物联网与移动支付的安全碰撞

陈家林　　安天移动安全副总经理

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

目录

物联网助力移动支付2.0

物联网成就移动支付新载体

B端 + C端

移动支付B端的安全关注太少

移动支付 = 手机支付？

当我们提到移动支付。。。

C端

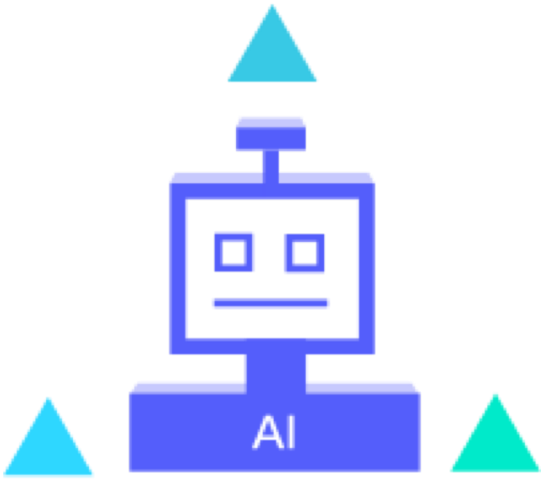
物联网成为移动支付收款端的重要载体

B端

支付B端成为巨头新入口之争

- 物联网，人工智能，大数据等技术赋能移动支付，加速产业发展
- 智能手机之后，B端已成为巨头新的入口之争

物联网



人工智能

大数据

移动支付安全 = 手机支付安全？

付款端安全
C段

移动支付安全
B + C

收款端安全
B端

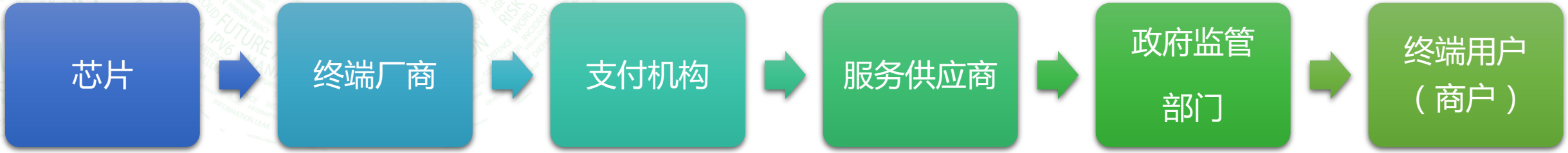
支付智能终端安全问题凸显

产业链复杂，投入低

碎片化

监管无或滞后

产业链复杂，安全在指数化降级



各个环节风险累积成指数化放大

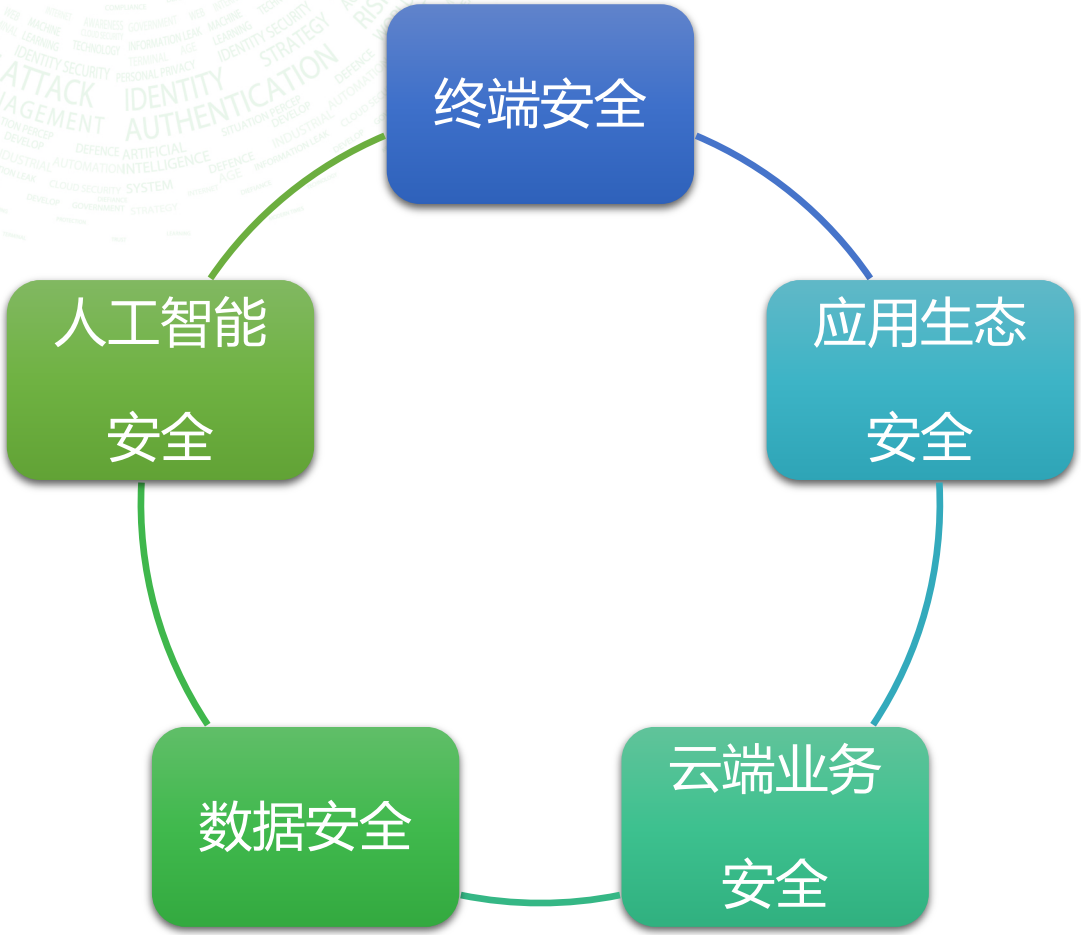
- 终端软硬件碎片化导致安全防护复杂
- 同质化竞争，价格战，安全投入严重不足
- 新形态终端无监管或标准滞后

