# 物联网安全
# Internet of Things Security



## 第八章 物联网认证安全

冀晓宇
浙江大学

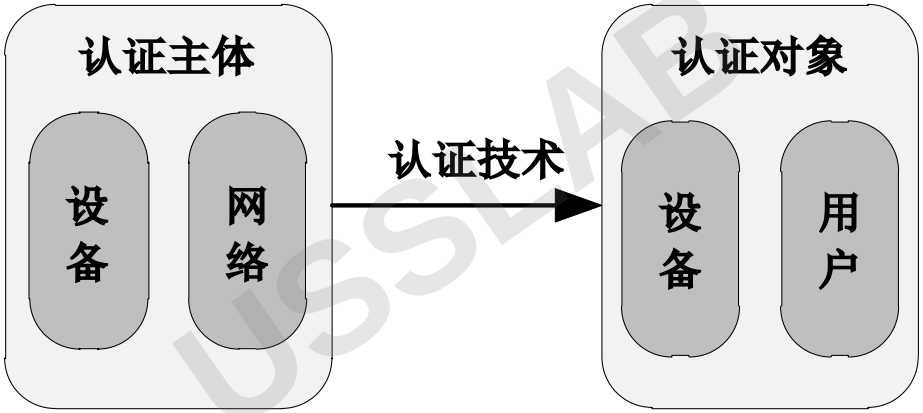
# 物联网认证安全

- **4.1 物联网认证安全概述**
- **4.2 物联网生物认证技术**
- **4.3 物联网设备指纹认证技术**
- **4.4 物联网设备配对技术**

# 4.1 物联网认证安全概述

# 身份认证 （Authentication）

- **定义：**由认证主体通过一定的认证技术，对认证对象身份进行确认的技术，目的是为了保证真实性



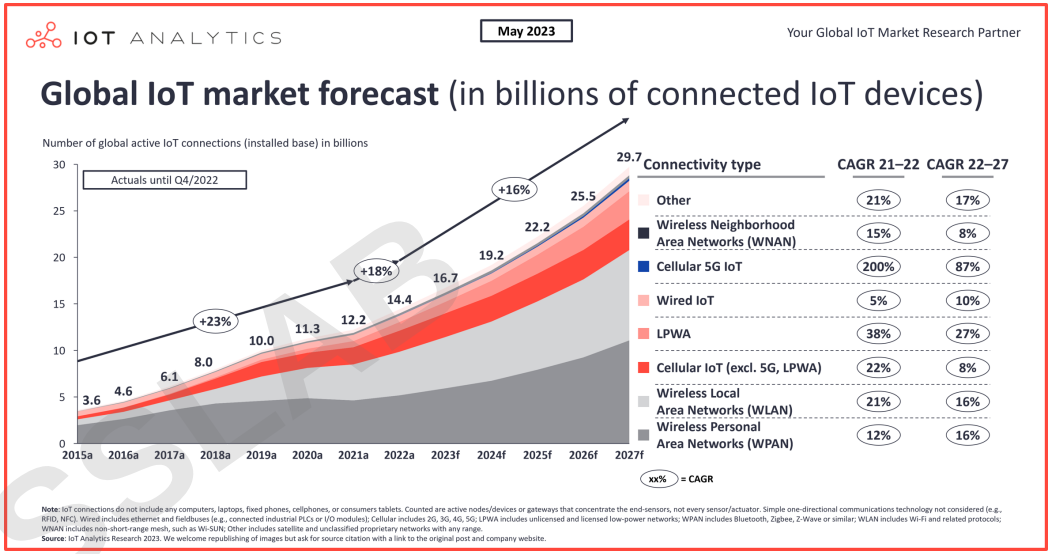

- **典型场景：**
  - 用户使用账号密码登入浙大邮箱
  - 智能设备使用密码接入Wi-Fi
  - 用户使用U盾进行网上转账
  - 用户指纹解锁手机
  - …

# 传统互联网认证

- 技术基础：基于密码学的方法，如数字签名等
- 示例：用户使用密码登录邮箱
- 特点：注重**对用户的认证**

# 物联网认证

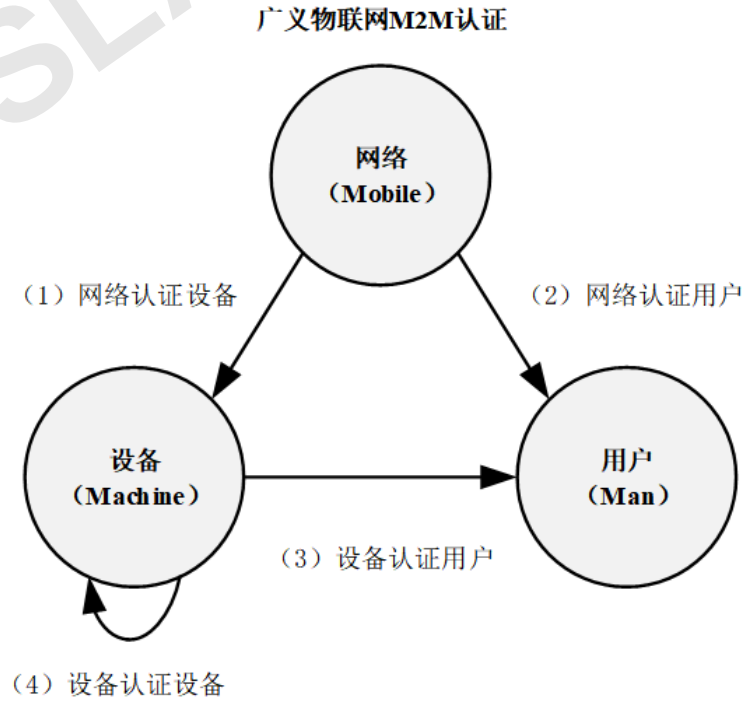
- **物联网特点**
  - 终端海量
  - 信息巨量
  - 多元异构
  - 资源受限
- **物联网认证**
  - 对象：从人到万物
  - 要求：跨平台、轻量级
  - 特点：**设备认证与用户认证并重**
- 示例：电力物联网设备请求接入电力系统内网




