2017 中国互联网安全大会
China Internet Security Conference

物联网时代的智能身份认证技术

蔡准

北京芯盾时代科技有限公司
技术总监

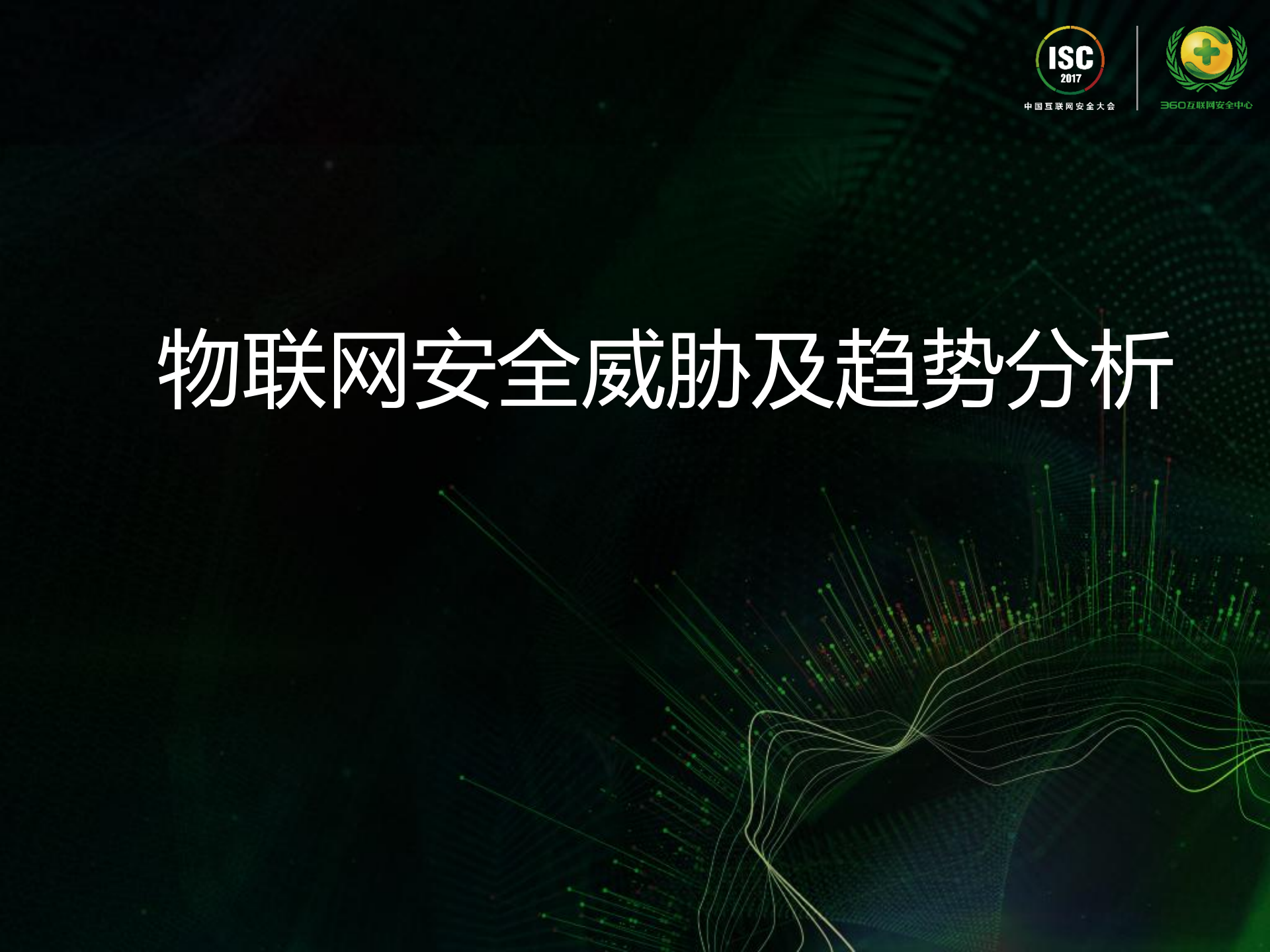
目录

- 物联网安全威胁及趋势分析
- 智能身份认证技术
- 物联网与智能身份认证

ISC 2017 中国互联网安全大会

360互联网安全中心

物联网安全威胁及趋势分析



物联网安全背景

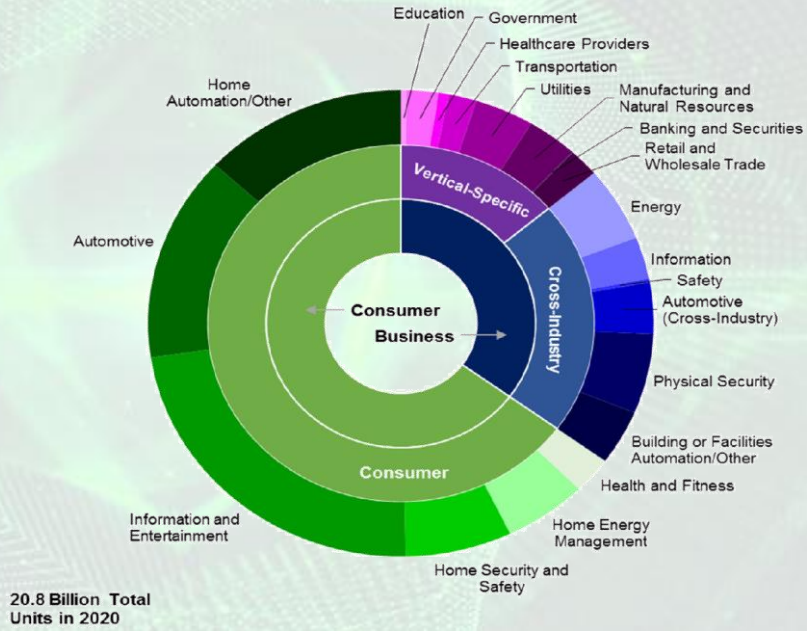
智能家居

智能穿戴

车联网

办公/楼宇

- 物联网装机容量：从2013年到2020年，物联网端点将以32%的复合平均增长率增长，达到210亿台。
- 受益于能源管理和汽车应用的推动，跨行业类别以36%的复合增长率成为最高增长类别。
- 电子产品、能源管理、家居安全、汽车等物联网消费爆发，推动消费物联网类别成为下一个高速增长类别。



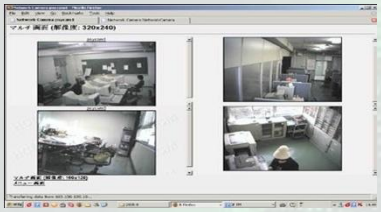
