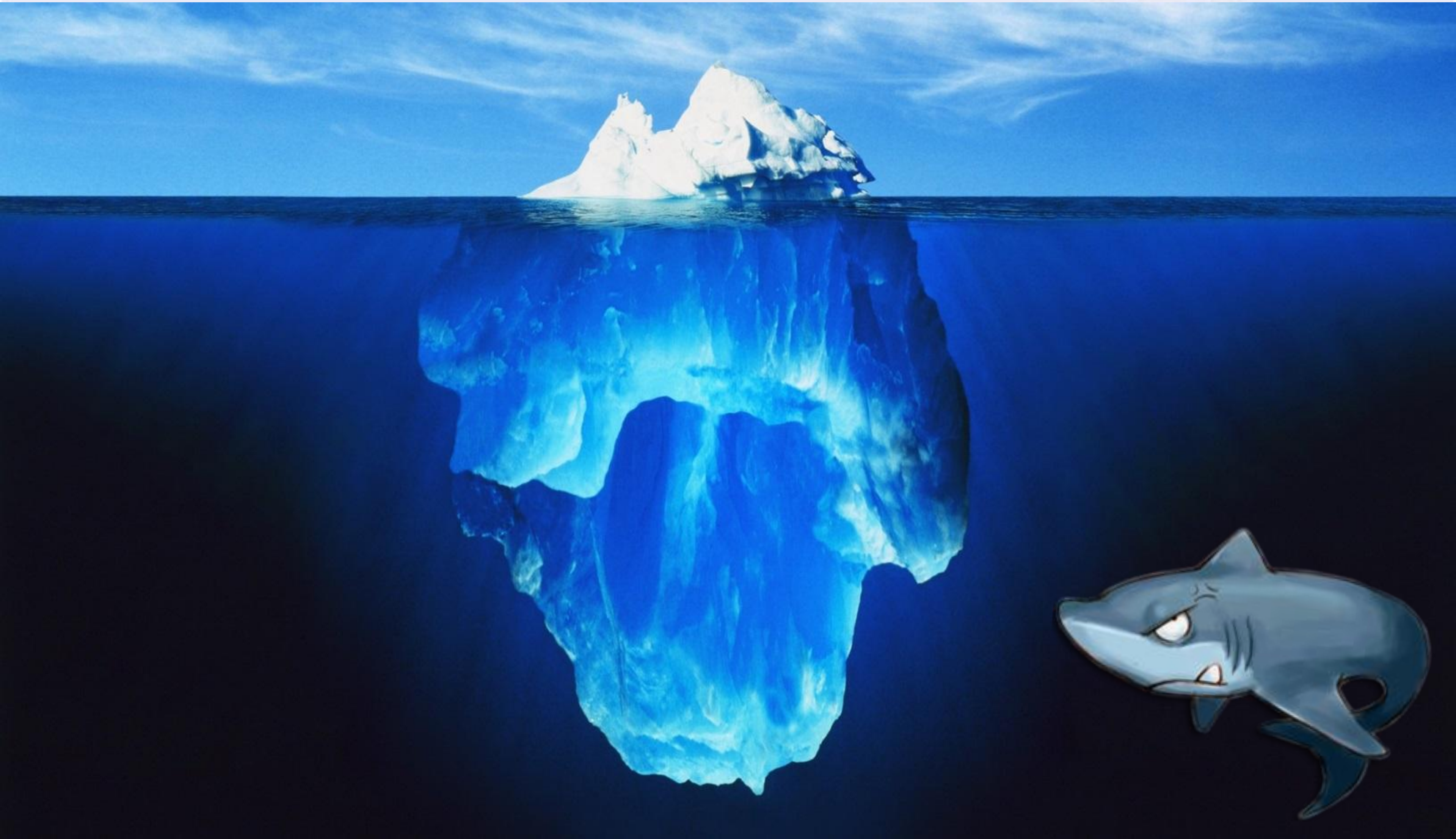

一网通用户登录
用户名:
请安装安全控件, 并重启浏览器
请输入登录名/手机号码/邮箱
登录密码:
请安装安全控件, 并重启浏览器
请输入注册时输入的密码
验证码:
9928
看不清?
请输入右侧图形中的数字
登 录
忘记登录名或密码?
无法输入密码?
下载安全控件
免费注册一网通用户


●●●○○ 中国电信
15:24
74%
招商银行
CHINA MERCHANTS BANK
一网通
一卡通
信用卡
卡 号
请输入卡号
查询密码
请输入查询密码
附 加 码
点击附加码可刷新
6476
记住卡号
登 录
卡片太多难管理?请用一网通