据IoT Analytics预测，2027年全球物联网设备数量将超过350亿

# 物联网认证框架

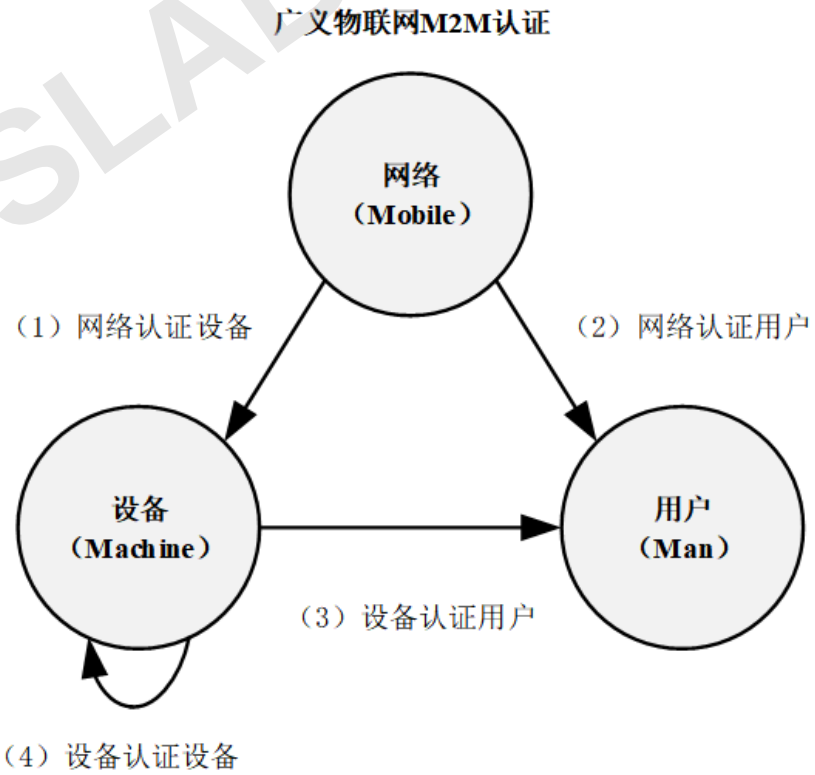
- **物联网认证的3M要素**
  - **网络(Mobile)**：4G, 5G, Wi-Fi等通信网络
  - **设备(Machine)**：各类终端设备，如手机、智能音箱、自动驾驶汽车等
  - **用户(Man)**：物联网用户



# 物联网认证框架

- **物联网认证主体：**网络（Mobile）、设备（Machine）
- **物联网认证对象：**设备（Machine）、用户（Man）



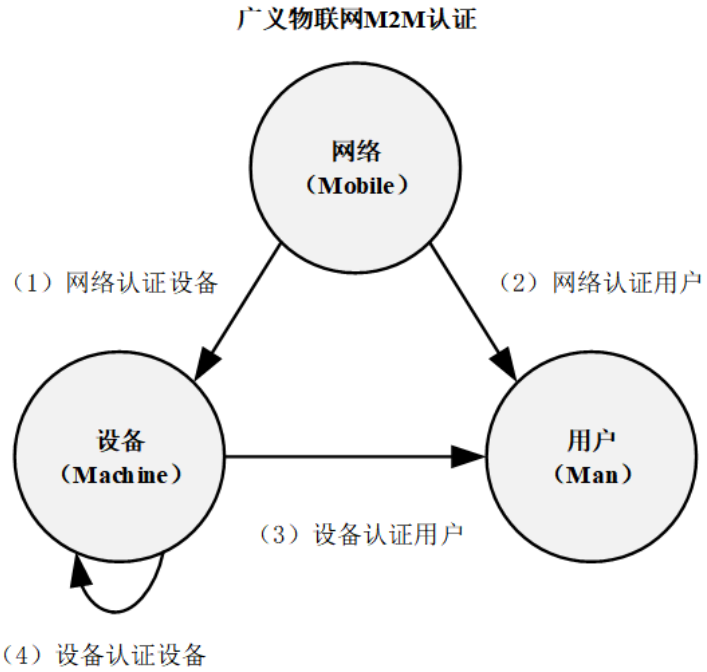



Q1：网络对用户认证和对设备认证有什么关系？

A1：网络对用户的认证可以是基于设备(device-based)的，即用设备表征用户；也可以是设备无关(device-free)的，比如对用户的生物特征如步态进行认证。

