自然语言处理和病毒防护技术在网购安全中的应用

周晓波

2014-10-16

提纲

- 网银简介
- 盗取用户网银信息的途径
- 如何防护
- 结论

网银的便捷

- 网银给我们的生活提供了极大的便利

付款收款	生活助手	网购导航	会员账户管理
转账付款	水电煤缴费	海淘	账户管理
转账到银行卡	手机充值	全球直购	交易记录
信用卡还款	固话宽带	海外转运	支付方式管理
找人代付	有线电视缴费	返利商家	账户通
收款主页	还贷款	促销活动	集分宝
AA收款	校园一卡通	一淘比价	余额宝

网银的规模

艾瑞咨询《2012-2013年中国网上银行年度监测报告》数据显示，到2014年，中国网上银行的交易规模有望突破1195万亿元。成为全球最大的网购市场。

网银的安全

- 支付宝用户遭窃， 32万存款被转走

网银的安全

- 蹭网贪便宜网银被盗3.4万

网银的安全

- 手机扫描二维码后，银行卡被盗刷

网银的安全

- 网上“退款操作”损失1.3w

填写信息后，客服特别提醒李小姐点击获取验证码，但奇怪的是，李小姐输入提交了多次，页面却始终显示未成功付款。按照客服提示换张信用卡尝试后，手机短信提示已支付5000元。而此前使用的招商银行信用卡，也被刷8000元。李小姐这次所谓的退款操作，前后共被骗子盗刷了1.3万元。

盗取目标

- 网银用户密码
- 诱导用户付费

盗取途径

- 恶意木马
  - 传统恶意木马，设法躲查杀
  - IE BHO
  - Email
  - Chrome扩展
  - Firefox扩展
  - 手机rom
  - 扫描二维码

盗取途径

- 网络攻击
  - 网站漏洞利用
  - 拖库撞库
  - 免费WIFI
  - 家庭路由：改变DNS设置，诱导下载Flash player

盗取途径

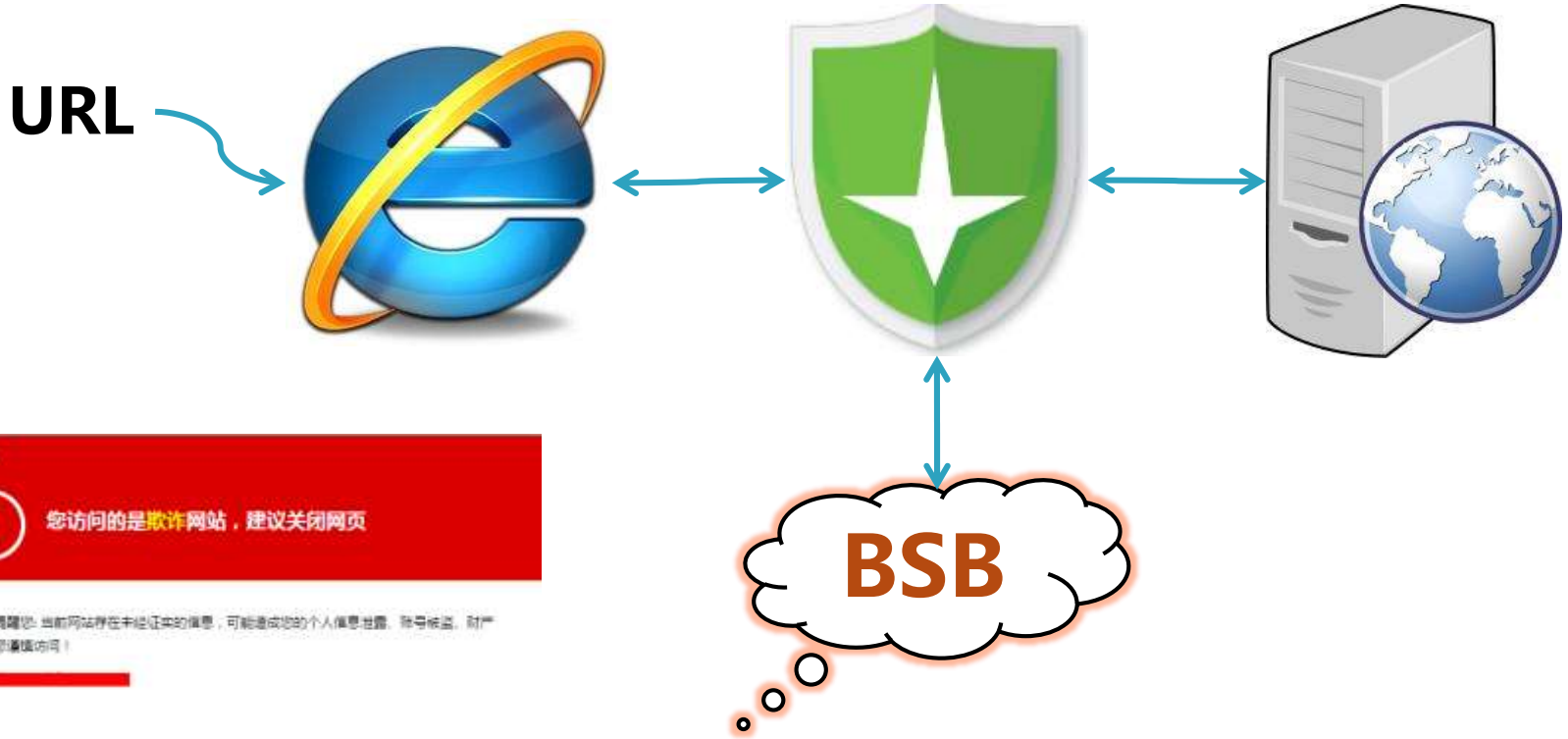
- 钓鱼网站 – 攻心
  - 仿冒网站：银行，电商，医院，票务等
  - 欺诈中奖
  - 虚假信息发布