以上数据来源于Gartner报告

管中窥豹，聚焦物联网安全威胁

汽车被黑客远程操纵

- 两名互联网专家利用互联网技术侵入一辆行驶中切诺基吉普车的电子系统，远程控制了这辆车的加速和制动系统以及电台和雨刷等装置。
- 2015年7月24日，美国菲亚特克莱斯勒汽车公司在美国召回140万辆轿车和卡车，防止黑客通过互联网远程控制车辆。

摄像头被入侵



- 大量家庭智能摄像头遭破解而导致摄像头被入侵，从而利用摄像头进行偷窥，侵犯他人隐私。
- 2017年6月18日，QQ群中兜售远程控制家庭摄像头的破解软件，此类破解软件可扫描出存在漏洞的摄像头IP，不法分子利用此漏洞可远程控制摄像头。

智能家居安全事件

- 智能家居联网之后，黑客通过网络对其进行各种智能控制。惠普通过对市面上最热门的10款消费级智能家居产品进行研究分析，发现250种安全漏洞，分别来自电视、网络摄像头、家用恒温箱等。
- 2013年，心脏起搏器入侵事件。9m外入侵植入式心脏起搏器，然后发出指令，让其释放出高达830伏的电压，形成让人瞬间致命的电流。（由于很多厂商的心脏起搏器存在安全漏洞）