# 物联网认证框架

- **物联网认证形式：**
  - **网络认证设备**，例如服务器认证终端设备确认接入的设备合法
  - **网络认证用户**，例如服务器认证用户身份确保用户身份合法
  - **设备认证用户**，例如手机认证用户身份确保用户身份合法
  - **设备认证设备**，例如设备配对，设备相互确认身份以建立连接
- 物联网认证：**设备和用户并重**！

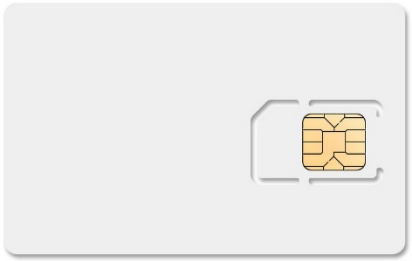


# 物联网认证技术

# 物联网认证——用户认证技术

- 基于**用户知道什么（what you know）**，通过认证主体和认证对象间共享信息完成认证的技术，如静态口令技术
- 基于**用户有什么（what you have）**，通过认证对象拥有的软硬件设备及其承载的信息完成认证的技术，如智能卡（IC卡）
- 基于**用户是谁（who you are）**，使用用户本身固有属性完成认证的技术，其典型代表主要为生物认证技术





示例：智能卡
用户知道什么

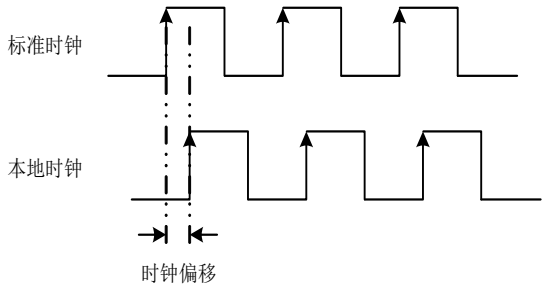

示例：金融行业电子令牌
用户有什么

示例：指纹扫描仪
用户是谁

# 物联网认证——设备认证技术

- **电子认证技术**：通过静态口令、数字证书等验证用户身份和保护数据安全的技术
- **设备指纹技术**：借助设备的软硬件等“指纹”作为设备身份标识，完成设备身份认证，如浏览器、传感器指纹
- **设备配对技术**：不存在先验知识的设备间利用共同知识来完成对彼此的安全关联，如蓝牙配对等


设备软件指纹技术
浏览器Cookies




设备硬件指纹技术
时钟晶振


设备配对技术
蓝牙耳机配对

# 物联网认证特点

- **认证对象：用户与设备并重**
  - 物联网认证主体和对象需要兼顾人和设备
- **认证算法：轻量级**：
  - **功耗**：平衡设备安全和设备能耗
  - **计算**：适配于配置简单、资源受限的终端
  - **功能**：用于控制设备接入、访问和密钥交换等
- **认证算法：跨平台**：
  - 适用于不同硬件结构、软件、操作系统、通信协议等不同平台
- **认证需求：多安全等级**：
  - 不同功能、不同等级的物联网终端设备需要的安全等级不同

# 物联网认证——新兴技术

- **生物认证**
  - 物联网设备交互方式受限，例如某些设备不具有输入、显示功能（键盘、屏幕），无法使用密钥认证
  - 依靠被认证主体的生物特征进行认证，如声纹、面纹等
- **设备指纹**
  - 物联网大量设备，如果使用加密方法认证，计算开销巨大
  - 依靠设备自身的软件和硬件指纹，具有轻量级特点
- **设备配对**
  - 物联网设备对设备的认证场景
  - 在资源受限条件下，两个物联网设备如何彼此信任对方

# 利用可穿戴设备的生物认证

- 可穿戴设备品类众多、在物联网市场中逐渐兴起
- 可穿戴设备交互方式受限，往往不具备输入功能，但相比于传统设备可搭载更多传感器，如加速度计、血氧仪、虹膜识别器件等，都可用作生物认证
- 问题：物联网可穿戴设备对信息的安全性的影响



VR眼镜

智能手表


可穿戴血糖仪

4.2

# 物联网生物认证技术

# 物联网生物认证技术

- **定义：**利用人体固有生物特征进行用户个人身份的认证技术，通常需要结合光学、声学、生物传感器和生物统计学等原理和手段，包括：
  - **生理特性：**如指纹、人脸等
  - **行为特征：**如笔迹、说话方式、步态等
- 基于“用户是什么（what you are）”：声音、指纹、面纹等生物识别技术
- 特点：通常用于设备对用户的认证，不需拥有或者记忆特定的身份信息

# 物联网生物认证技术

- 生物度量标准
  - 生物识别技术使用生物度量标准（biometrics）建立个体身份信息

- 生物度量标准应满足以下四个要素
  - 普遍性：即任何个体均具有该项特征
  - 独特性：即任何两个个体在该项特征上均具有区分性
  - 持久性：特征在一定时间内具有稳定性、不变性
  - 可采集性：特征可被定量采集