防护建议

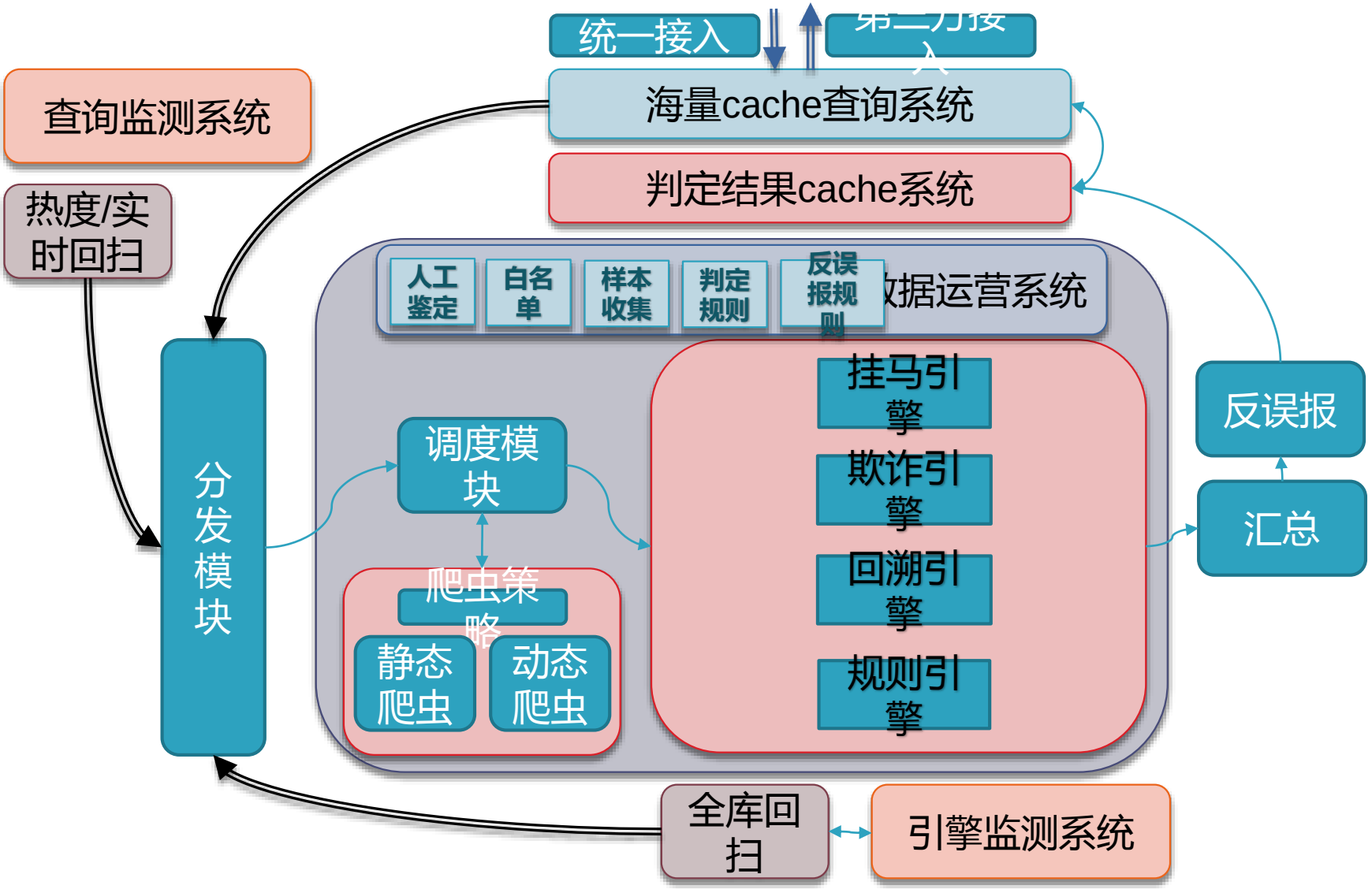
- 常规防护：比如不要设置简单密码，访问正规网站
- 保护好自己的数字证书，使用完USBKEY等网银硬介质后及时拔下
- 提高自己网银密码的保密性，两三个月更换一次密码
- 不使用公共场所的计算机进行网银业务
- 不随意扫描不明二维码
- 安装百度杀毒等安全杀毒软件

网购安全引擎 – BSB

- 百度安全浏览服务



网购安全引擎 – 架构

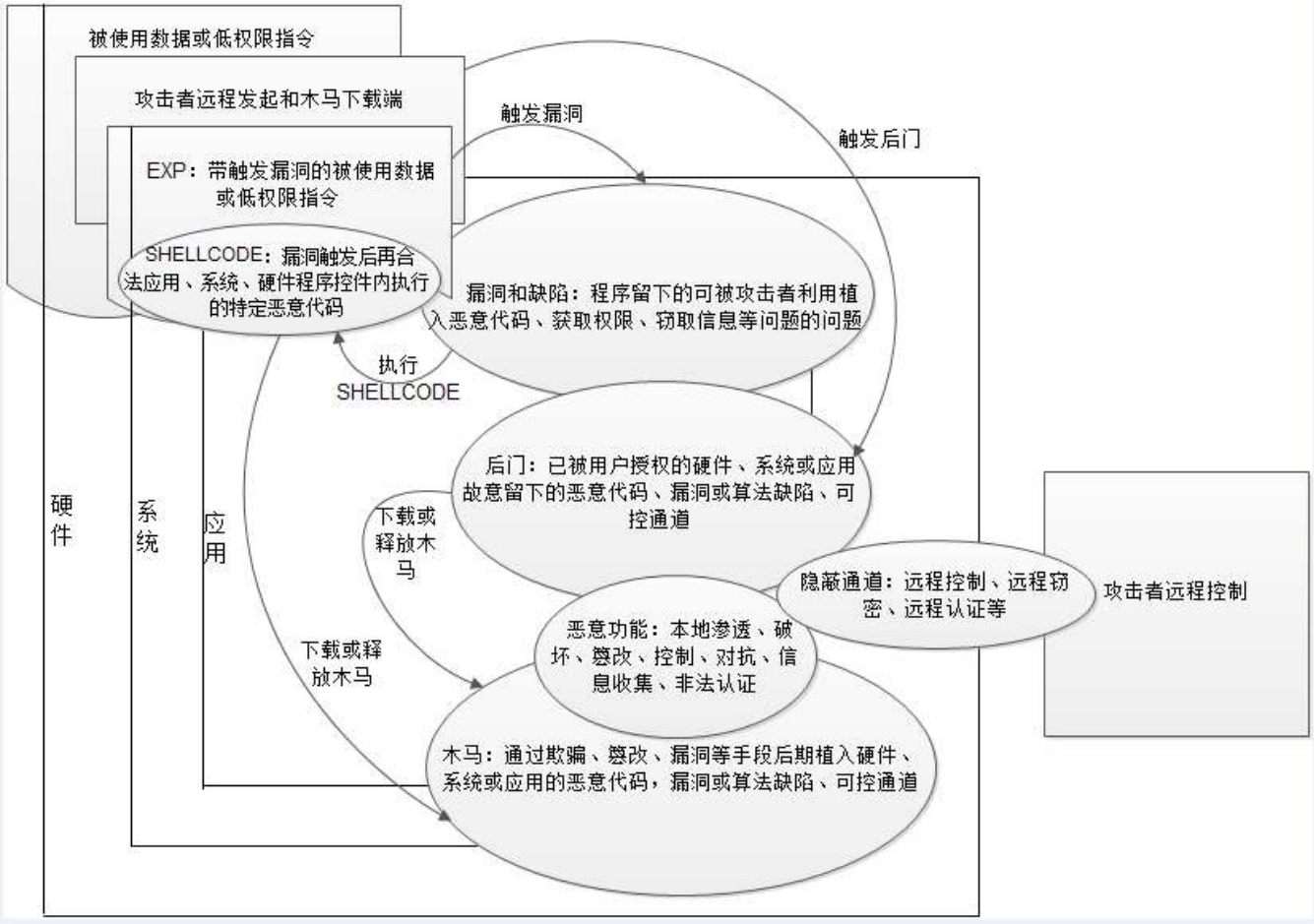

统一接入
查询监测系统
海量cache查询系统
判定结果cache系统
热度/实时回扫
人工鉴定
白名单
样本收集
判定规则
反误报规则
数据运营系统
挂马引擎
欺诈引擎
回溯引擎
规则引擎
反误报
汇总
分发模块
调度模块
爬虫策略
静态爬虫
动态爬虫
全库回扫
引擎监测系统