支付宝钱包 Touch ID
请验证已有指纹
验证登录密码
取消


取消
请按住按钮，贴近手机下方话筒，匀速读出数字
49[redacted]85

账户泄漏

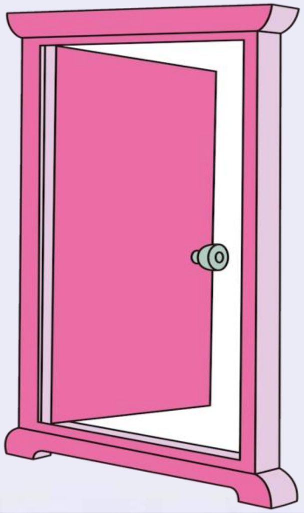


例一:高危数据 == 禁止 ？

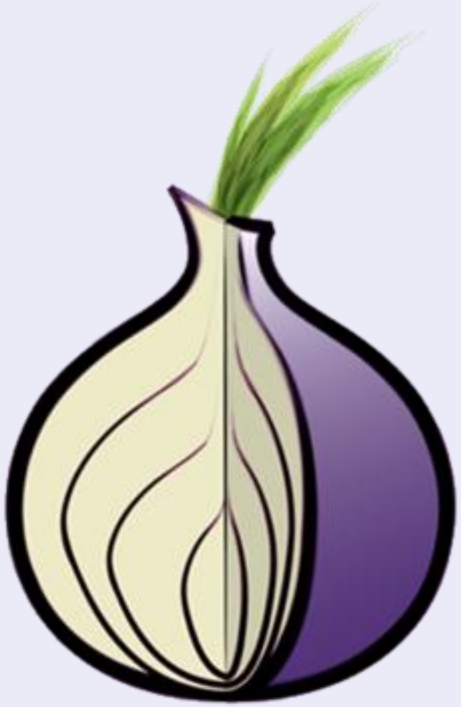
地理位置

OWASP 中国

The Open Web Application Security Project

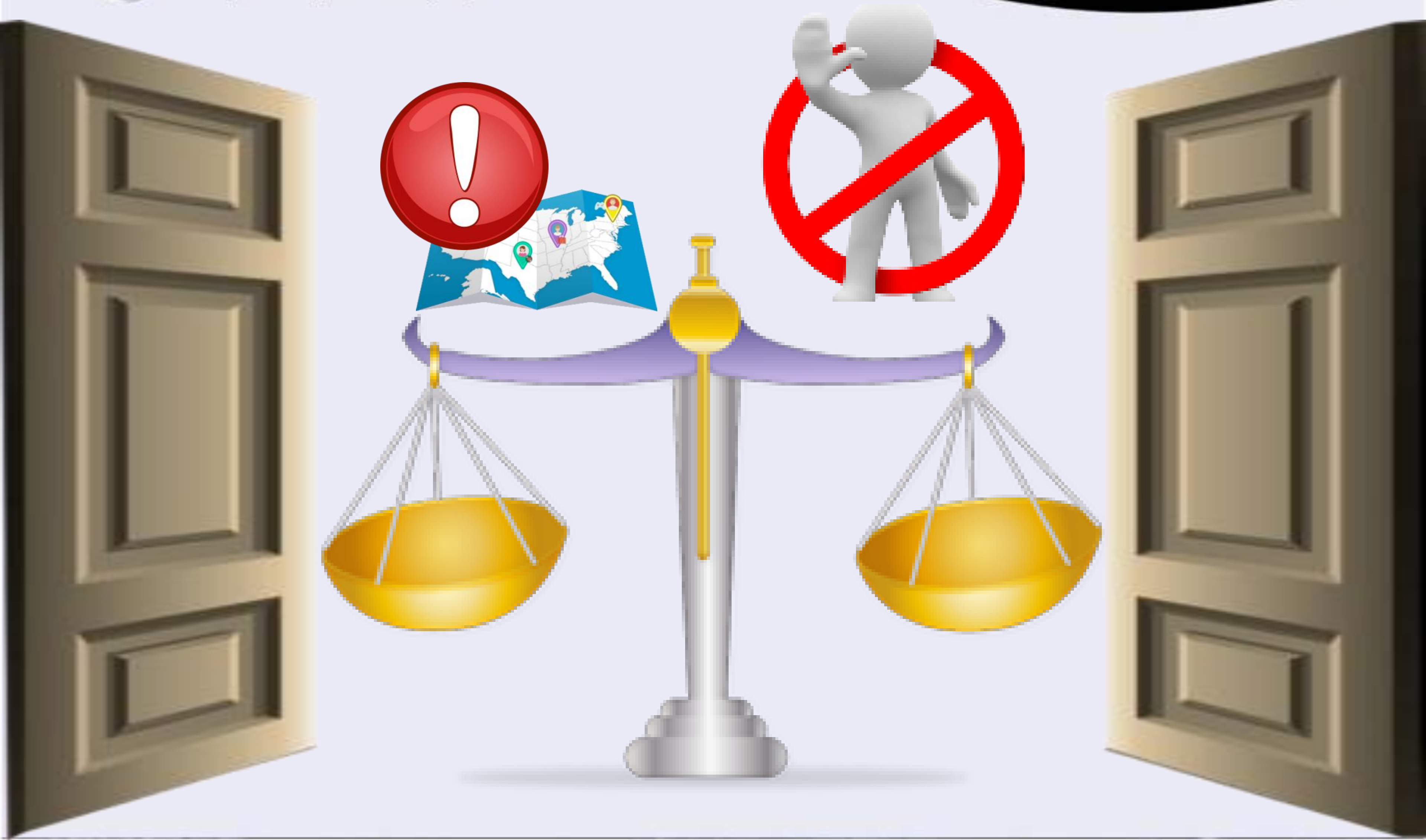


伪造地理位置



例二：高危数据 + 伪造位置 == 禁止 ？

OWASP 中国
The Open Web Application Security Project



丰富多彩的设备种类

APPLE 3G
5:18
Wednesday, September 15
slide to unlock
4.2
MILES

伪造设备

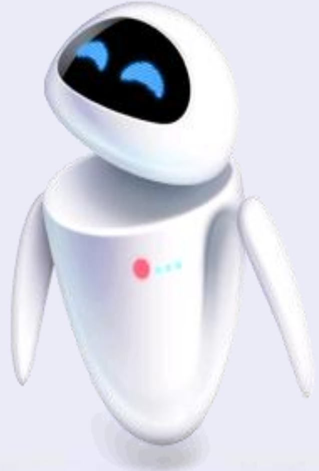
13:44

Android

13:44

7 月 24 日周日

正在充电 (50%)