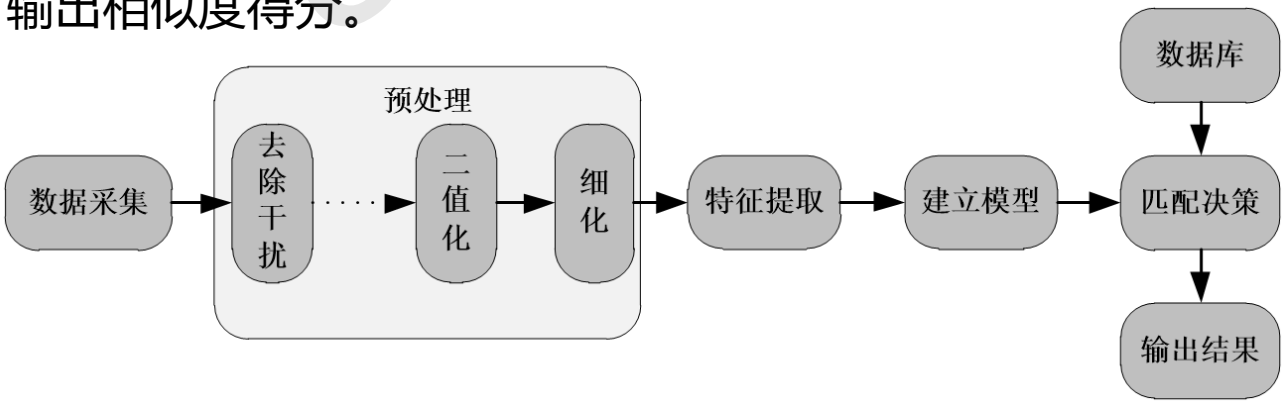
# 物联网生物认证技术

- 从实用性的角度出发，应同时考虑
  - 性能：如识别精度和速度，所需的资源等
  - 用户接受度：即用户对于在日常生活中使用该生物特征进行身份认证的接受程度
  - 安全性：即该系统是否易受攻击、易被欺骗

- 选取原则
  - 每种生物识别技术均拥有其优点和缺点，没有一种可以有效地满足所有应用的要求
  - 生物识别技术的选用通常取决于应用的实际需求

# 物联网生物认证——技术框架

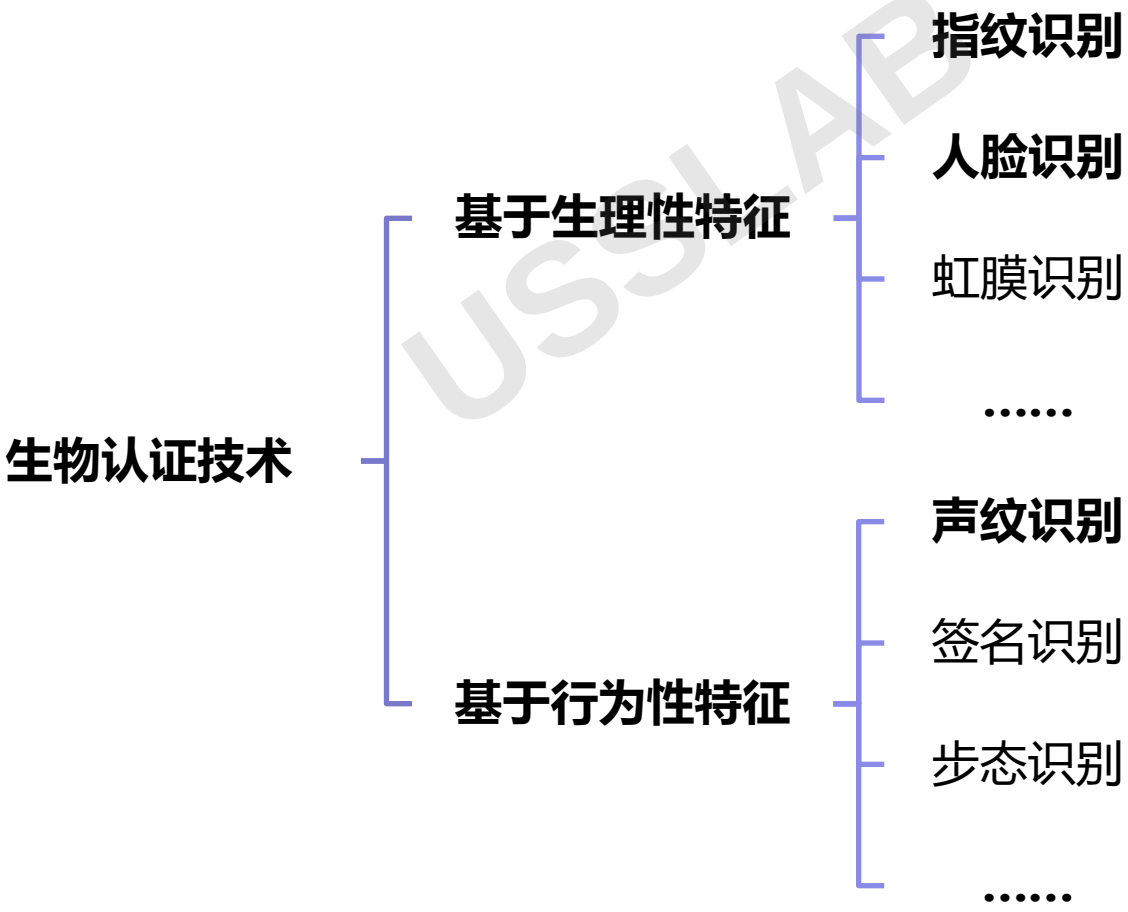
- 主要包括四个步骤：
  1. **数据采集**：使用合适的设备如摄像头、麦克风等采集数据的采集；
  2. **预处理**：对采集到的数据进行处理，如对图像或声音信号进行预处理。
  3. **特征提取**：对预处理后的数据提取可以满足生物度量标准的特征或特征集合，并建立模型。如使用轮廓、灰度、MFCC等信息。特征的选取需要兼顾可用性和安全性。
  4. **匹配决策**：将输入系统的目标数据与数据库内已确认身份的数据模型进行比对，输出相似度得分。