网购安全引擎 – 病毒防护技术

- 挂马引擎

网购安全引擎 – 病毒防护技术

- 虚拟机中监控网页脚本对操作系统的破坏表现：注册表/内存/网络请求等



网购安全引擎 – 病毒防护技术

- 浏览器模拟：可以认为一个利用浏览器漏洞来获得执行权限的挂马网页包含两个特征
  - 使用堆喷技术
  - 堆喷分配的是Shellcode
- 当发现脚本申请/消耗大量内存后，检测当前上下文各属性是否含有shellcode

网购安全引擎 – 病毒防护技术

- 漏洞POC片段：DoCmd函数未检查参数长度导致溢出

```
<object classid='clsid:77910CD3-5447-4CCB-92DE-35BA8198BE81' id='uusee' ></object>
<script language='javascript'>

for(counter=0; counter<200; counter++)
   memory[counter]= block + shellcode;

arg='';
for(counter=0; counter<=1000; counter++) arg+=unescape("%0C%0C%0C%0C");

uusee.DoCmd(arg);

</script>
```

网购安全引擎 – 病毒防护技术

- 检测代码：严格模拟浏览器对Javascript解析执行的过程，根据各漏洞执行特点hook相关漏洞函数，当满足漏洞运行特征时判定为触发漏洞

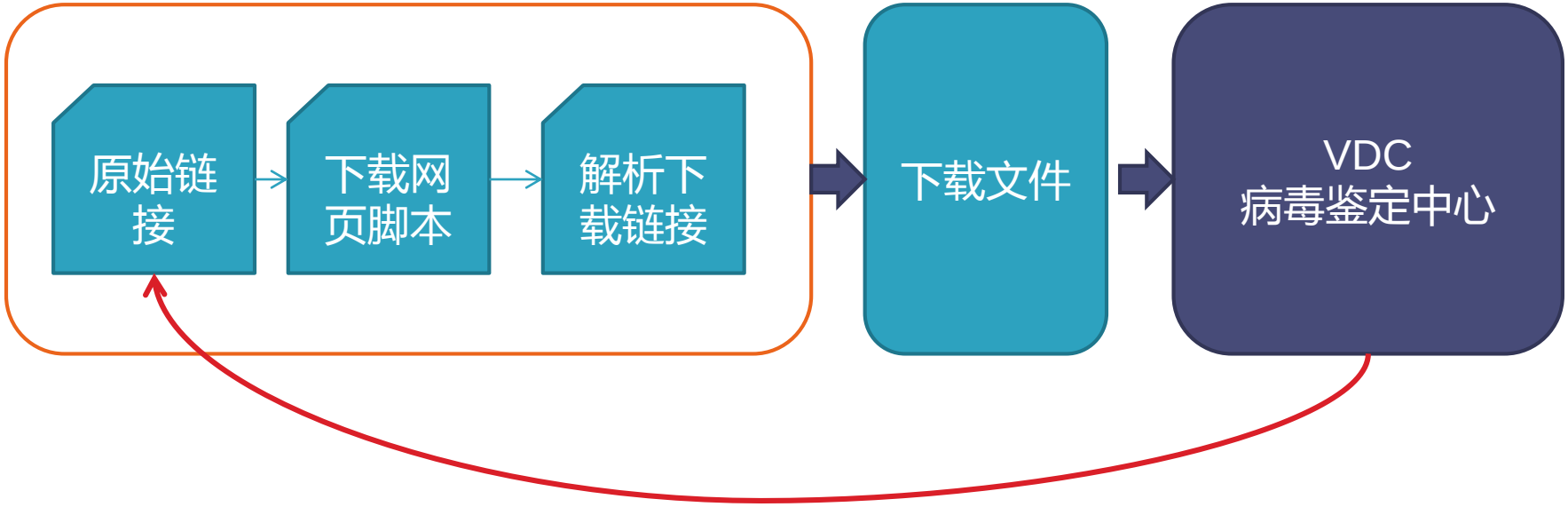
```
{
    //UUPlayer Buffer SendLogAction/DoCmd Buffer Overflow Added by jeeeryliu 2011-11-15
    "UUPlayer ActiveX缓冲区溢出漏洞",
    "UUPlayer.ocx.6.x",
    "uuplayer.ocx.6.x",
    "77910CD3-5447-4CCB-92DE-35BA8198BE81",
    "77910cd3-5447-4ccb-92de-35ba8198be81",
    {NULL, m_UUPlayerSendLogActionFunc}
},
JSFunctionSpec CJSLeakObject::m_UUPlayerSendLogActionFunc[] =
{
    {"SendLogAction", UUPlayerSendLogAction},    // CVE-2011-2589
    {"DoCmd",UUPlayerDoCmd},
    {"",NULL}
};
Handle<Value> CJSLeakObject::UUPlayerSendLogAction(const Arguments& args)
{
    char URL[MAX_DOWNEXELEN] = {0};
    if( args.Length() >= 1 && !args[0].IsEmpty())
    {
        string strArg = ObjectToString( args[0] );
        if( !strArg.empty() && strArg.length() > 200 )
        {
            EnumProperty( URL, MAX_DOWNEXELEN, EnumPropertyGetUrlInShellcode);
            CJSParseBase::AddLeakList(
                    m_lObject[emUUPlayerSendLogAction].szDesc,
                    m_lObject[emUUPlayerSendLogAction].szProgID,
                    m_lObject[emUUPlayerSendLogAction].szClsid, URL
```