例三：高危数据 + 伪造位置 + 伪造设备 == 禁止 ？

OWASP 中国
The Open Web Application Security Project

身份认证场景小结

- 大数据反欺诈技术
  - 高危数据情报
  - GeoIP（代理检测、VPN识别）
  - 设备指纹（机器人识别）
- 认证真实用户

自适应验证

2014年以来，国际安全厂商提出自适应验证（Adaptive Authentication）做新型的身份认证，应用于反钓鱼、反撞库、无密码登录等多种场景

ThreatMetrix® BUILDING TRUST ON THE INTERNET™

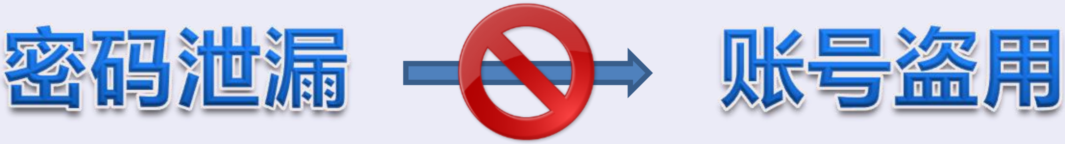
RSA SECURITY

ca technologies

SECUREAUTH

SAFELAYER

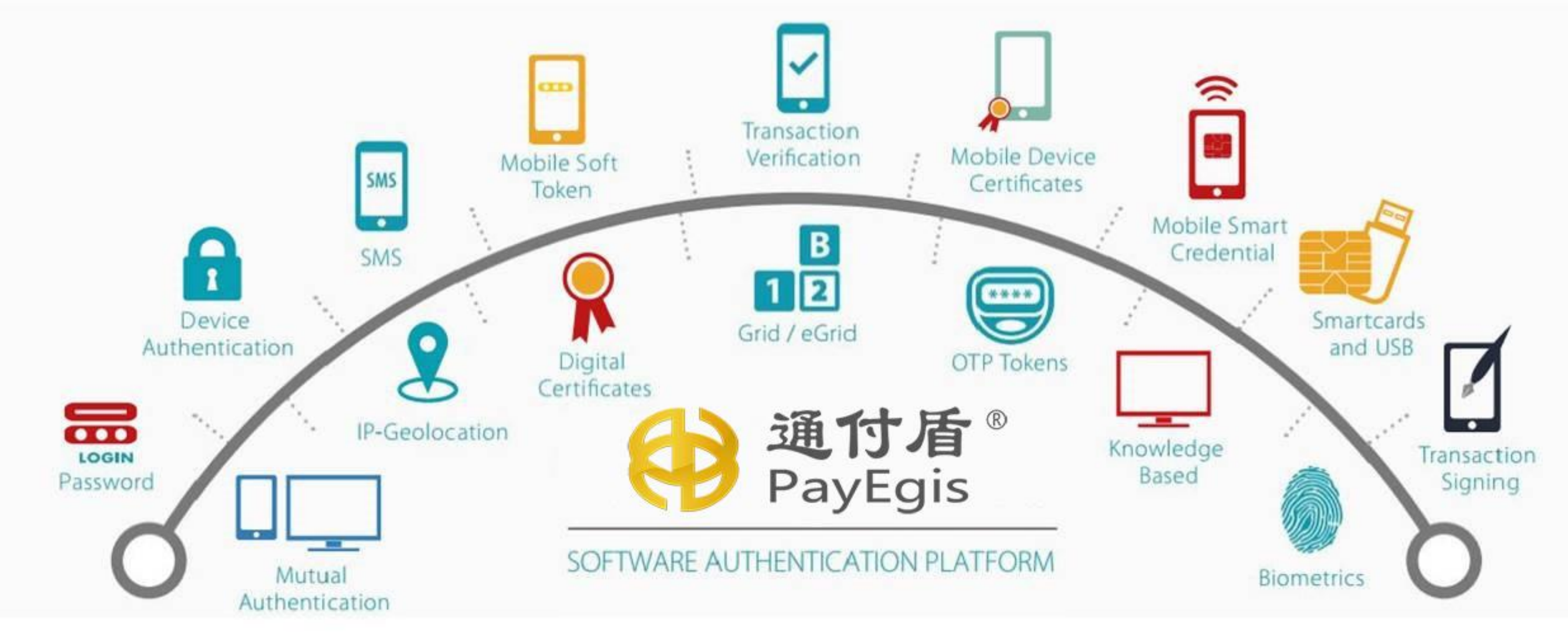
通付盾® PayEgis



传统方案**缓解**账号泄漏产生的影响，新技术**控制**隐私数据泄漏带来的**风险**

基于风险的身份认证

OWASP 中国
The Open Web Application Security Project



基于风险的身份认证(续)

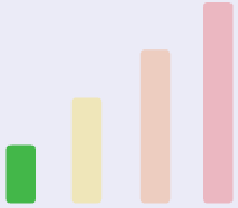
Scenario 1

Legitimate employee attempts to log in to access corporate data from office in Southern California using work desktop at 9:00 a.m. PST

Risk-based authentication analyzes:

