金融科技助力支付安全

杨阳 中国银联电子商务与电子支付国家工程实验室首席安全技术专家

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China

目录

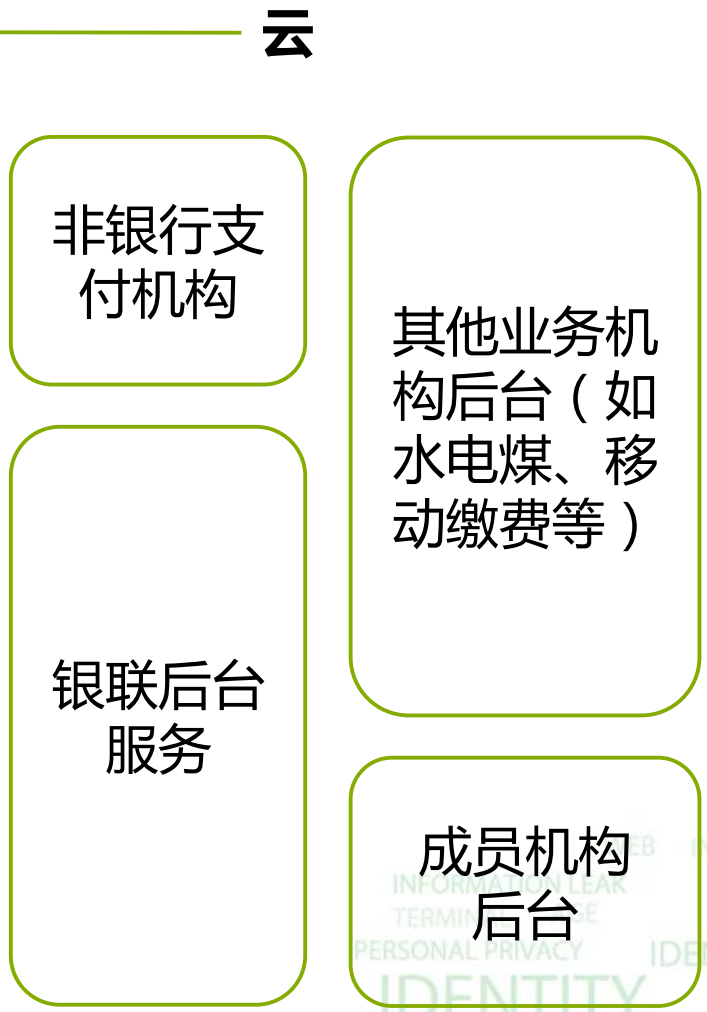
电子支付安全研究背景

电子支付网络基本架构

常见电子支付安全风险

电子支付面临新的安全挑战

电子支付网络基本架构



常见电子支付安全风险

入侵检测与防御　社工攻击　内网渗透　APT攻击　管理缺陷利用

软件开发安全　生命周期管理失控　后门植入　业务逻辑缺陷

端	管	云
APP安全 缓冲区溢出　重打包　逆向工程	**网络安全** HTTPS 钓鱼WiFi 伪基站 中间人	**系统安全** 操作系统/中间件/数据库缺陷 不安全配置
身份识别与认证 POS移机　伪卡 持卡人身份识别		**Web安全** XSS　SQL注入 DDoS　CSRF
可信计算 开放系统的安全隐患		**数据安全** 数据泄露　非法访问　隐私保护