ZERO TRUST SECURITY

大数据和人工智能的引入加剧安全风险

- 信息化，数字化，智能化需要打通更多数据，却带来更多安全隐患
- 大量交易信息导致企业核心数据泄露以及用户隐私泄露
- 人工智能的新技术引入带来更多安全风险

终端安全 ！= 终端的安全



摒弃
“我封闭，故我安全”
的执念，
拥抱开放

ZERO TRUST SECURITY

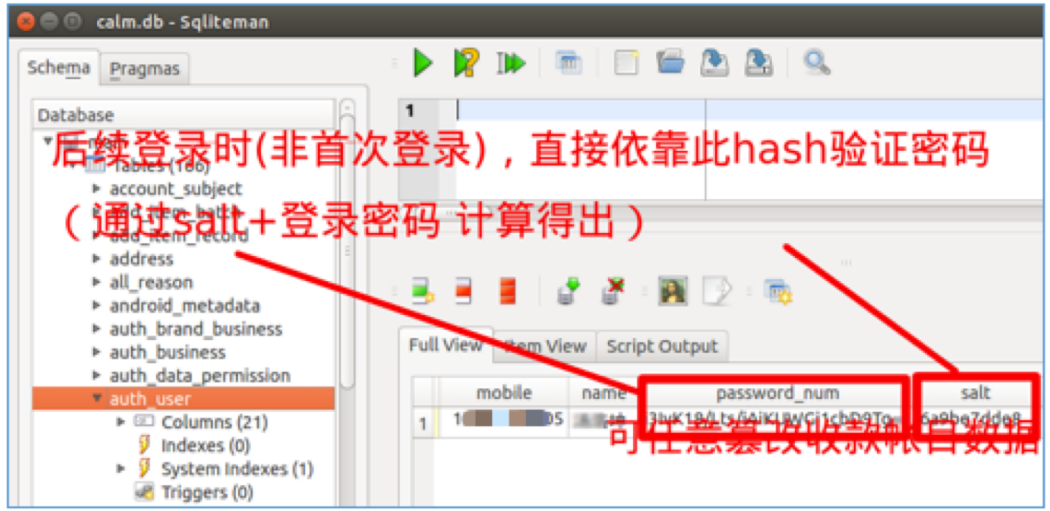
典型案例分析1 – 智能收款终端交易APP问题

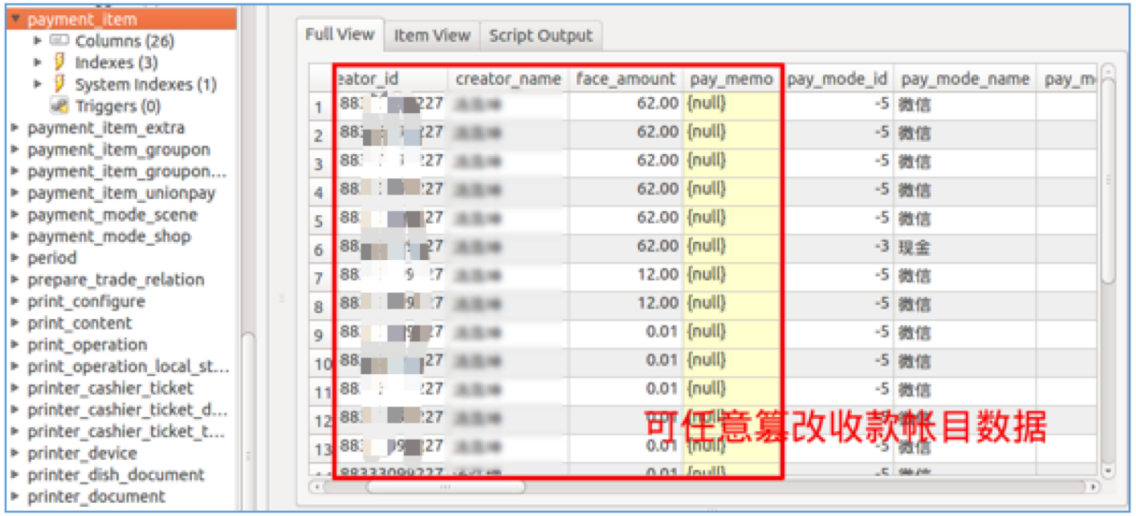
某交易应用数据库可被任意篡改业务关键数据

跟业务相关的数据库存于sdcard开放目录中，且无加密，可导致：

* 重置登录密码

* 篡改收款记录



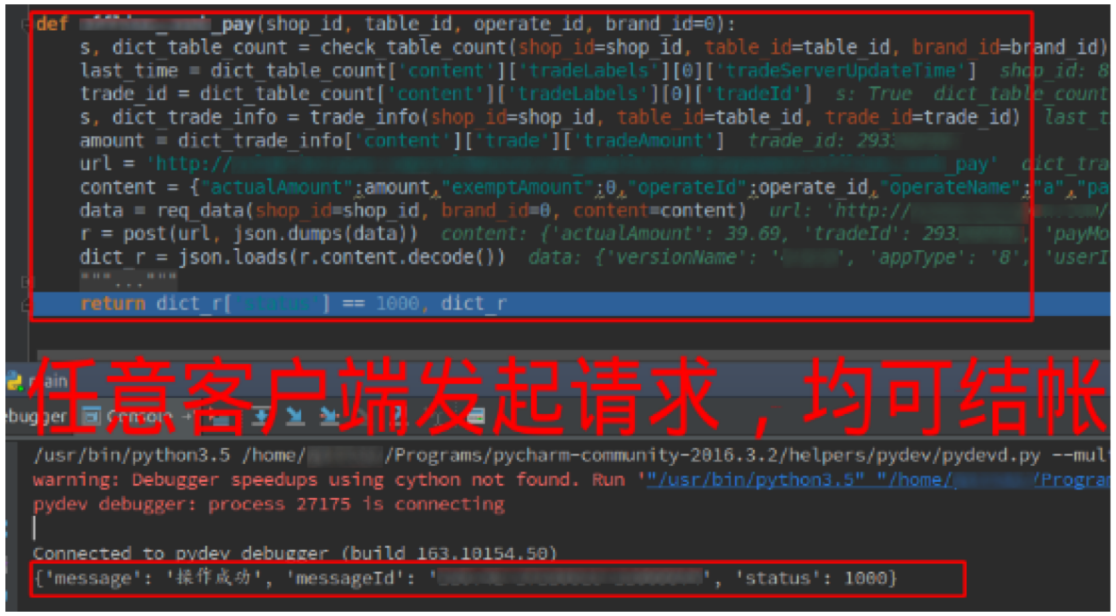


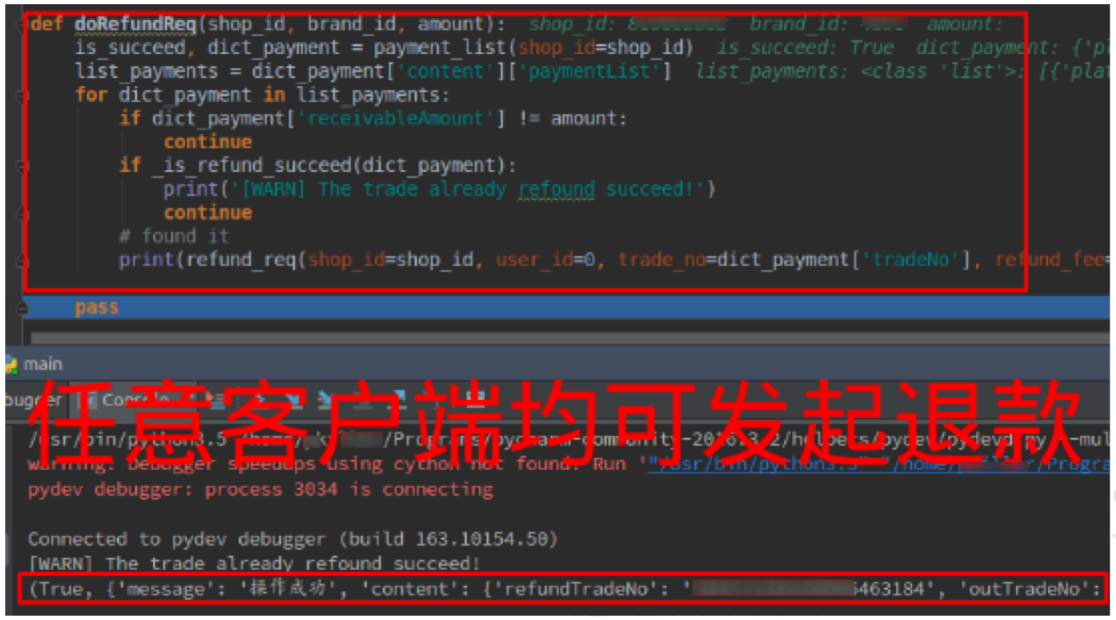
典型案例分析2 – 支付交易后台问题

某服务器结账操作未进行鉴权，进行伪造请求攻击

服务器商户接口未进行鉴权保护，无条件接受客户端发来的各种指令 ，导致：