Traditional Pattern

User ID	Password	Device Fingerprint	Location	Geo-velocity	IP Address	Login History
✓ Valid	✓ Valid	✓ Corporate-issued computer, normally utilized by user	✓ Location of company, from where user normally works	✓ No distance traveled, accepted geo-velocity range	✓ Valid	✓ During normal working hours



PASS

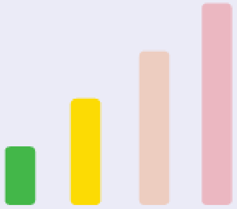
Scenario 2

Legitimate employee attempts to log into corporate email in San Francisco on smartphone at 8:30 p.m. PST

Risk-based authentication analyzes:

Traditional Pattern

User ID	Password	Device Fingerprint	Location	Geo-velocity	IP Address	Login History
✓ Valid	✓ Valid	✓ Recognized device associated with user	⚠ Not normal location, but near enough geographically	⚠ Distance traveled appropriate for user's last login time	✓ Valid	⚠ During abnormal working hours



PASS

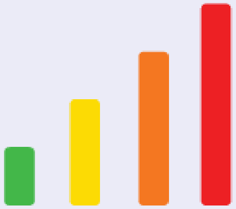
Scenario 3

Attacker attempts to log in to access corporate data from the UK using a personal computer at 2:30 a.m. PST

Risk-based authentication analyzes:

Traditional Pattern

User ID	Password	Device Fingerprint	Location	Geo-velocity	IP Address	Login History
✓ Valid	✓ Valid	✗ Unknown device, no association to user	✗ Abnormal Location and not near to standard location	✗ Distance travel inappropriate for user's last login time	✓ Valid	⚠ During very abnormal working hours



FAIL

提纲

- 场景一：登录(认证问题)

- 场景二：支付(授权问题)

- 场景三：贷款(审核问题)