Hook住DoCmd函数

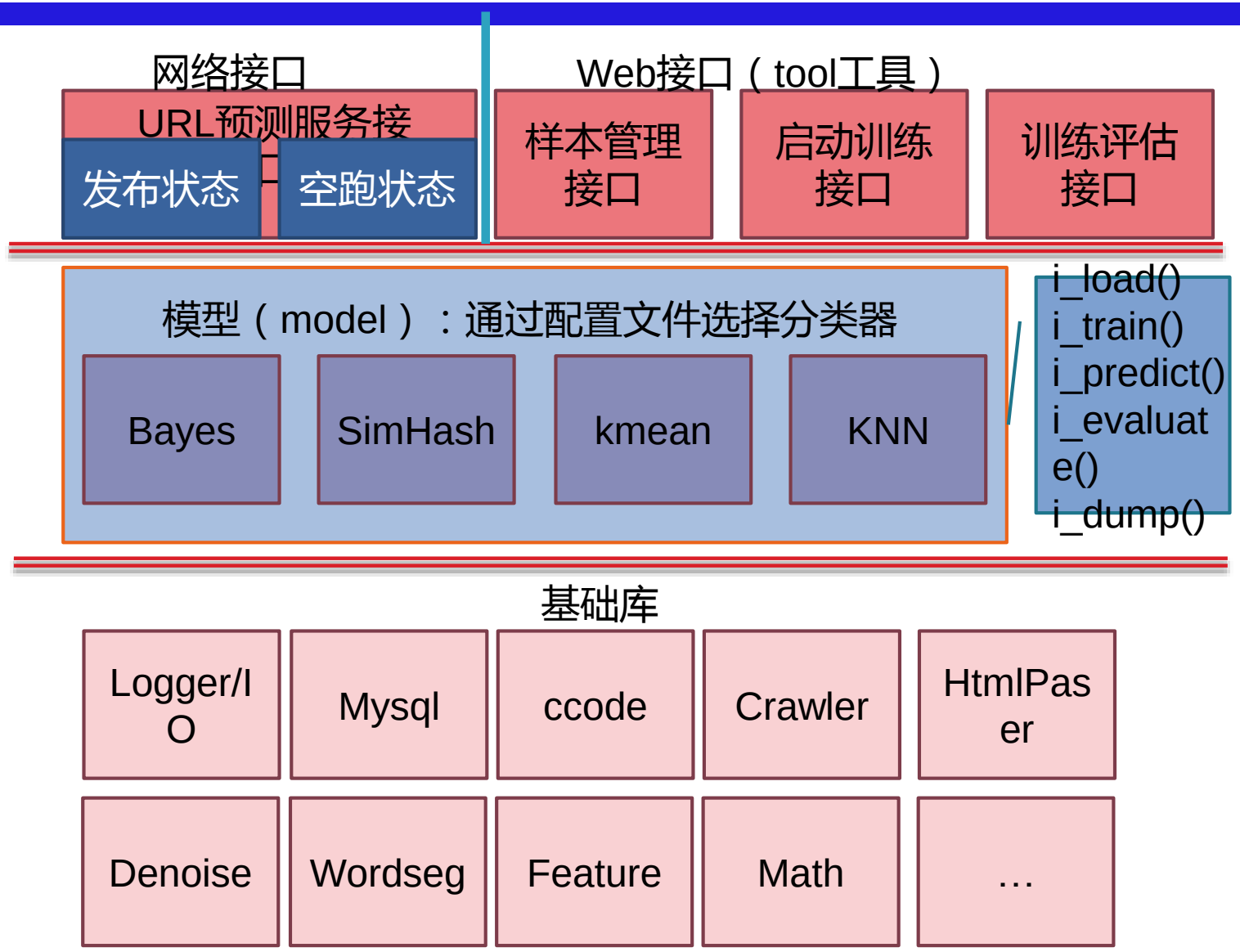
传超长参数则判为恶意

网购安全引擎 – 病毒防护技术

- 网页嵌入文件本身为有害，通过查询PE引擎来判断网页是否有害
  - 例如网页www.a.com中包含代码：<embed src=nb.swf>
  - 查询PE引擎www.a.com/nb.swf是否有害
  - 有害则拉黑原始链接