- ✧ 安全物联网端点数量：具有安全要素的物联网端点将从2013年的1.03亿增加到2020年的7.75亿。
- ✧ 物联网安全支出费用：用于物联网安全方面的支出费用2020年将达到8.455亿美元。
- ✧ 安全端点比例：从2013年的11.41%下降至2020年的8.14%，导致复合年均增长率为负4.7%
- ✧ IoT设备漏洞1117个（2016年CNVD数据），漏洞类型为权限绕过（23%）、拒绝服务（19%）、信息泄露（13%）、跨站（12%）、命令执行（9%）、弱口令（2%）等十大类风险

物联网安全威胁现状及风险分析

物联网行业所面临的安全威胁，从终端节点到感知网络、通信网络，从应用层面到管控层面，以及一些非技术层面的因素都关联和影响着物联网的安全问题。

ISC 2017 中国互联网安全大会

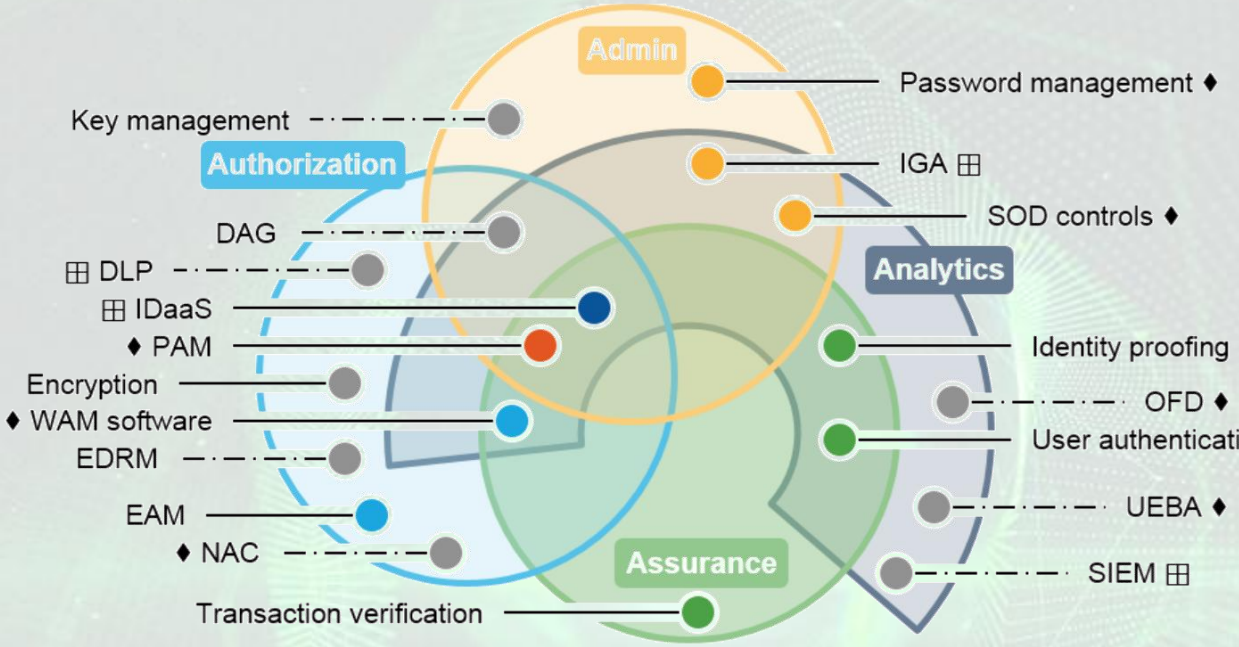
360互联网安全中心

智能身份认证技术

——不基于单一认证凭证的动态身份认证方法

我们是如何认证身份的

身份认证领域，由最初的口令管理、密钥管理，发展到网络访问控制、数据访问控制，再到IDaaS。管理范围已经从简单的信息管理扩展到身份相关全生命周期管理。



身份认证技术正发生本质的变化

Gartner《Hype Cycle for Identity and Access Management Technologies 2017》

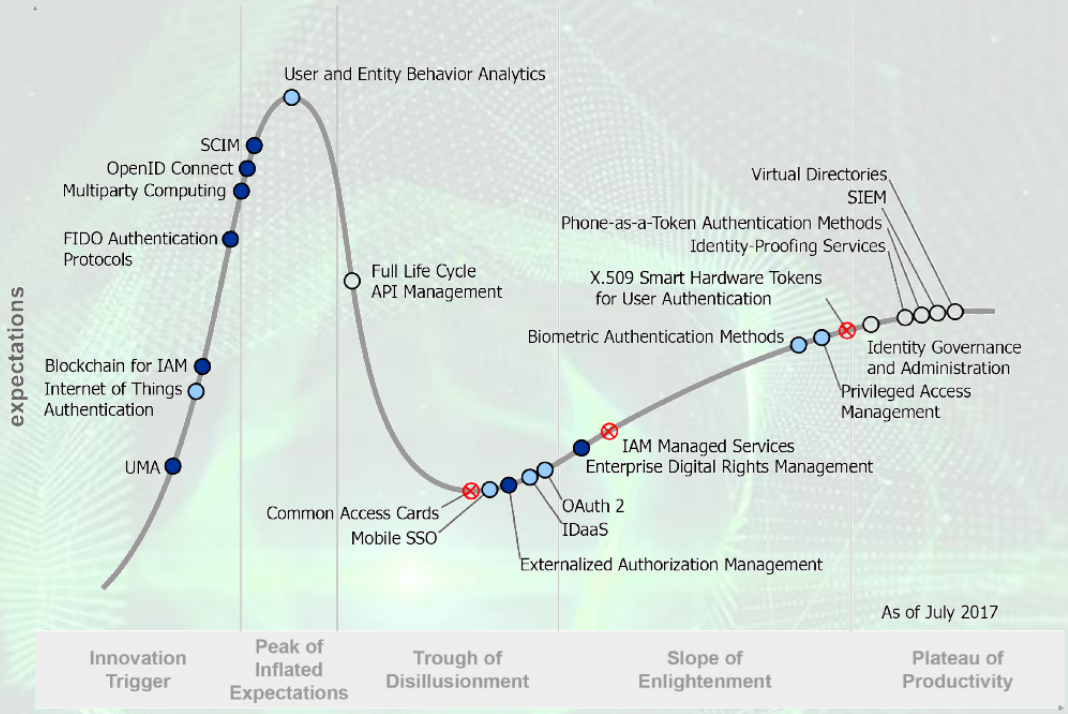