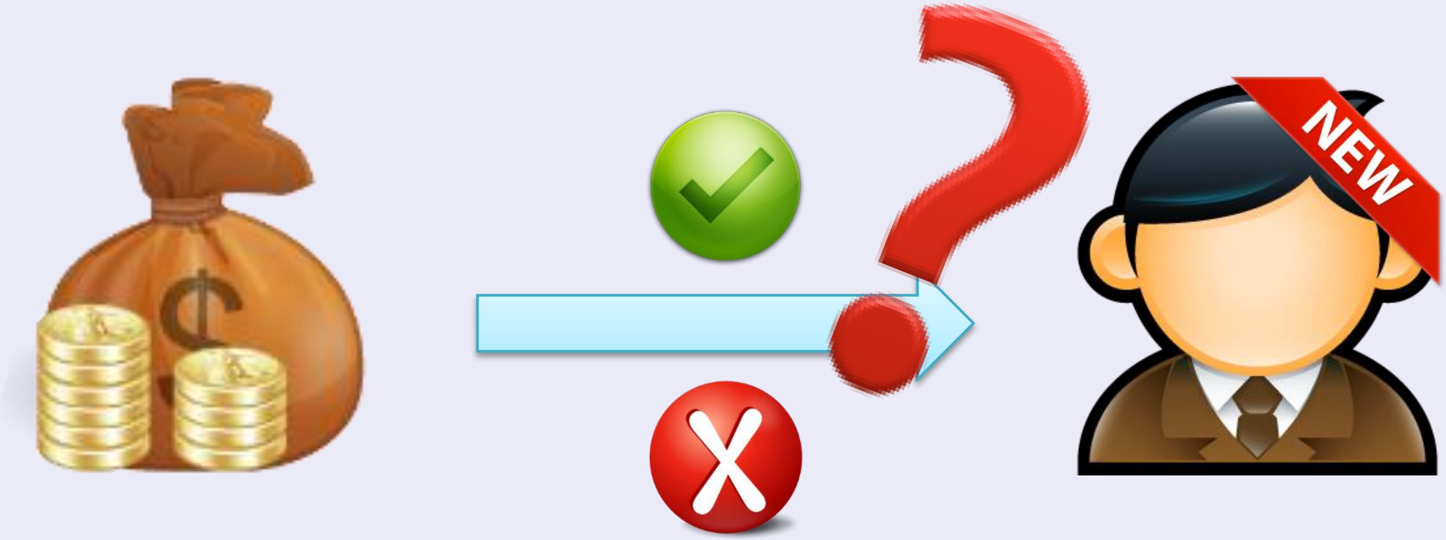
- 总结

支付场景

关系

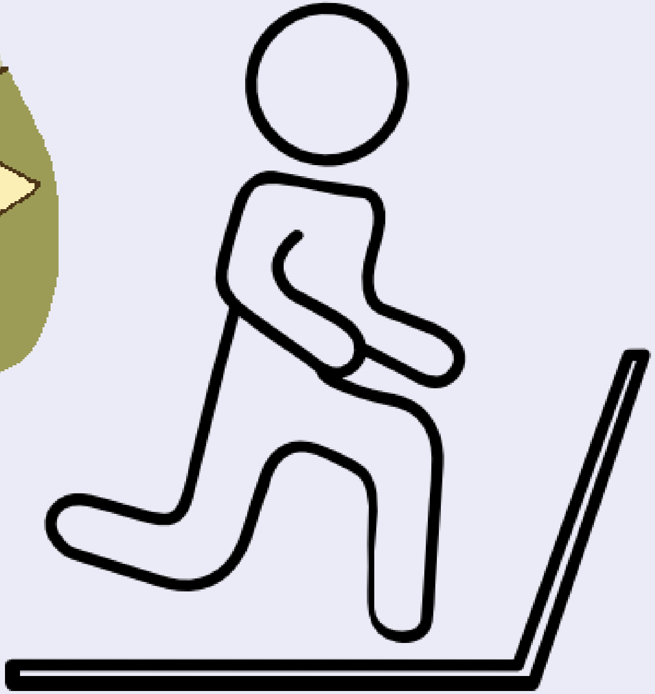
六度空间理论

例四：新关系 == 拒绝？



行为习惯

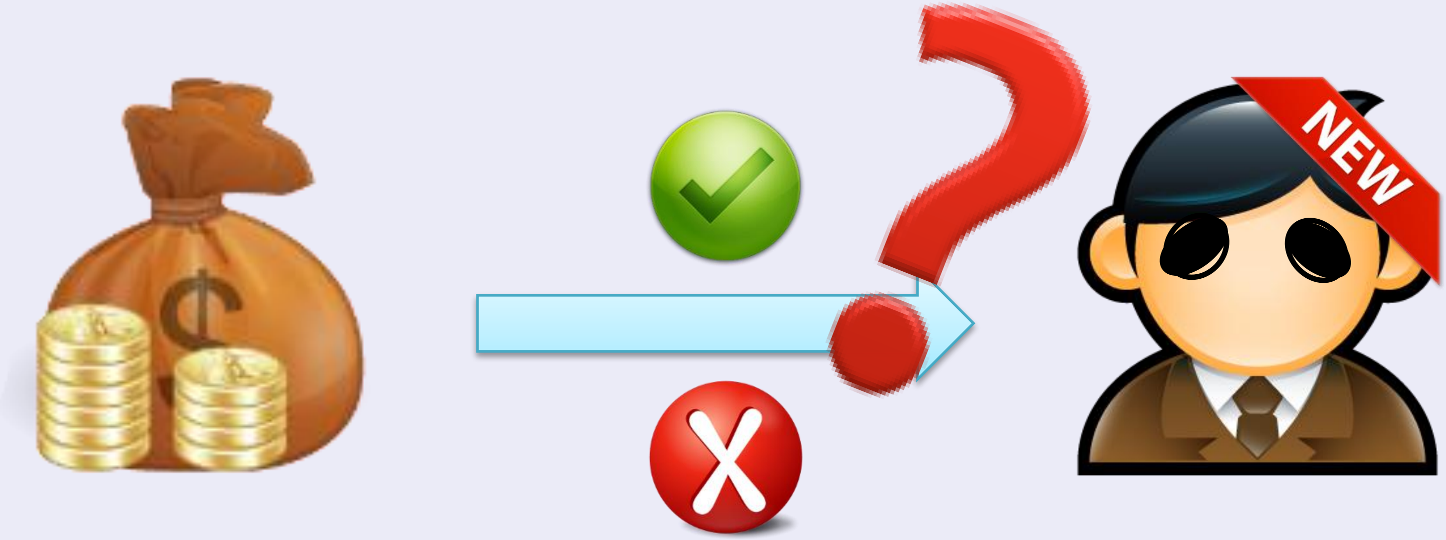
OWASP 中国
The Open Web Application Security Project



例五：新关系 + 新行为 == 拒绝？