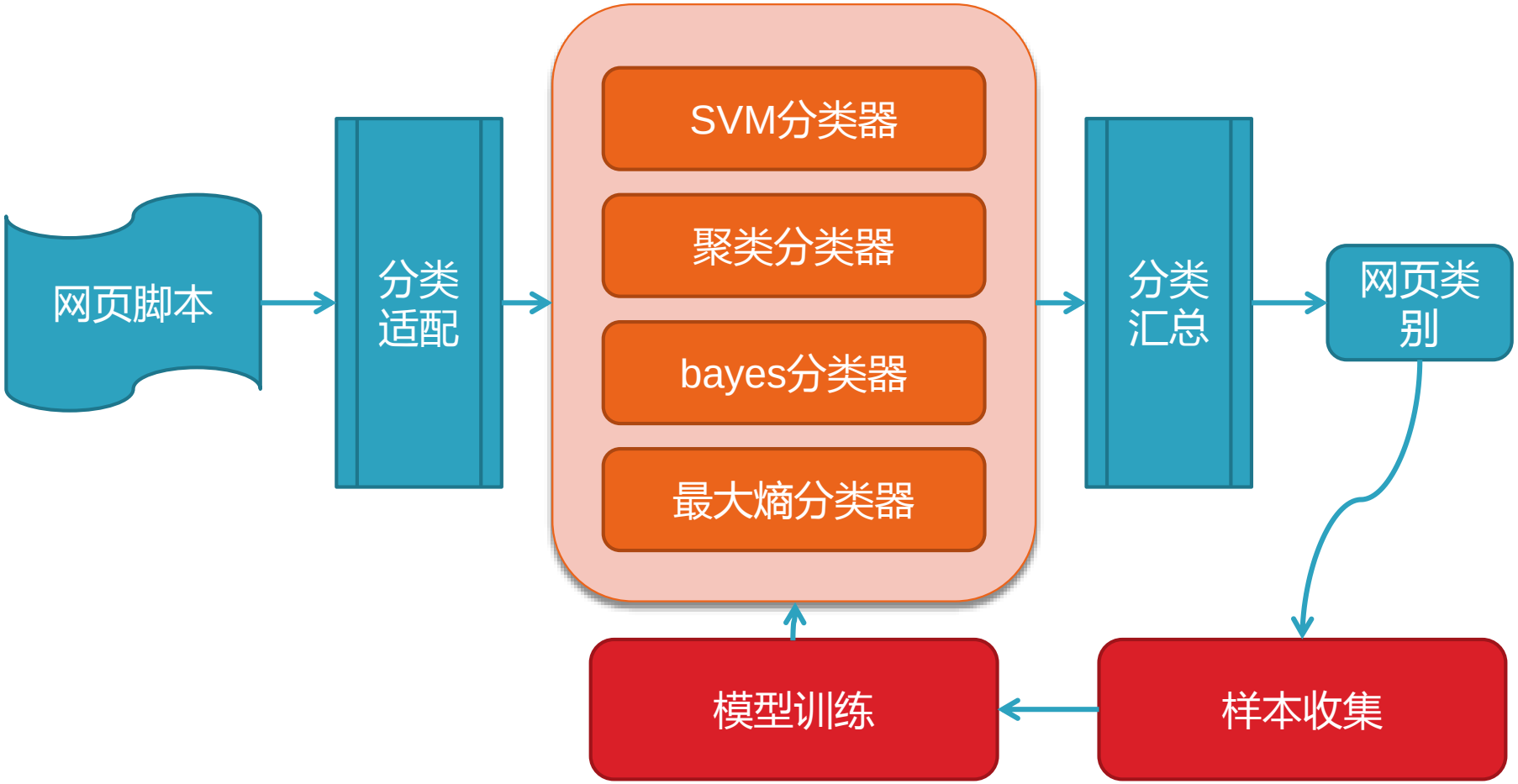


网购安全引擎 – 自然语言处理技术



网购安全引擎 –自然语言处理技术

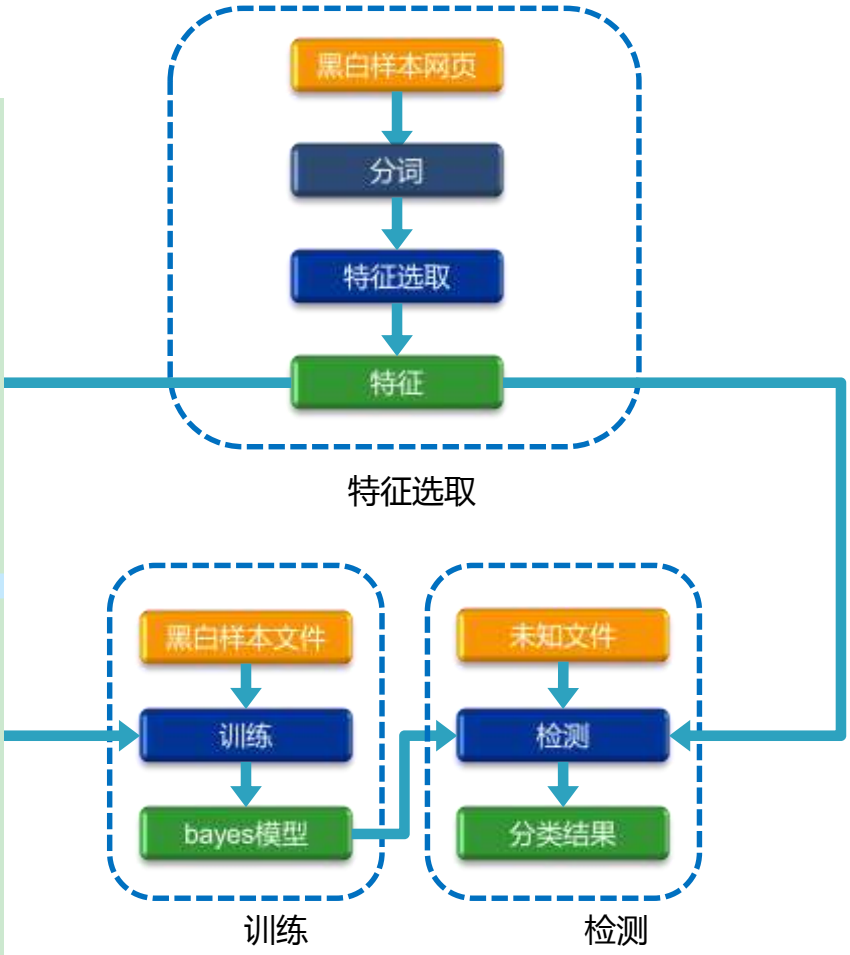
- 网页分类技术



网购安全引擎 –自然语言处理技术

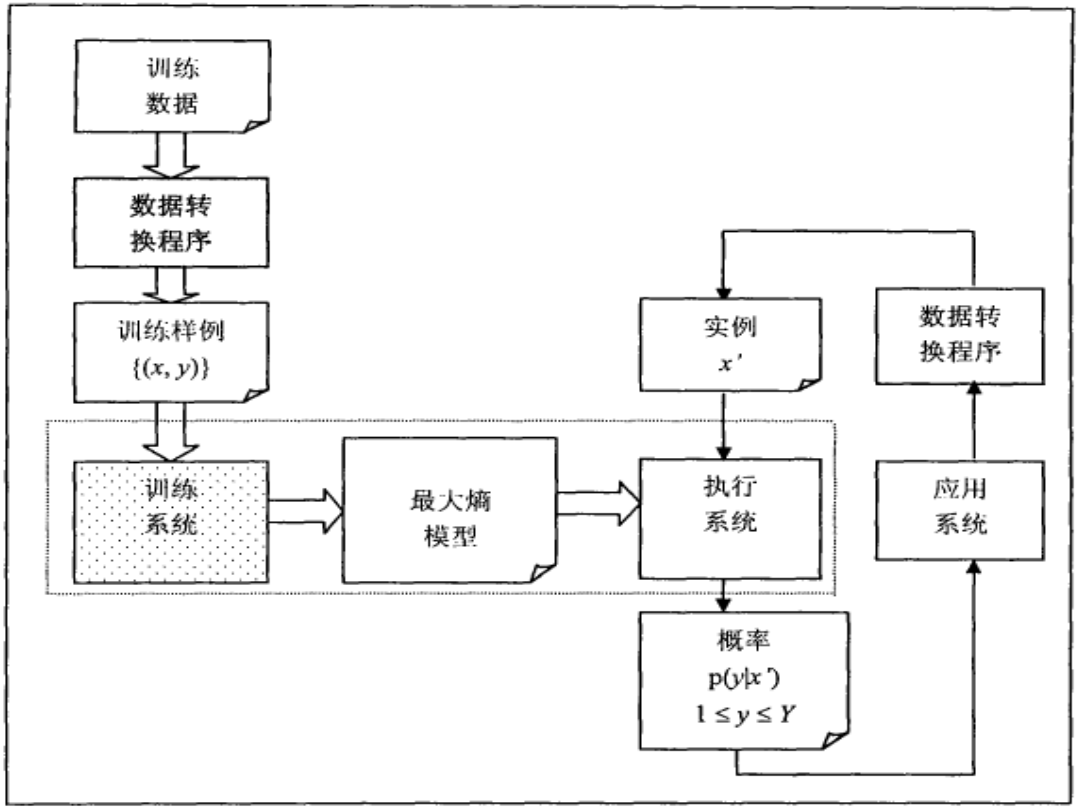
- 网页分类技术 - Bayes：

3D, 0.001933, 2	3D, 0.103151, 2
888真人, 0.004695, 1	888真人, 0.000172, 1
88娱乐城, 0.003038, 1	88娱乐城, 0.000172, 1
E世博, 0.004143, 1	E世博, 0.000172, 1
KK娱乐城, 0.000368, 1	KK娱乐城, 0.000172, 1
TT娱乐城, 0.004971, 5	TT娱乐城, 0.000172, 5
百家乐, 0.038203, 8	百家乐, 0.000172, 8
宝马, 0.002393, 2	宝马, 0.014810, 2
博狗, 0.006536, 1	博狗, 0.000172, 1
彩民, 0.019332, 1	彩民, 0.019976, 1
返水, 0.003038, 1	返水, 0.000172, 1
福彩, 0.004879, 2	福彩, 0.054417, 2
皇城国际, 0.001105, 1	皇城国际, 0.000172, 1
皇冠开户, 0.003590, 4	皇冠开户, 0.000172, 4
皇冠现金, 0.005984, 10	皇冠现金, 0.000172, 10
皇冠足球, 0.004971, 1	皇冠足球, 0.000172, 1
皇家, 0.004235, 3	皇家, 0.004650, 3
金宝博, 0.003958, 2	金宝博, 0.000172, 2
开奖, 0.020344, 2	开奖, 0.033752, 2
利记, 0.004603, 5	利记, 0.000172, 5
立博, 0.001749, 1	立博, 0.000172, 1
六合彩, 0.050078, 1	六合彩, 0.000172, 1
免费, 0.031023, 4	免费, 0.107629, 4
全讯网, 0.014545, 5	全讯网, 0.000172, 5
赛马会, 0.020989, 4	赛马会, 0.000172, 4
收藏本站, 0.004695, 1	收藏本站, 0.004994, 1