- 根据应用场景和用户需求的不同，具体实施方法可能存在差异。

# 物联网生物认证技术

- **生理性特征**：与用户身体生理构造等有关
- **行为性特征**：与用户行为习惯、动作方式等有关



# 物联网生物认证——生理特征

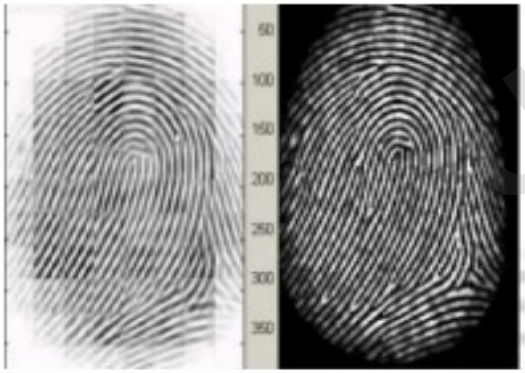
- **指纹：**一种典型的生理特征，是灵长类动物手指末端指腹上由凹凸的皮肤所形成的纹路，其形成在胎儿发育的前七个月期间确定。
- **指纹识别：**利用人类手指末端指腹纹路在物品上留下的印痕来进行识别，特征包括脊状特征、隆起线末端和隆起线分叉等。