OWASP 中国

The Open Web Application Security Project



偏爱喜好

8:00	起床
9:00	上班
9:30	开会
10:00	编码
11:40	午饭
12:00	午休
13:00	工作
18:00	下班
18:30	加班
22:00	下班
23:00	睡觉

No Game ！

No Life ！

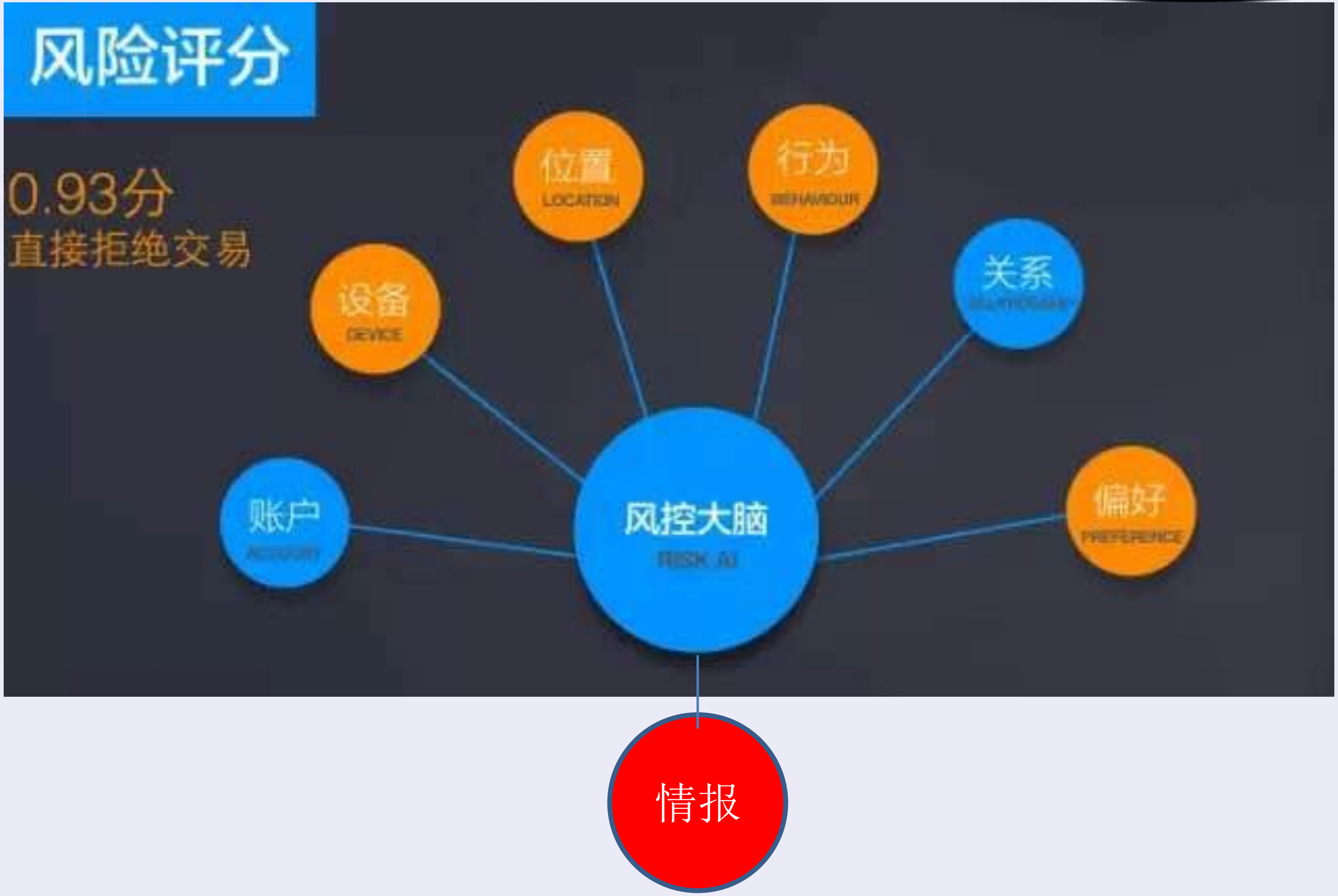
No Money!