首页, 0.015005, 1	首页, 0.065266, 1
太阳城开户, 0.002946, 7	太阳城开户, 0.000172, 7
太阳城亚洲, 0.001197, 1	太阳城亚洲, 0.000172, 1
淘金盈, 0.001841, 1	淘金盈, 0.000172, 1
投注, 0.015834, 3	投注, 0.035819, 3
伟易博, 0.001473, 1	伟易博, 0.000172, 1
亚洲, 0.010402, 5	亚洲, 0.011710, 5
盈丰国际, 0.003314, 1	盈丰国际, 0.000172, 1
云顶国际, 0.001381, 3	云顶国际, 0.000172, 3



网购安全引擎 –自然语言处理技术

- 网页分类技术
  - 最大熵：
    - 特征选取
    - 模型选择：SCGIS算法



UrlPathLength
UrlWord
UrlPathWord
UrlSiteWord
UrlDateEnd
UrlStandardDateContentEnd
UrlStandardEnd
AnchorWord
HtmlTag
HtmlAttr
TagCombineAttr
TagCombineAttrValueLength
TagTextLength
TagCombineAttrNumber
TagInfoValue
TagInfoText
AllText
PureText
StylePureText
NotAnchorPureText
XPathInfo
RetinaHtmlTag
RetinaTagInfoValue
RetinaTagInfoText
RetinaPureText

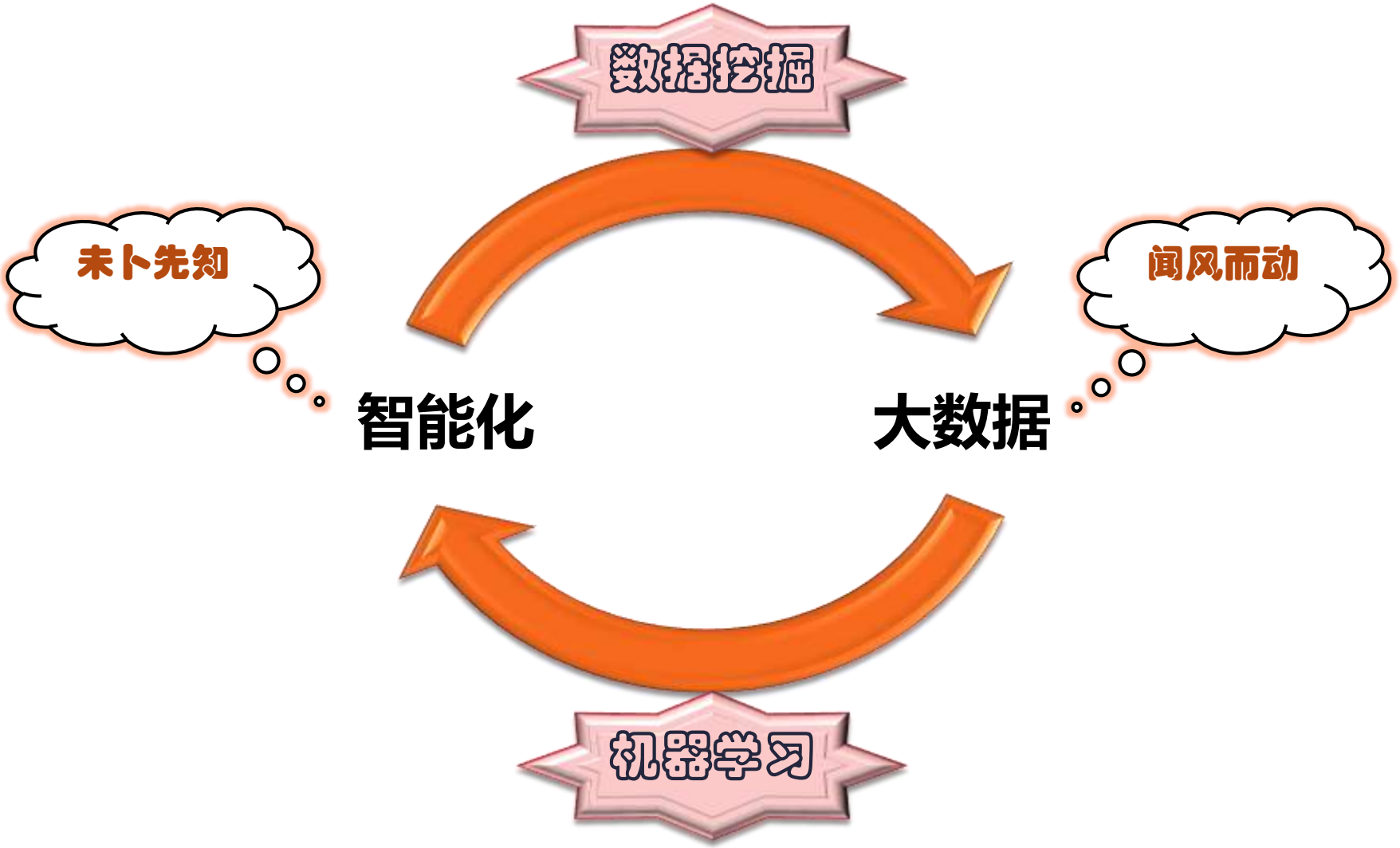
MaxRepeatVnodeYpos
MaxRepeatVnodeXpos
MaxRepeatVnodeArea
MaxRepeatVnodeMaxDepth
MaxRepeatVnodeWx
MaxRepeatVnodeHx
MaxRepeatVnodeMaxSameDepthLinkPicNum
MaxRepeatVnodeBeforeTextLen
MaxRepeatVnodeRepeatNum
MaxRepeatVnodeAvgLinkLen
MaxRepeatVnodeAvgTextLen
MaxRepeatVnodeAvgArea
MaxRepeatVnodeId
MaxRepeatVnodeDepth