IoT Authentication：因物联网的广泛应用而逐渐兴起，利用新的安全技术解决新的场景问题。

User and Entity Behavior Analytics：使用大数据分析和机器学习模型，进行用户行为分析。

Biometric Authentication：生物特征识别，逐渐进入主流技术行列，商用化程度提高。

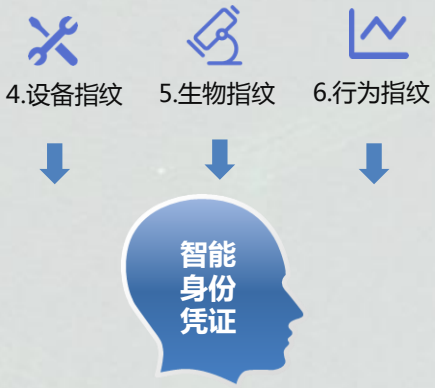
IDaaS：云服务的基础上，将身份作为一种服务进行提供。目前已经进入成熟期。

Figure 1. Hype Cycle for Identity and Access Management Technologies, 2017



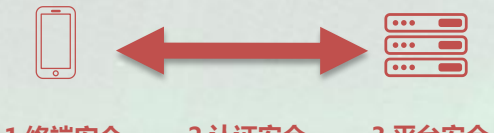
Gartner《Hype Cycle for Identity and Access Management Technologies 2017》

智能身份认证核心技术



多维度智能认证技术

1. 智能认证：20多个维度，2000多个特征，智能化判断
2. 动态可调：基于风险的认证，认证方法及规则随风险调整
3. 主动发现：UEBA，事前、事中、事后主动发现风险
4. 体验好：正常用户弱感知或无感知，恶意用户增强认证



端到端安全技术框架

1. 终端安全：动态静态安全保护，防御白盒环境下安全攻击
2. 认证安全：协议防破解、仿冒，一次一密、不易扩散
3. 平台安全：金库授权、安全硬件、自毁机箱，防内部隐患