具有不同形状的人类指纹

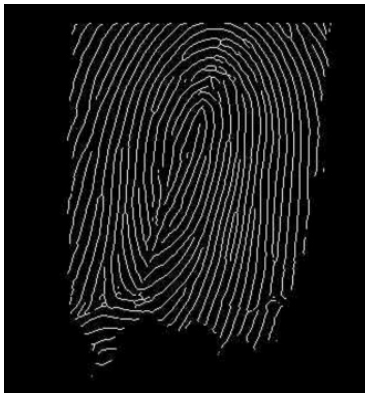
# 生理特征——指纹

- **指纹识别四个环节：**

1. **采集：**通过特定的指纹扫描仪采集活体指纹图像；
2. **处理**：指纹区域检测、图像增强、指纹图像二值化和细化等；



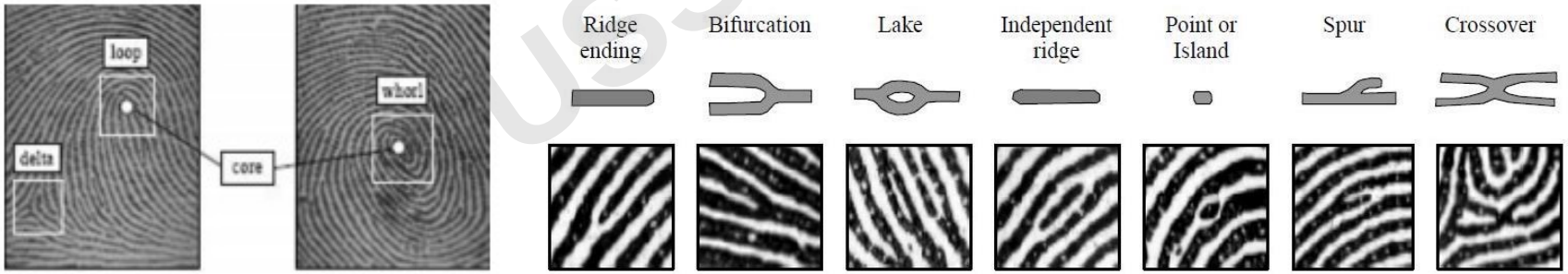
指纹图像增强



指纹图像细化

# 生理特征——指纹

- **指纹识别四个环节：**
  3. 特征提取（核心和关键）：
     - 基于细节：利用指纹图像的细节特征（例如隆起线的分叉点位置、端点位置等）进行认证



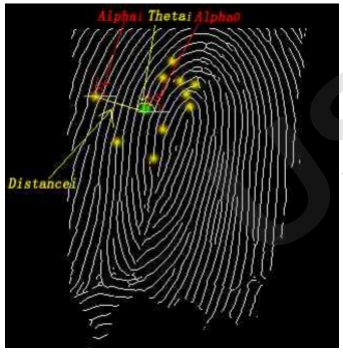

基于细节的方法

举例：分叉，循环、螺纹、山脊末端，山脊分叉等

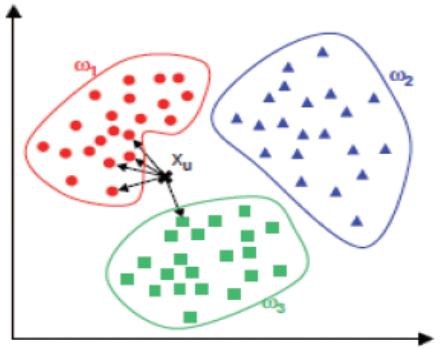
# 生理特征——指纹

- **指纹识别四个环节：**

3. 特征提取（核心和关键）：
   - 基于模式识别：包括贝叶斯算法、KNN算法等，首先创建已知数据的数据库，然后与待测数据进行匹配，最后输出结果




基于模式识别的方法
举例：特征点

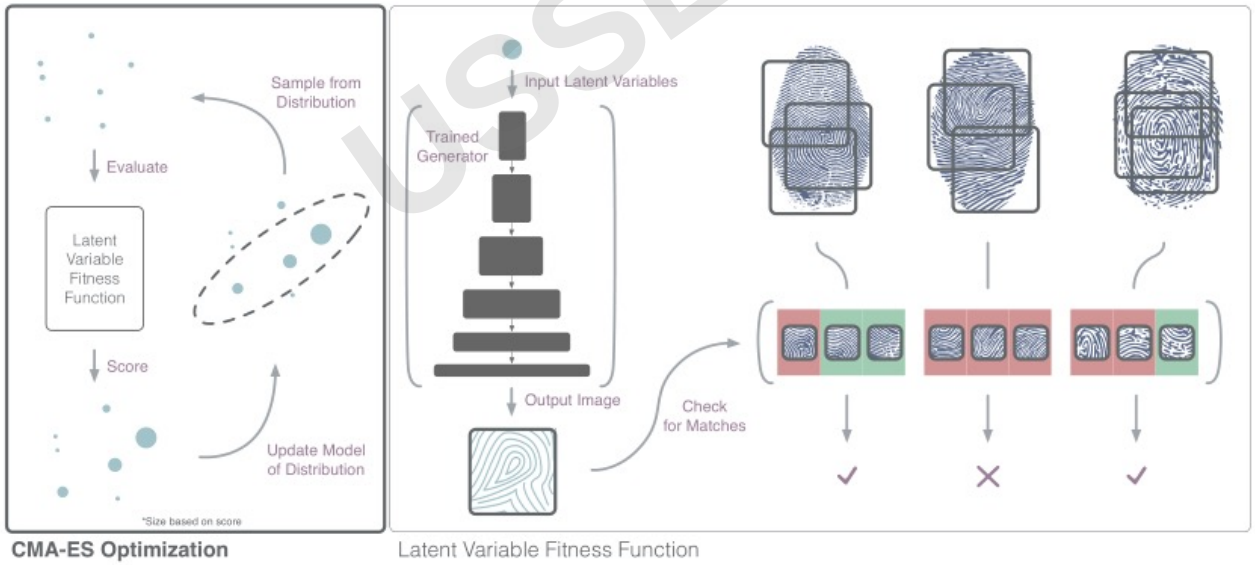



模型识别方法
举例：KNN识别

4. **指纹比对**：根据使用方法的不同，输出待确认目标和数据库内已确认身份用户数据的相似性得分。

# 针对指纹认证技术的攻击

- **仿冒攻击**：如3D打印机打印指纹、指模等欺骗指纹认证系统
- 新兴研究：基于GAN（对抗生成网络）的指纹攻击方法
  - 原理：指纹特征在大量用户样本条件下具有相似性
  - GAN：通过小样本真实指纹构建用于字典攻击的万能指纹





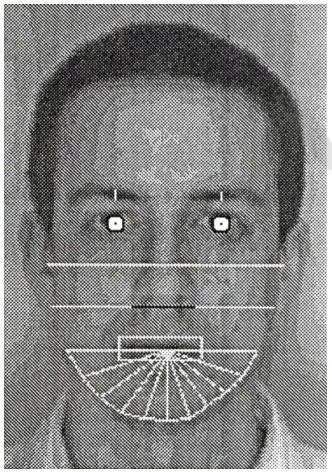

Ref: Philip Bontrager, etc., "DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution", in IEEE BATS, 2018

# 生理特征——人脸

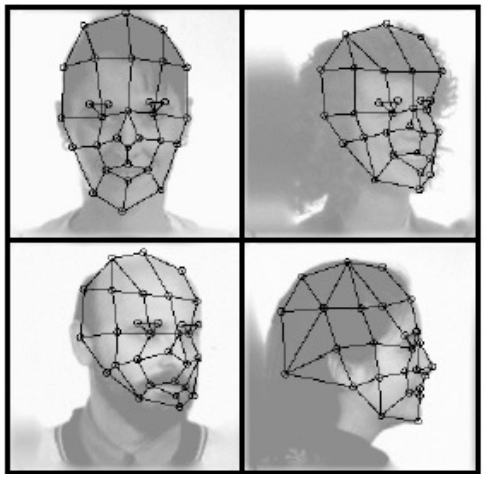
- 人脸识别：又称面部识别，是一种利用人类面部生理特征来进行用户识别的方法，主要特征包括眼睛、眉毛、鼻子等面部属性的位置和形状。

# 生理特征——人脸

- 人脸识别四个环节：
  1. **图像采集**：使用摄像头作为采集设备，获得单张图像或者视频；
  2. **检测定位**：为消除观察角度、遮挡和表情变化影响，需对人脸检测定位，方法包括几何特征、全脸模板、基于多视图样本训练等；