* 攻击者可以远程对任意创建订单，随意进行“结帐”、 “退款”等等
* 仅需要一个脚本即可 —— 攻击成本极低





典型案例分析3 – 智能商业终端远程ROOT执行问题

某智能商业终端存在开放root后门，未进行鉴权保护，可进行远程提权

系统存在后台常驻进程，开启9999端口，未进行鉴权保护，无条件接受端口任意请求，导致：

* 攻击者可以远程连接设备，发送命令，以root执行

```
*(_DWORD *)&v14[1] = -1;
memset(&serverAddr, 0, 0x10u);                  // sin_addr = 0.0.0.0
serverAddr.sin_family = 2;
serverAddr.sin_port = 3879;                     // Big Endian: 9999
fdSocket = socket(2, 1, 0);
fdSocket_1 = fdSocket;
if ( fdSocket >= 0 )
{
  v15 = 1;
  setsockopt(fdSocket, 1, 2, &v15, 4);
  v19 = 0;
  v20 = 0;
  v21 = 0;
  v18 = 1;
  setsockopt(fdSocket_1, 1, 21, &v18, 8);
  setsockopt(fdSocket_1, 1, 20, &v20, 8);
  v16 = 256;
  setsockopt(fdSocket_1, 1, 8, &v16, 4);
  *(_DWORD *)&v14[1] = setsockopt(fdSocket_1, 1, 7, &v16, 4);
  if ( bind(fdSocket_1, (const struct sockaddr *)&serverAddr, 16) )// listen any client
  {
```

任意客户端可连9999端口，发送shell命令

XPWN解读 – 破解收银台

- 低版本Android，大量CVE未修复，轻松Root提权
- 为了方便下游开发，随意开放提权后门，轻松利用
- 对收银台的远程控制存在漏洞，松松接管
- 收银台App的业务机制存在漏洞，轻松伪造
- 通信采用明文等低安全等级通信方式，轻松中间人
- 收银台后台API权限管控有漏洞，轻松窃取数据