传统身份认证，静态规则、被动发现、易扩散、体验差。

智能身份认证，领先算法技术，主动发现风险，动态调整策略，识别准确率高，毫秒级性能，体验好。

终端安全和SSE（Soft Secure Element）技术

终端安全和SSE技术特点

静态保护：

- 密钥转换与隐藏
- 差异化处理
- 数据分割

动态保护：

- 内存加扰及反跟踪
- 攻击识别
- 病毒、木马、恶意代码识别

运行环境安全

- ✓ 环境安全清场
- ✓ 模拟器识别
- ✓ 攻击框架识别

SSE技术

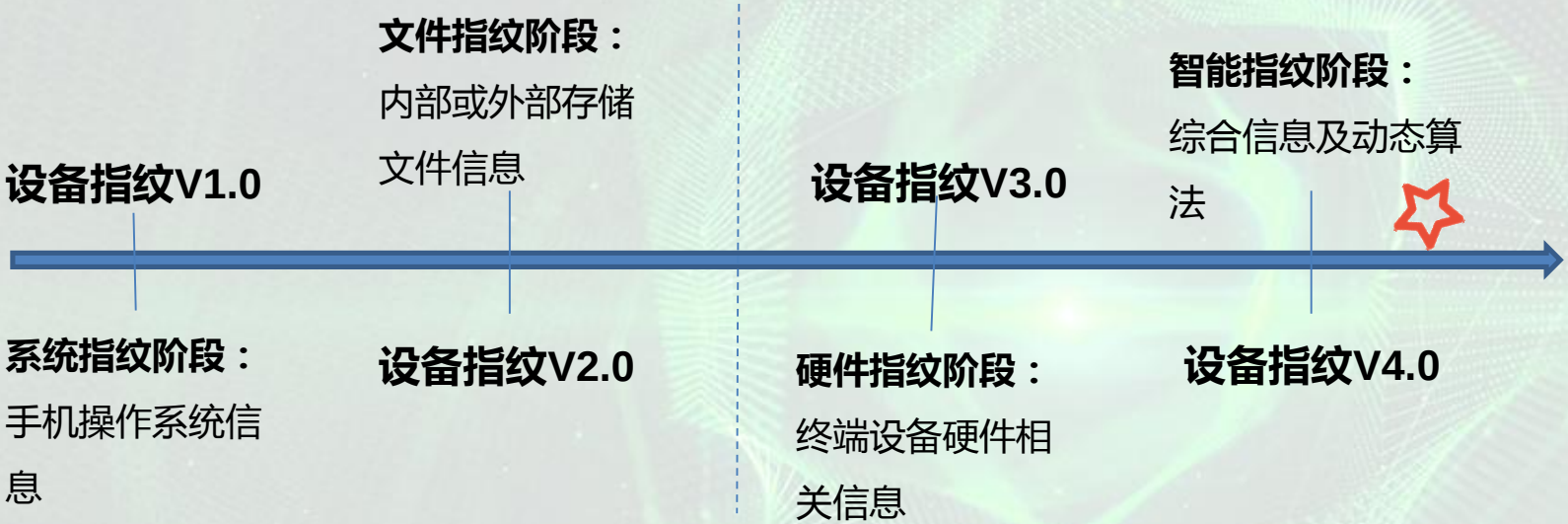
- ✓ 可信安全沙箱
- ✓ 内存保护
- ✓ 防复制

密钥安全

- ✓ 白盒算法
- ✓ 密钥协商
- ✓ 动态分割存储

动态设备指纹

设备指纹：采用第四代智能指纹技术，将数百个系统及硬件信息，通过智能指纹算法生成唯一可靠的设备指纹。指纹算法及相关阈值，根据机器学习技术进行动态更新和调整。