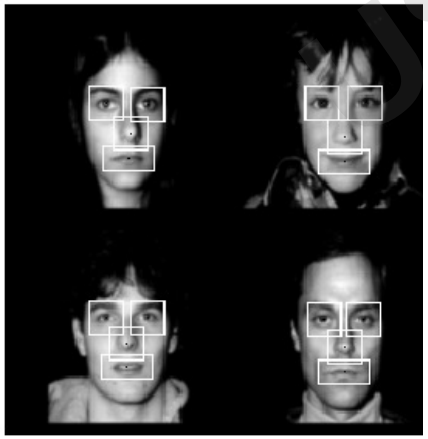
人像检测定位
举例：几何特征



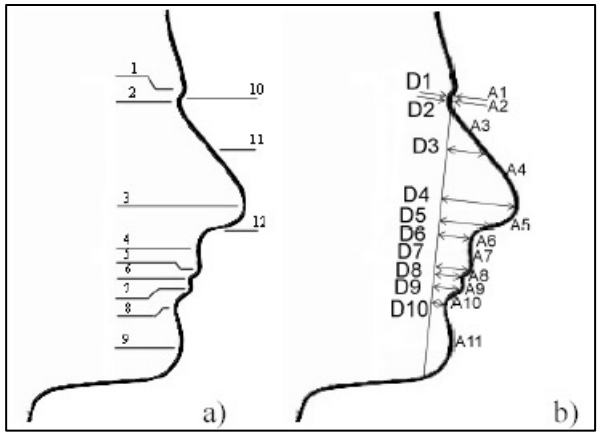
人像检测定位
举例：基于多视图样本训练

# 生理特征——人脸

- 人脸识别四个环节：
  3. **特征提取和选择（核心和关键）**：包括基于边缘直线或曲线的通用方法、基于特征模板的识别方法和结构匹配方法等；
  4. **匹配比对：**将待确认目标的数据与数据库内已确认身份的数据进行对比，相似度高则证明为同一对象。



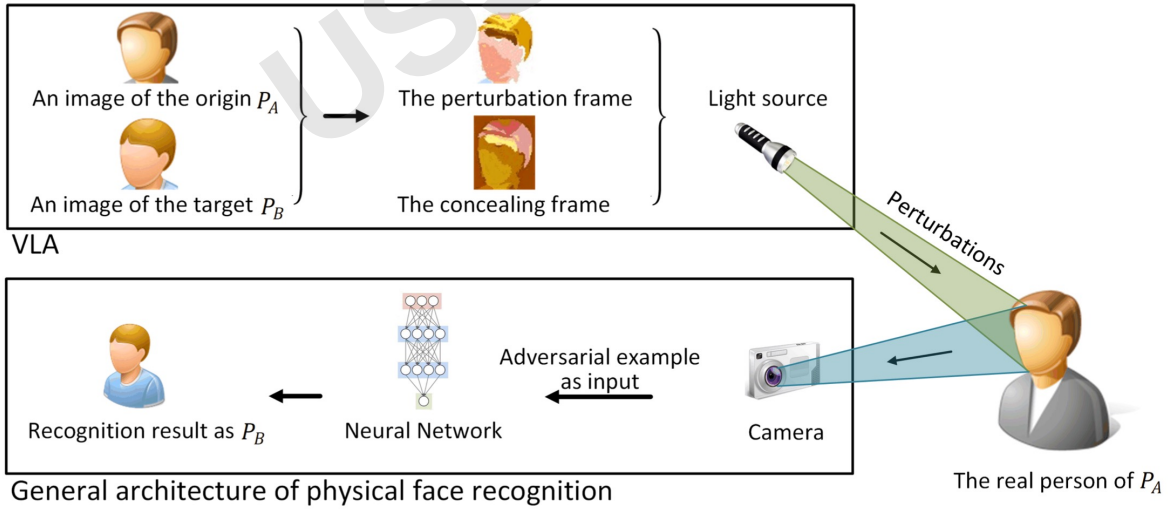
特征提取
举例：特征模板（眼睛、鼻子、嘴巴）




特征提取
举例：边缘直线或曲线（面部基准点）

# 针对人脸认证技术的攻击

- **安全性**：人脸识别受到光照、姿态、遮挡、年龄、图像质量等影响。除了传统攻击方式外，还可以利用机器学习进行深度伪造和人像欺骗。
- 案例：VLA——基于可见光投影的人脸识别攻击，利用灯光投影，实现对目标人物的人脸认证欺骗。