例六：新关系 + 新行为 +新喜好== 拒绝？

授权场景小结

- 大数据反欺诈挖掘
  - 挖掘关系
  - 挖掘行为
  - 挖掘偏好
- 授权真实意图

七度空间里的决策大脑



情报收集、交换、大数据挖掘，构建威胁前摄型安全防御体系

提纲

OWASP 中国
The Open Web Application Security Project

- 场景一：登录（认证问题）
- 场景二：支付（授权问题）
- 场景三：贷款（审核问题）
- 总结

贷款场景

贷 OR 不贷？

That’s a question ！

我要贷款！

真有说的那么好？还是慎重点好，元芳你怎么看？

我需要贷款，我现在的项目非常好，只要贷款成功，肯定可以获取很多回报，到时候连本带利都还你！

我是业务员，我已经实地考察过了，并访问了周边的商户，调研了他们产品的市场，未来潜力非常大，赶快审核通过吧。

你们的产品什么时候量产啊？亲戚朋友试用后都说好，我七大姑八大姨还都等着用呢，赶快啊~

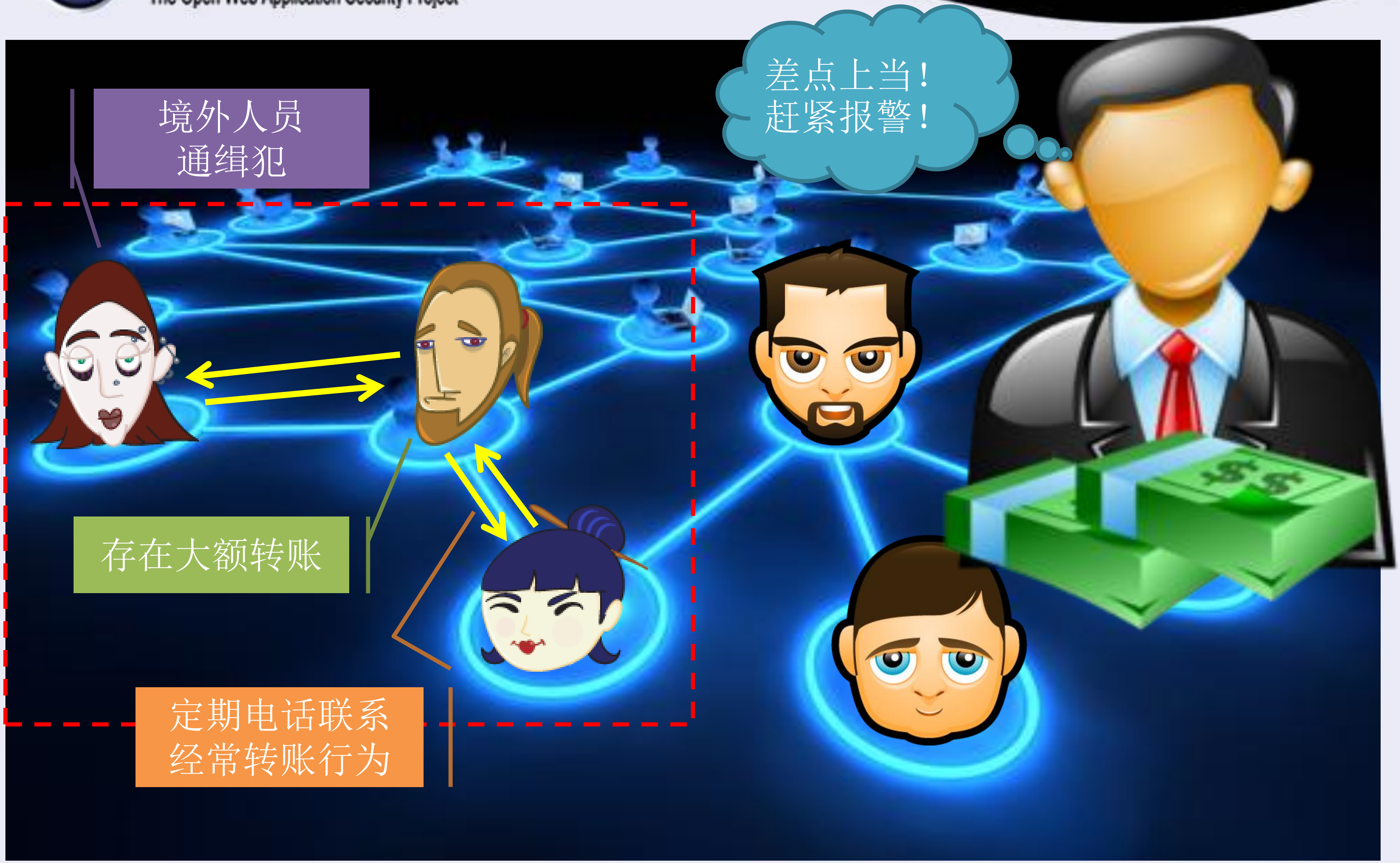
例七：侦查隐藏关系

OWASP 中国
The Open Web Application Security Project

此事必有蹊跷，
仍需再仔细调
查一番！
经常打电话
存在万元转账记录
共用过一台设备
互相为对方充话费

例八：侦测欺诈环

OWASP 中国
The Open Web Application Security Project



境外人员
通缉犯

存在大额转账

定期电话联系
经常转账行为

例九：捕捉异常事件

黑名单

异地

大额交易

设备关联

非常规时间执行敏感操作

一切皆为“事件”！

例十:用户信誉

姓名:XXXXX

性别:男

不良记录:

- 拖欠信用卡
- 有逃票行为
- 盗窃过自行车
- 打架斗殴
- 关在看守所X个月

审核场景小结

- 大数据反欺诈应用
  - 侦查隐藏关系
  - 识别关系图谱中的欺诈环
  - 捕捉异常事件
  - 刻画用户信誉
- 审核真实身份

提纲

OWASP 中国
The Open Web Application Security Project

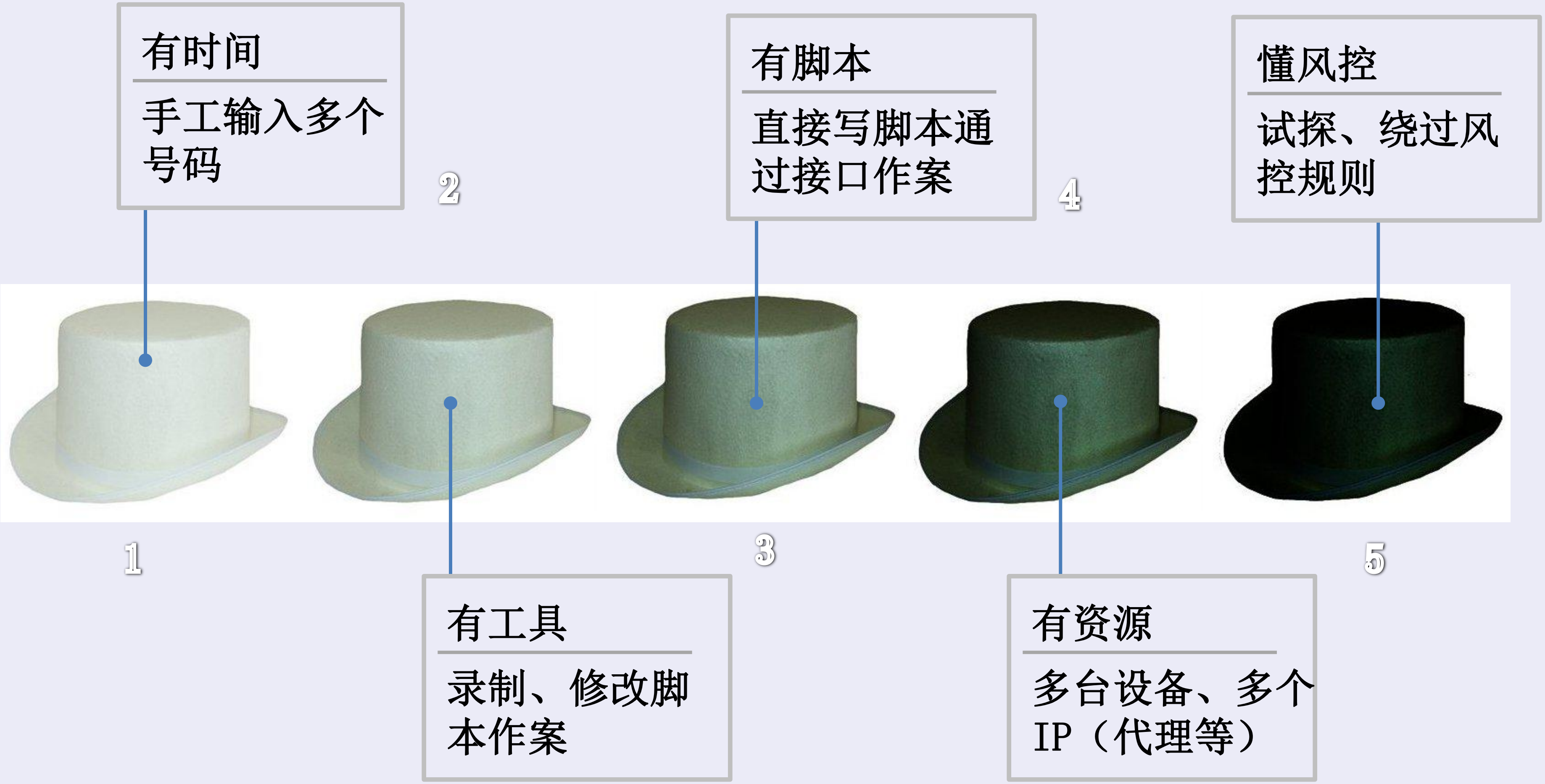
- 场景一:登录(认证问题)
- 场景二:支付(授权问题)
- 场景三:贷款(审核问题)
- 总结