生物指纹认证

指纹认证技术

- 智能终端：指纹认证
- 车联网：指纹开锁
- 智能家居：指纹门禁

人脸识别技术

- 智能终端：刷脸登录
- 智能家居：刷脸开门

声纹识别技术

- 智能终端：声纹认证
- 智能家居：声纹开锁

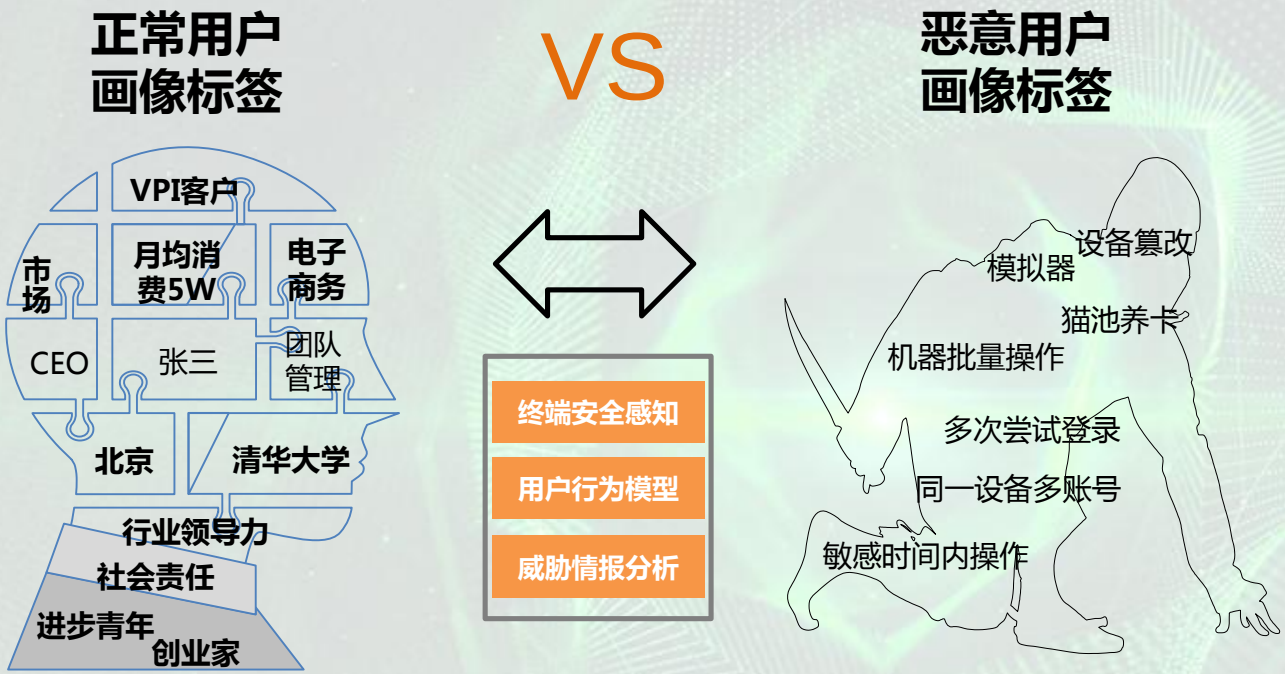
虹膜识别技术

- 机场、学校：虹膜门禁
- 二代身份证：预留空间

生物指纹认证：通过各种生物特征识别人的“主体”，确认当前操作的用户是本人。生物认证在智能终端已经普遍使用，尤其是指纹认证，已经可以作为移动支付认证方式之一。但物联网环境下，由于传感器、摄像头等采集设备欠缺，限制了生物技术的应用。

智能行为认证

智能行为认证：基于海量多源异构行为数据和和亿万量级精准欺诈数据，结合机器学习算法，形成了一整套由上千组规则因素、无监督学习引擎组成的智能实时身份反欺诈系统，毫秒级相应，千万级用户量支持，实现正常用户的无感知身份认证和欺诈用户精准识别。