网购安全引擎 –自然语言处理技术

- 网页信息抽取
  - 恶意电话号码
  - 恶意电子邮件
  - 恶意汇款信息

欢迎大家与我们**分享**和**共享**数据

网购安全引擎 –自然语言处理技术



结论 – 欺诈猖獗的原因

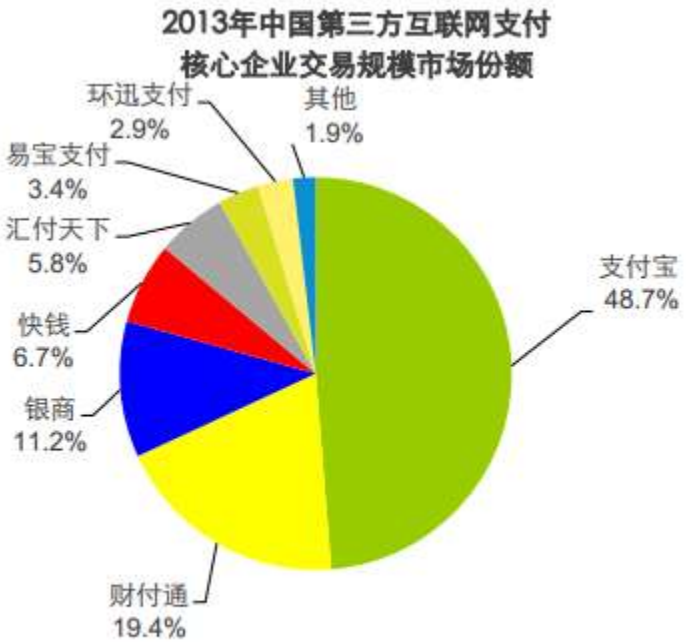
- 追回率低
  - 恶意账户信息作假，难以追踪
  - 案件频发，单价小，数量多
  - 手段变化多端
- 许多网站的安全意识不强
- 用户的安全意识不强
- 责任的相互推诿

结论 – 提高检出率

- 自然语言处理技术可以降低恶意程序的传播效率
- 病毒防护技术可以阻止病毒和其他可疑行为的发生
- 俩种技术综合运用，提高恶意行为检出率，降低网购风险

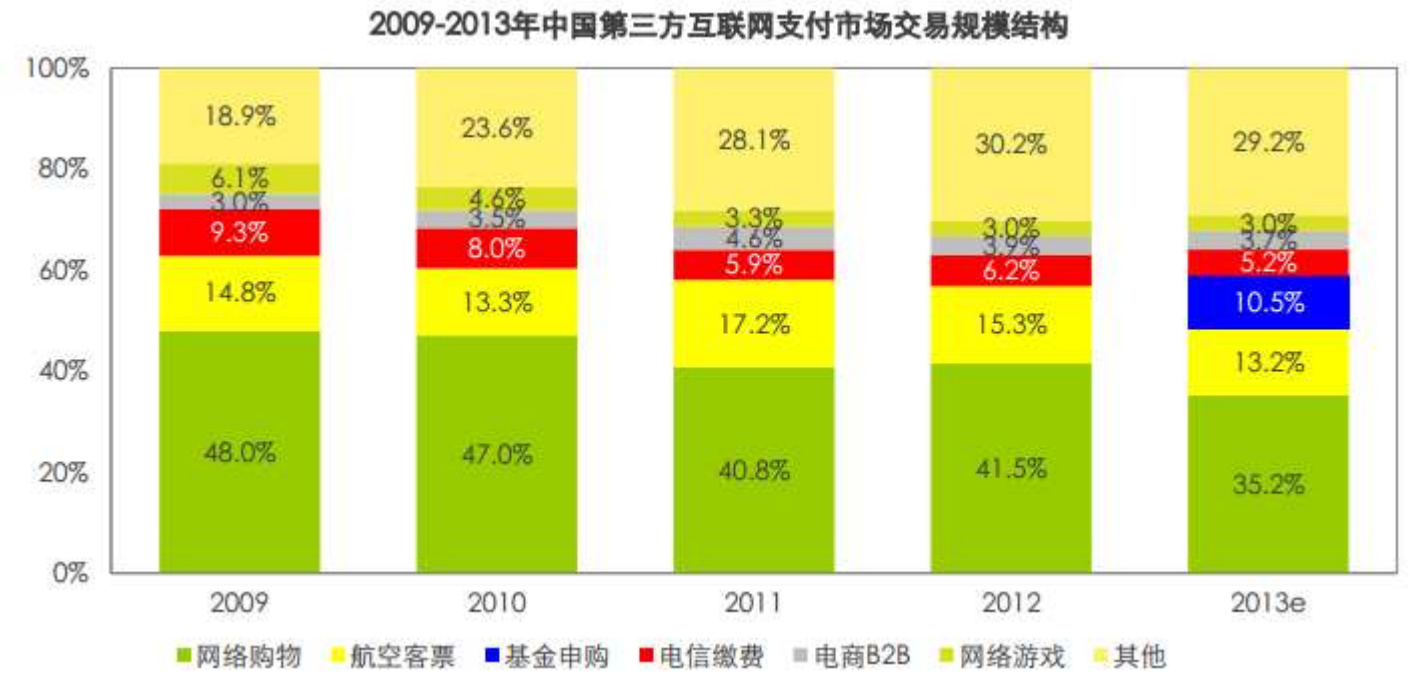
附录：互联网支付 – 规模

- 2013年中国第三方互联网支付市场交易规模达53729.8亿，同比增长46.8%，整体市场持续高速增长
- 2013年中国第三方互联网支付核心企业交易规模市场份额相对保持稳定。支付宝以48.7%的占比依然保持领先