安全漏洞与恶意代码　病毒　木马　漏洞

密码算法与安全协议

电子支付面临新的安全挑战

新挑战层出不穷……

安全事件

国内某大型旅行服务公司 部分信用卡明文信息泄露

韩国 近半数信用卡信息泄露

全球 WannaCry勒索病毒肆虐

新技术新业务

大数据 安全威胁与攻击隐藏的更深

智能化 与人身安全、隐私密切相关

云计算 所有权和控制权分离，传统的竖井式隔离消失

移动互联网 “体验为王”，产生新的信息安全洼地

外部攻击

特点 攻击后获利比较直接

数量 针对支付企业的攻击日渐增多

攻防对抗

木桶效应 一块没防住则满盘皆输

螺旋式上升 “道高一尺、魔高一丈”的不断博弈中

ZERO TRUST SECURITY

电子支付安全研究体系

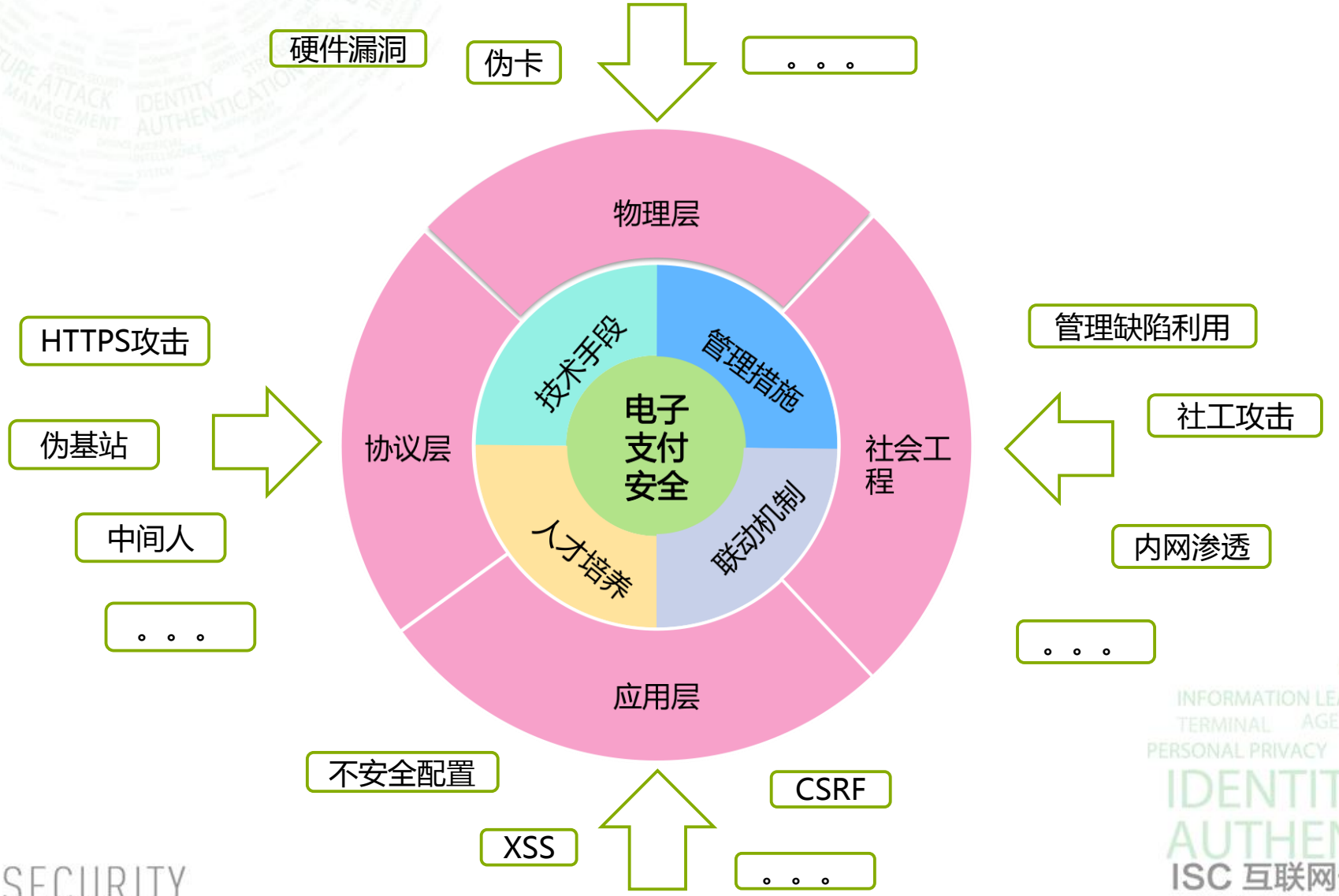
电子支付安全研究模型

安全研究平台框架与部署方案

研究方向

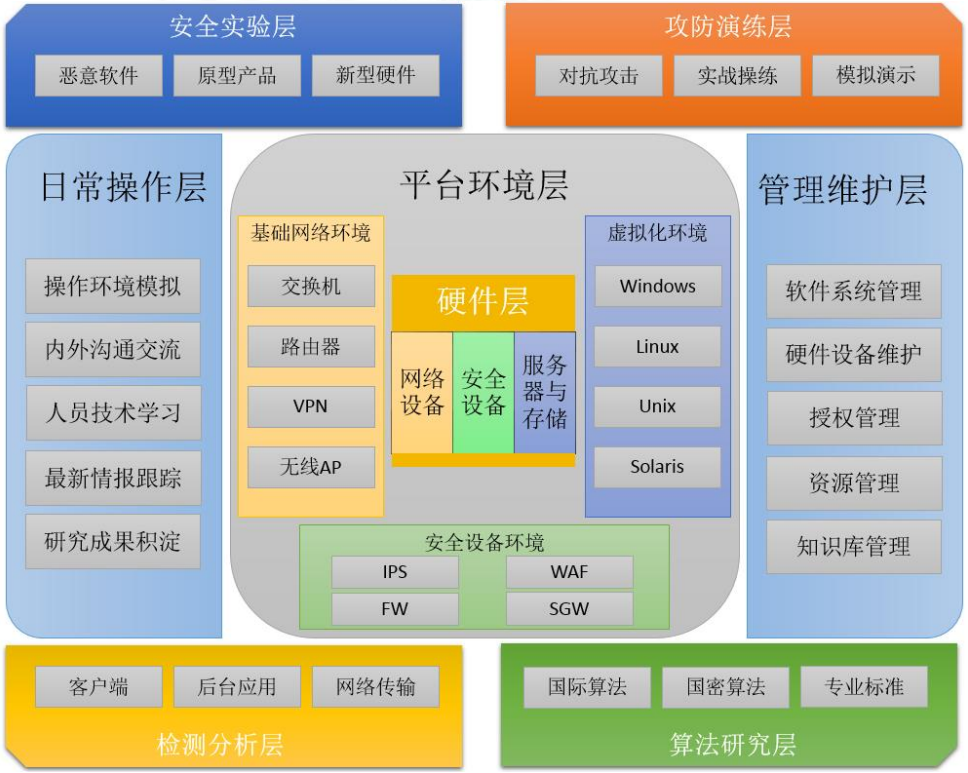
ZERO TRUST SECURITY

电子支付安全研究模型

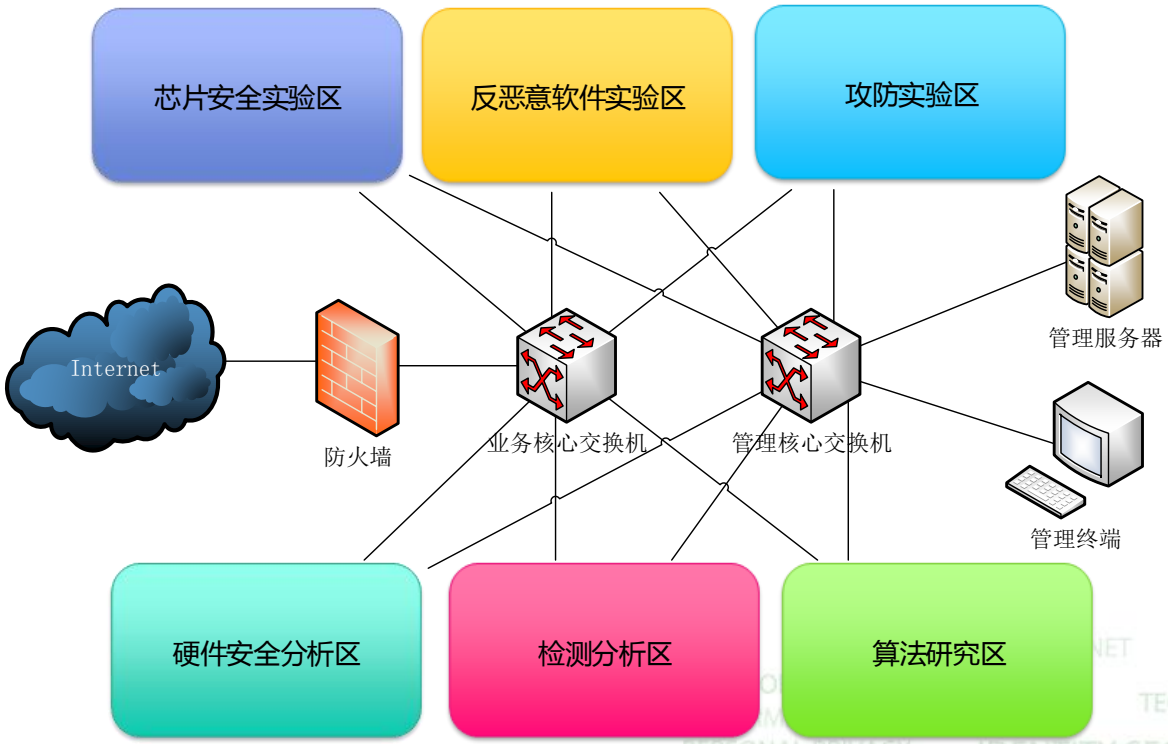


安全研究平台框架与部署方案

安全研究平台框架



安全研究平台部署方案



研究方向

方向	说明
检测平台	为电子支付安全攻防技术研究提供基础设施支撑
密码算法与协议	为电子支付安全攻防技术研究提供基本理论支持，包括国密算法、ECC/RSA密钥长度评估、SSL协议最佳实践、EMV/PCI标准等
芯片/硬件安全	研究IC卡侧信道攻击，下一代云加密机构架、TEE等
移动支付安全	深入探究手机操作系统的弱点、应用漏洞；对当前影响较大的短信验证码、病毒、伪基站等关键安全点，形成安全防护方案
网络安全	完成常见网络攻击的种类梳理，并形成对应的防御方案；同时对新兴的SDN安全、大数据安全分析等方向进行技术储备和原型研究
Web安全	对SQL注入、XSS、CRSF、撞库等Web攻击进行深入研究，形成检测和应对方案，同时对HTTP2.0等新协议进行预研
威胁情报	利用外部信息导入，进一步提升威胁发现的准确性。
基于AI的安全	将人工智能技术应用在攻击检测等相关领域（如APT、钓鱼网站、CC攻击检测等）
新兴方向预研	当前主要集中在区块链安全与物联网安全等方向