免费吃大餐！

你的订单我做主！

安天最佳实践分享

安全公司找好定位

案例1：智能POS行业安全赋能

案例2：银联手机POS项目

最佳实践1 - 智能POS行业的安全赋能

风险在哪，尽可能通过加固来防范，避免潜在危害程度/损失

威胁在哪
受害发生时间，发生位置

威胁是否清除
受害是否停止，损失是否遏制

纵深防御

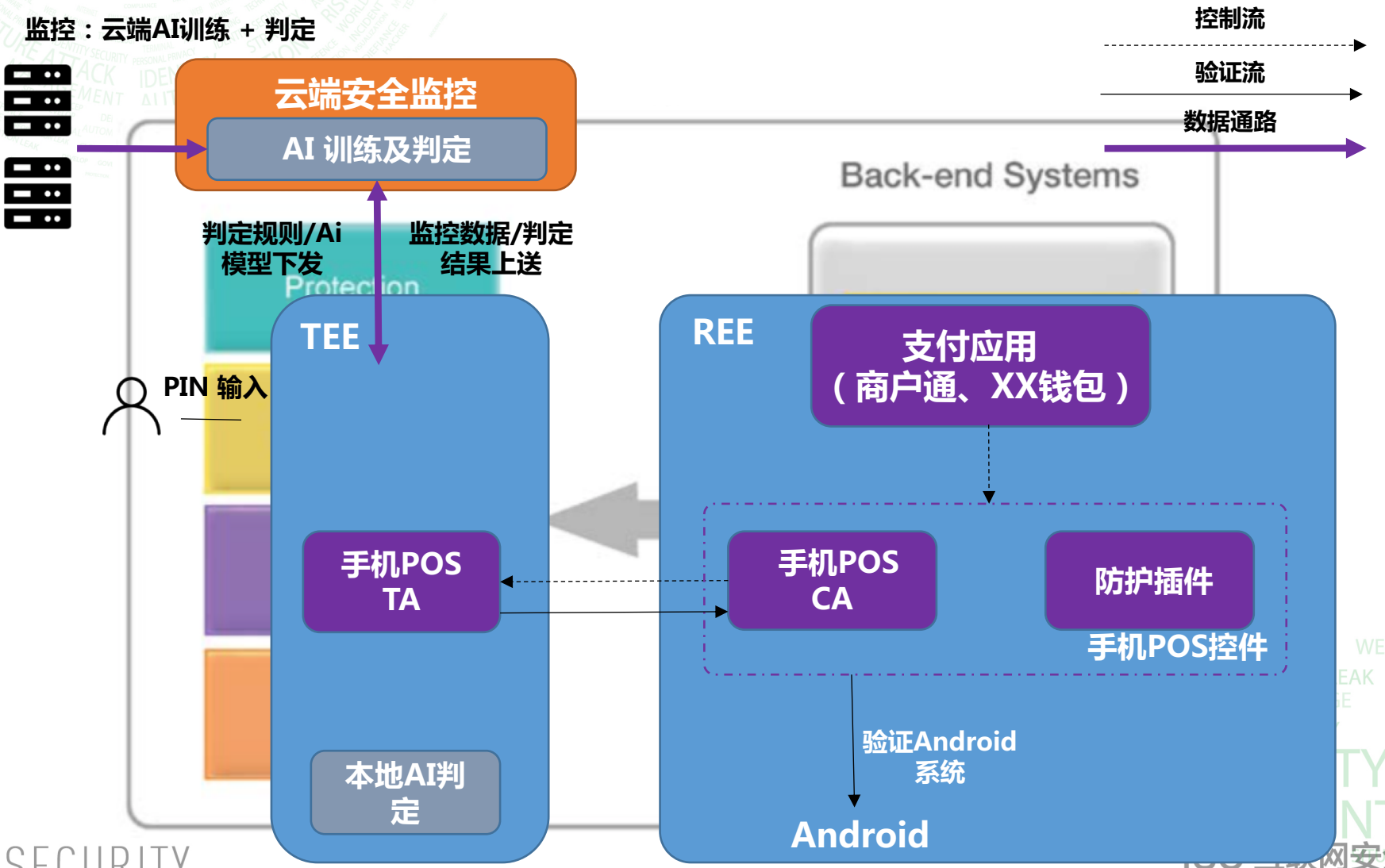
- 终端安全评测
- 应用安全评测
- 安全培训，咨询
- 威胁检测（病毒，网络）
- 漏洞动态防御
- 应用级数据安全保护
- 漏洞应急响应
- 漏洞修复

漏洞监控、终端态势感知

大数据驱动安全

ZERO TRUST SECURITY

最佳实践2 – 银联手机POS安全合作项目



未来展望

无处不在的移动支付

物联网下的大数据风控

ZERO TRUST SECURITY

海量物联网终端的大数据风控

- 物联网终端继续呈现爆发式增长
- 移动支付无处不在，抽象共性，软硬结合的支付模块化趋势即将出现
- 大数据下的商业数据和用户隐私保护越来越重视
- 用风控的思维解决不断出现的新型攻击

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

2018 ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原中国互联网安全大会）