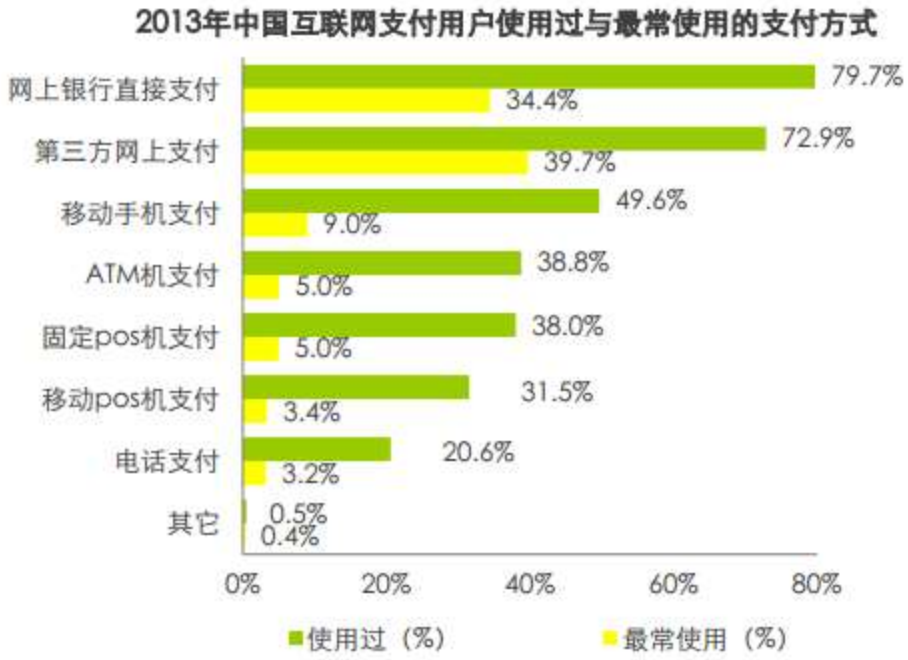
附录：互联网支付– 支付对象

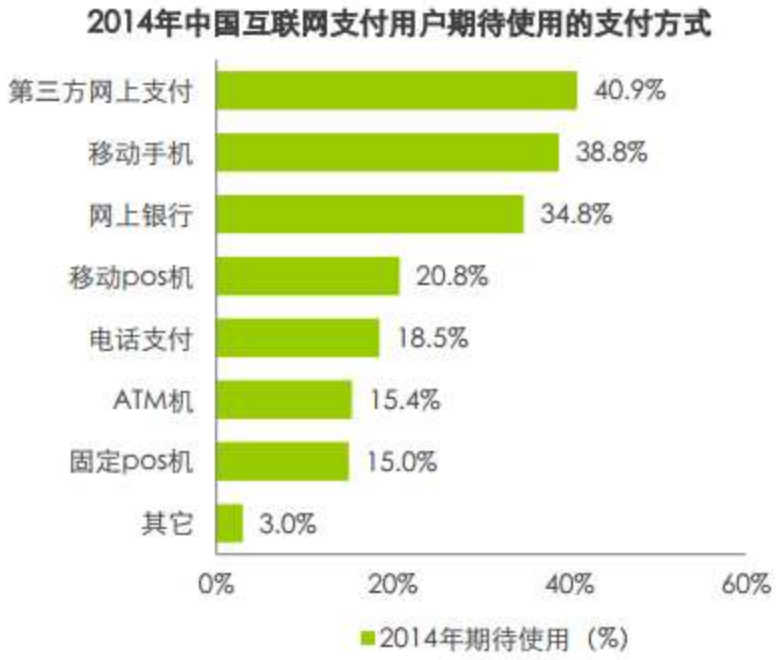
- 2013年中国第三方互联网支付交易规模结构中网络购物依然占据最大份额



附录：网购市场 – 支付方式

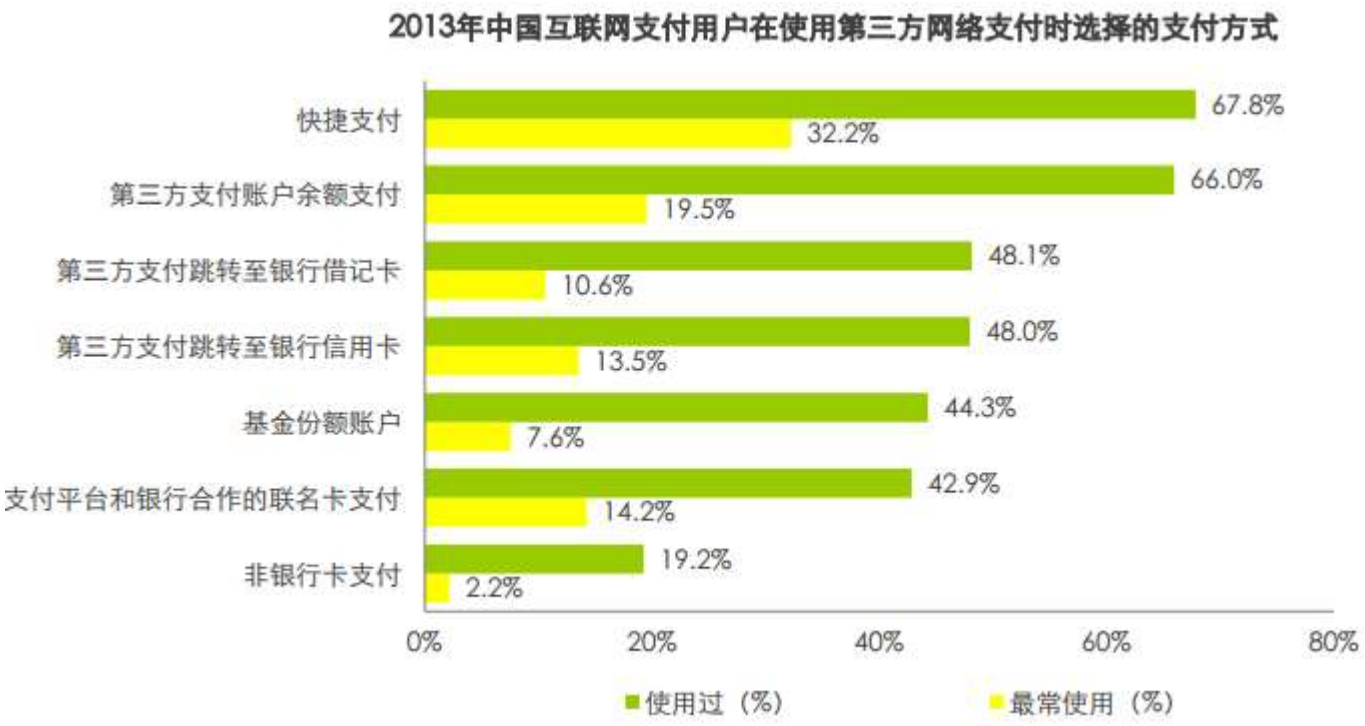
- 中国互联网支付用户使用最多的两种支付方式为网上银行直接支付和第三方网上支付
- 移动支付将成未来支付的新趋势





附录：网购市场 – 支付方式

- 快捷支付是第三方网络支付用户最常使用的支付方式



附录：网购市场 – 现状

- 2013年中国第三方互联网支付市场交易规模达53729.8亿，同比增长46.8%，整体市场持续高速增长
- 网络购物依然占据最大份额
- 第三方网上支付为用户最常使用的支付方式，占比39.7%
- 44.0%的用户使用第三方网络支付的频率为月均1-4次
- 83.8%的用户最常使用支付宝作为第三方网络支付平台
- 支付宝、银联在线与腾讯财付通是最常使用的三种第三方支付方式
- 67.8%的用户选择快捷支付作为第三方网络支付最常使用的支付方式