总结

一切的问题都是真实度的问题

- 真实的人
- 真实的设备
- 真实的位置
- 真实的行为
- 真实的偏好
- 真实的关系
- 真实的信誉

斗智斗勇、为欺诈者画像



有时间

手工输入多个号码

有工具

录制、修改脚本作案

有脚本

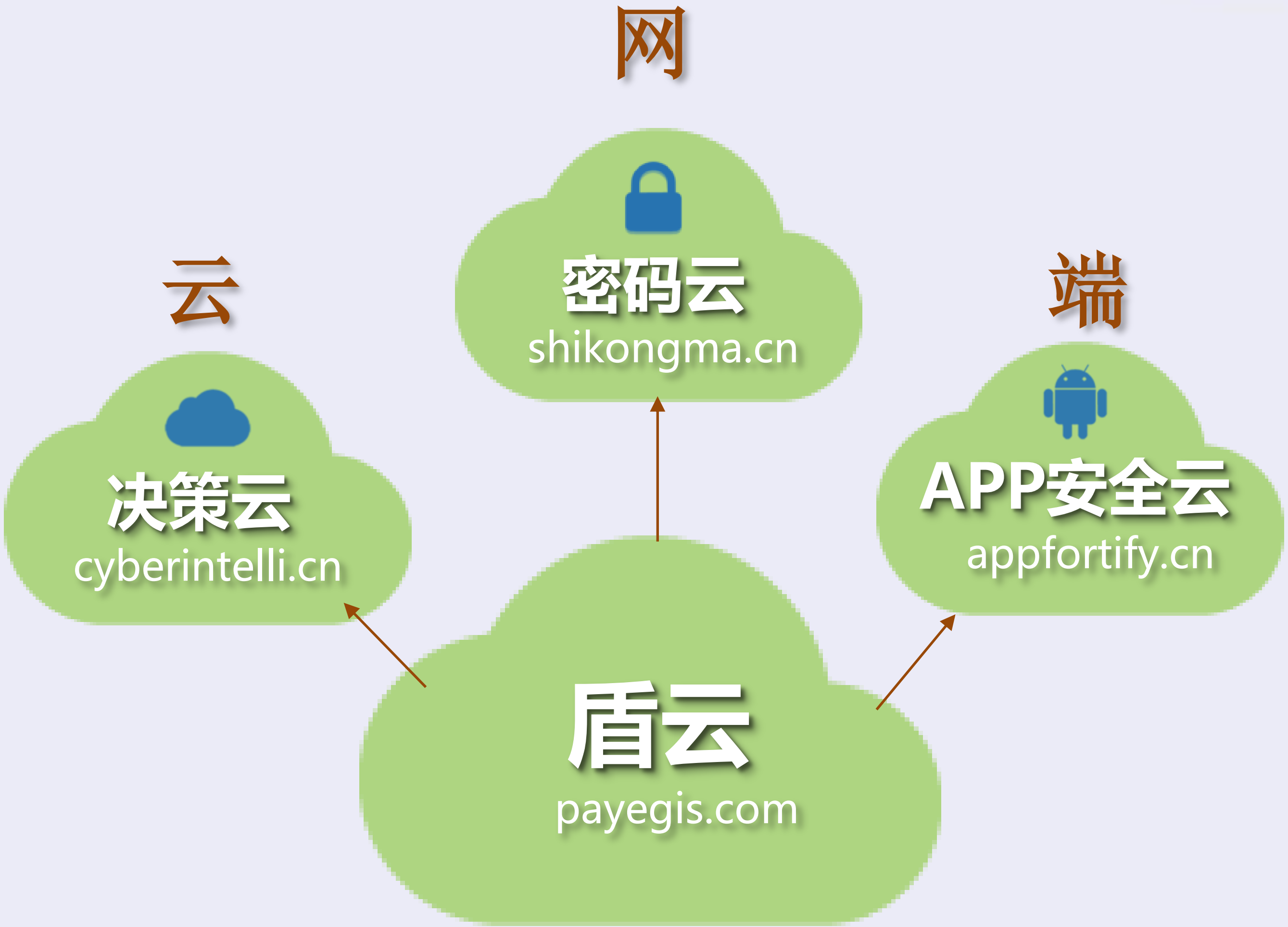
直接写脚本通过接口作案

有资源

多台设备、多个IP（代理等）

懂风控

试探、绕过风控规则



网

密码云
shikongma.cn

云

决策云
cyberintelli.cn

端

APP安全云
appfortify.cn

盾云
payegis.com

盾云（Enterprise SAAS）：移动互联、群防群控

OWASP 中国
The Open Web Application Security Project

谢谢！