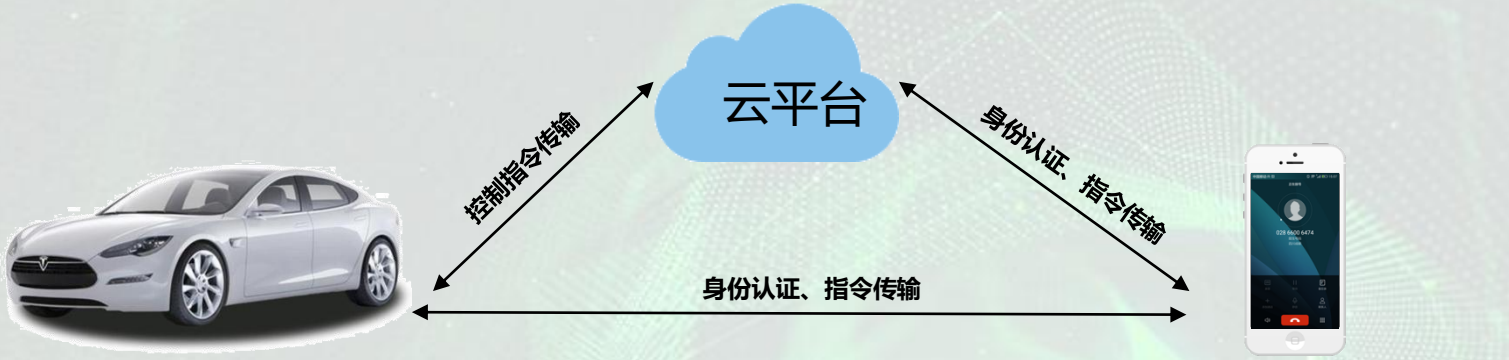
ISC 2017 中国互联网安全大会

360互联网安全中心

物联网与智能身份认证

物联网认证场景

管理平台
- ✓ 控制指令发送
- ✓ App管理
- ✓ 汽车管理
- ✓ 资讯管理



车载控制端
- ✓ 汽车控制
- ✓ 手机开锁
- ✓ 信息查询
- ✓ 信息推送

手机App
- ✓ 控制指令发送
- ✓ 汽车开锁
- ✓ 资讯查询

车联网场景下，云端管理平台及手机App，均可与车载控制器进行交互，发送控制指令。

控制汽车的过程中，需解决汽车、手机、云平台三者的认证以及数据传输安全。

汽车控制密钥管理

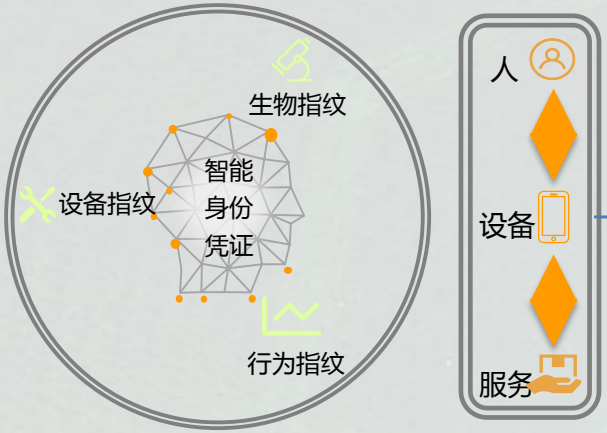
- **电话语音/生物认证**：验证用户真实身份，确保仅有合法用户可完成绑定。
- **设备指纹认证**：采集并标记设备，完成设备唯一性绑定。
- **终端安全SSE**：提供运行保护及安全存储，保障控制密钥安全性。

远程控制及近场开锁

智能行为认证+设备认证+生物认证：综合利用多维度联合智能认证，确保每次控制操作时的合法性校验

北京芯盾时代科技有限公司

芯盾时代智能身份认证



- 首推中国的移动身份认证，生成**唯一身份**
- 主动发现风险，动态调整策略，智能灵活认证
- 识别**准确率100%，漂移率低于0.001%**，毫秒级性能
- 应用场景广泛

身份认证与管理

一站式移动身份管理（IDaaS）

- 切入企业账号身份管理领域
- 解决多账号验证、权限管理的问题

移动多维联合认证（MFA）

- 识别用户身份
- 防止交易欺诈、身份欺诈

智能行为认证（IPA）

- 分析用户行为和操作意图
- 解决虚假注册、薅羊毛、盗刷盗转账

物联网

物联网身份管理（IoTAM）

- 切入个人用户身份管理领域
- 解决多终端、多设备与身份匹配管理

使用场景

银行　证券

电商　游戏

物流　政府　教育

多终端账户与身份管理

北京芯盾时代科技有限公司

芯盾时代
TRUSFORT.COM

知人善认，独具匠芯

国内领先的移动身份认证产品与解决方案提供商

谢　谢