电子支付安全研究成果

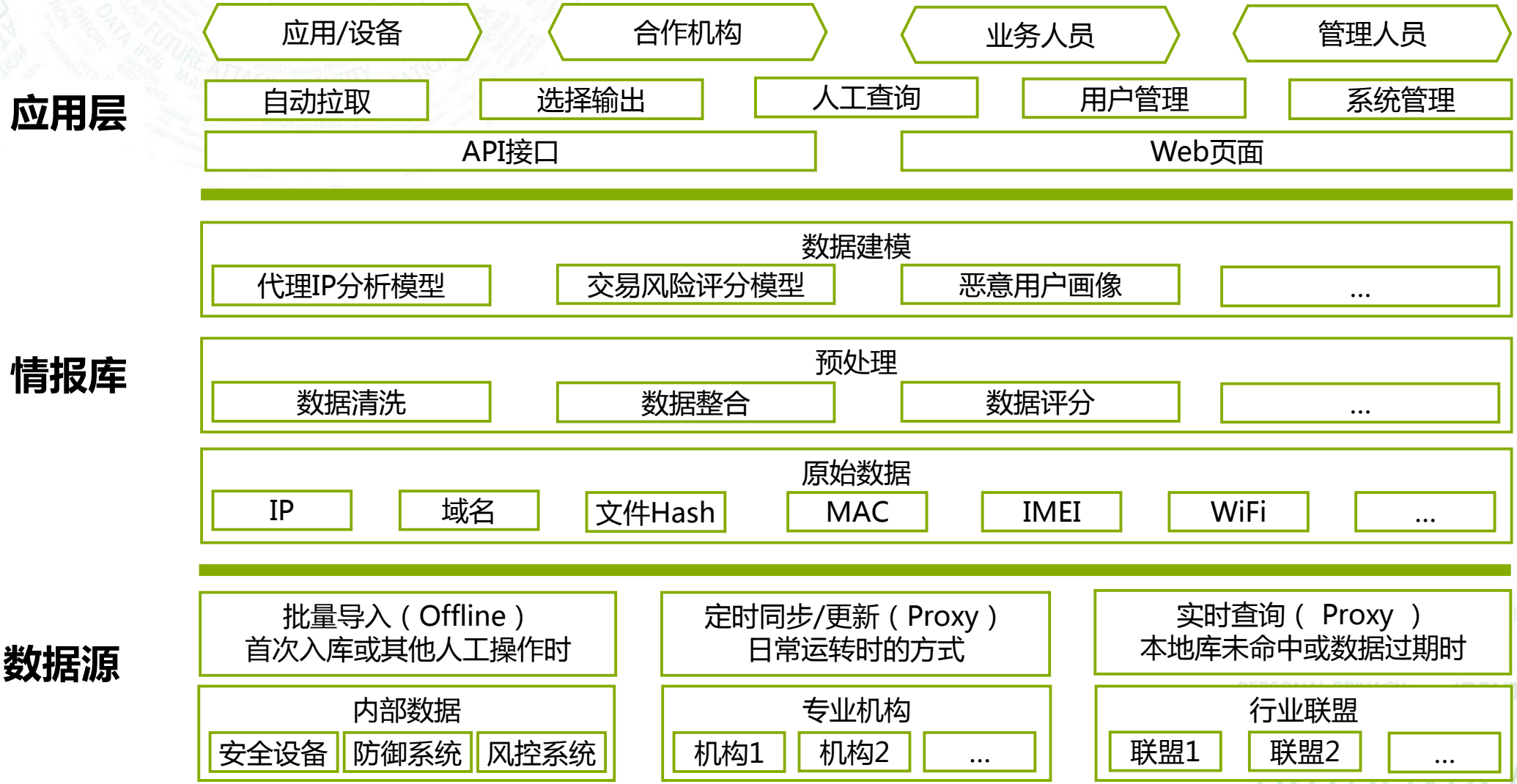
威胁情报情报库

网络流量分析

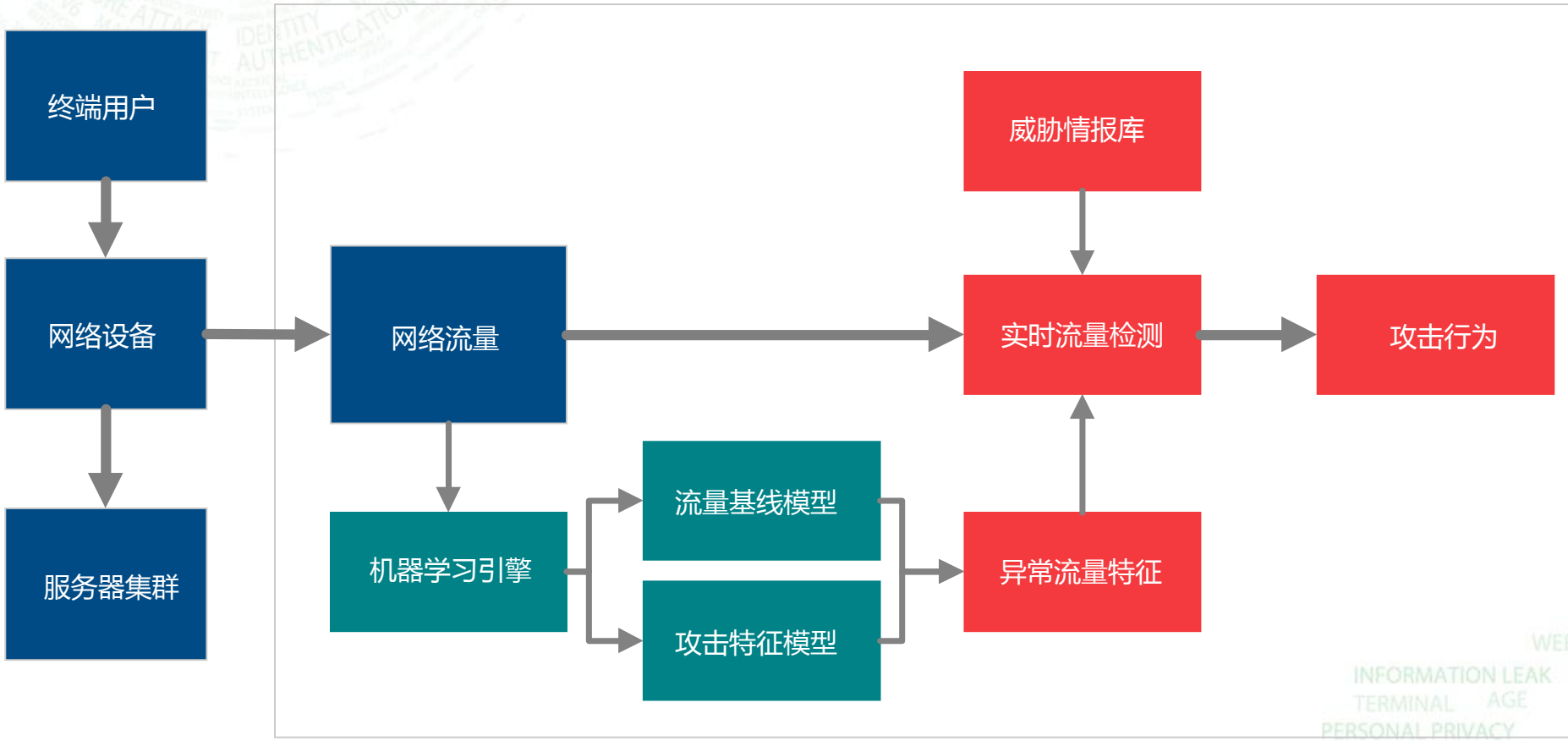
国密算法研究

其他研究成果

威胁情报情报库


应用层
应用/设备
合作机构
业务人员
管理人员
自动拉取
选择输出
人工查询
用户管理
系统管理
API接口
Web页面
情报库
数据建模
代理IP分析模型
交易风险评分模型
恶意用户画像
...
预处理
数据清洗
数据整合
数据评分
...
原始数据
IP
域名
文件Hash
MAC
IMEI
WiFi
...
数据源
批量导入（Offline）
首次入库或其他人工操作时
定时同步/更新（Proxy）
日常运转时的方式
实时查询（ Proxy ）
本地库未命中或数据过期时
内部数据
安全设备
防御系统
风控系统
专业机构
机构1
机构2
...
行业联盟
联盟1
联盟2
...

网络流量分析


终端用户
网络设备
服务器集群
网络流量
机器学习引擎
流量基线模型
攻击特征模型
威胁情报库
实时流量检测
异常流量特征
攻击行为

国密算法研究

安全是电子支付的核心，而算法是安全的基础。

国密算法是国家密码局制定标准的一系列算法。其中包括了对称加密算法、椭圆曲线非对称加密算法、杂凑算法等。为响应国家“安全可控”的政策要求，推动金融机构信息安全的发展，我们进行了国密算法的研究。

算法分析

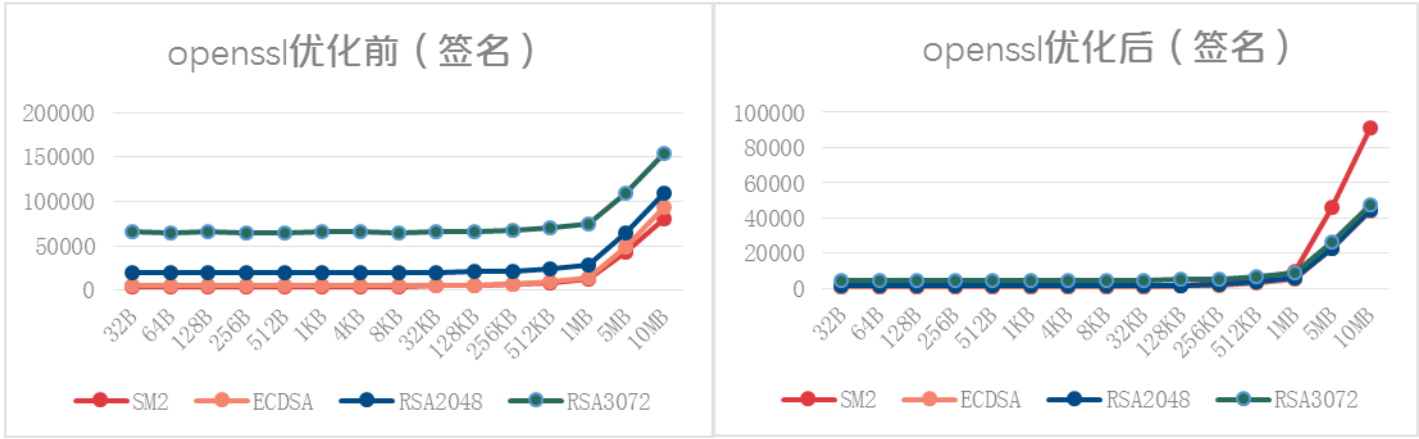
算法框架、算法流程、计算量分析

实现优化分析

对象 包括SM2/ECDSA/RSA/ECIES、SM3/SHA256、SM4/AES/3DES等算法，通过编写C语言测试代码，调用OpenSSL/**GmSSL**等开发包的相应接口，分别对各种算法进行性能测试。

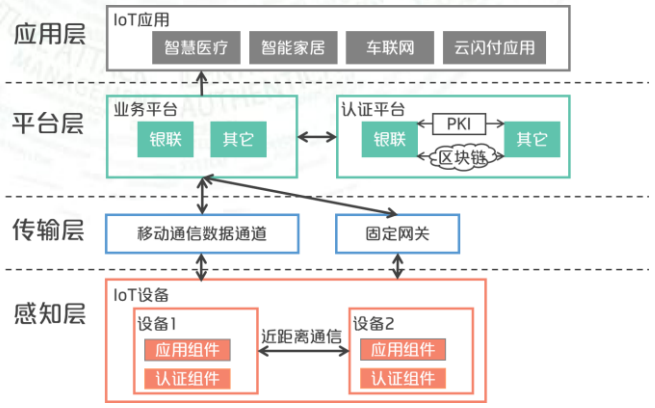
结果 国密算法的在实现时，优化较少

优化方向 汇报优化是基础且有效的优化方式；ECC曲线的选择和快速算法对结果影响非常大；对称加密如能获得硬件加速支持将可取得较好的效果。



SM2/ECDSA/RSA的签名对比

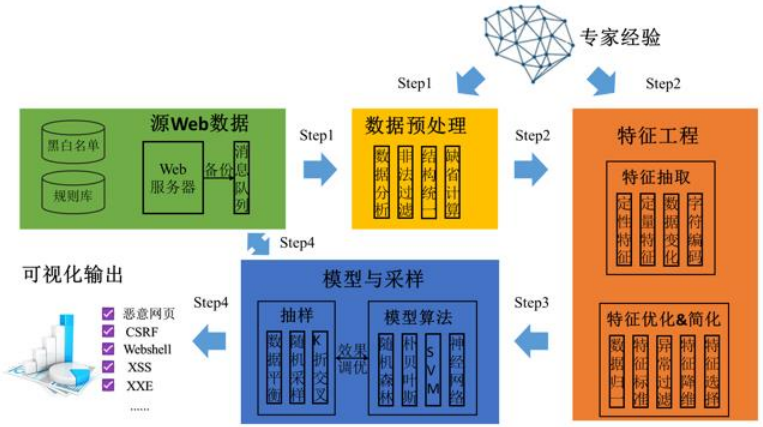
其他研究成果



物联网安全认证

网络安全攻防与态势感知

移动APP安全攻防



人工智能在Web安全领域的应用

我们还关心和研究这些

大数据安全

可穿戴设备安全

无线安全

区块链安全

隐私保护

身份认证

APT攻击

免密认证

ISO27001安全管理体系

软件定义安全

FIDO

……

ZERO TRUST SECURITY


ISC
2018
ISC互联网安全大会
360互联网安全中心
谢 谢！
ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China