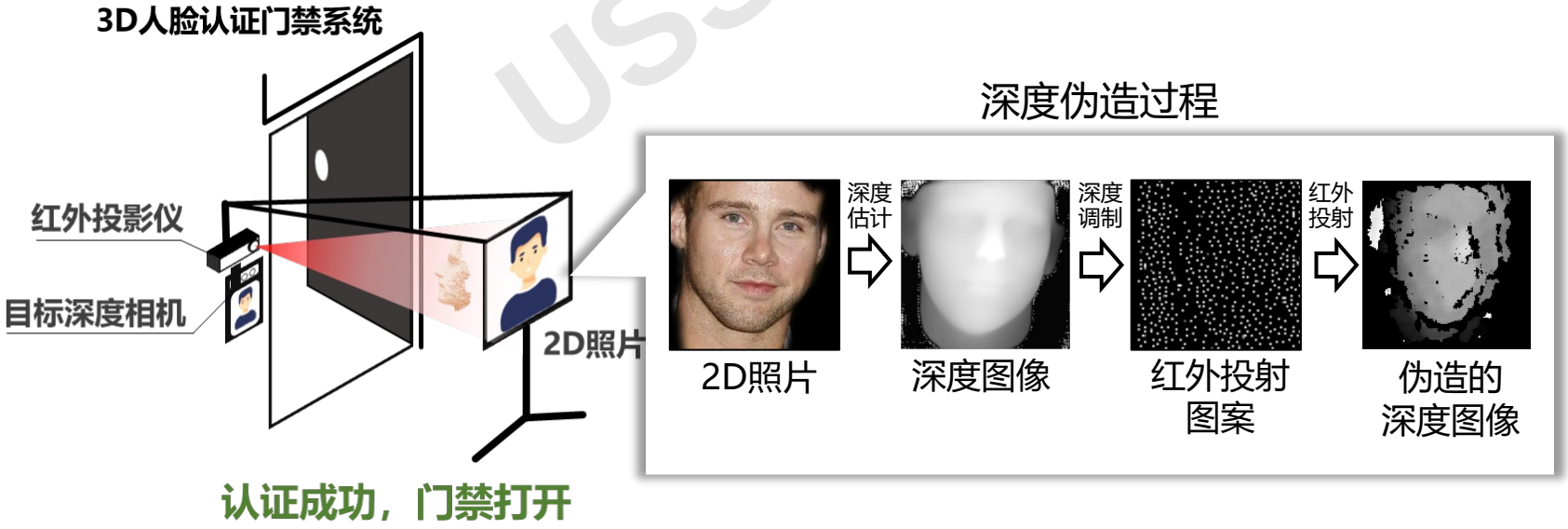





Ref: Shen, Meng & Liao, Zelin & Zhu, Liehuang & Xu, Ke & Du, Xiaojiang. (2019). VLA: A Practical Visible Light-based Attack on Face Recognition Systems in Physical World. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 3. 1-19. 10.1145/3351261.

# 针对3D人脸认证攻击——DepthFake

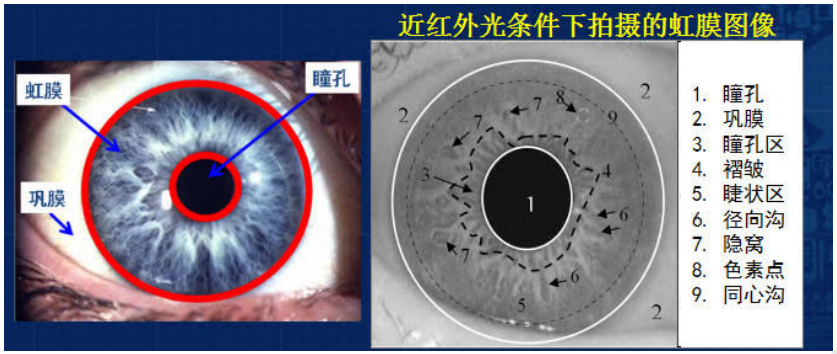
- **基本思想：**基于结构光相机的深度测量原理，向目标相机投射调制有深度信息的红外光图案，使其捕获到虚假的3D人脸，进而欺骗3D人脸认证系统。
- **攻击效果：**可使用单张2D照片欺骗3D人脸认证系统，并成功欺骗腾讯、百度、3DiVi等国内外人脸认证系统。



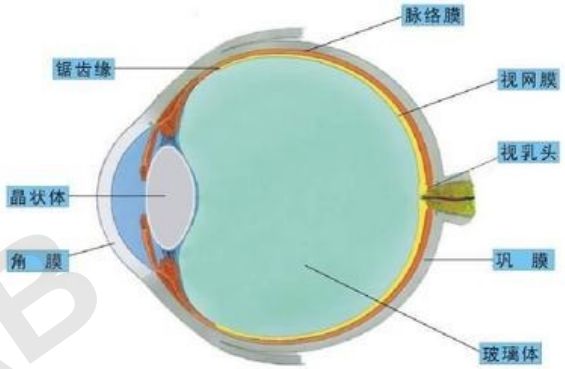



Ref: Zhihao Wu, Yushi Cheng, Jiahui Yang, Xiaoyu Ji, Wenyuan Xu, et al. DepthFake: Spoofing 3D Face Authentication with a 2D Photo[C]//2023 IEEE Symposium on Security and Privacy (SP), 2022.

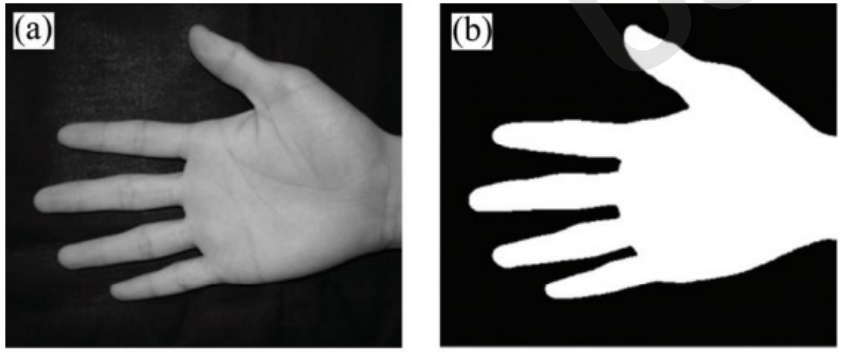
# 生理特征——其他




虹膜识别技术



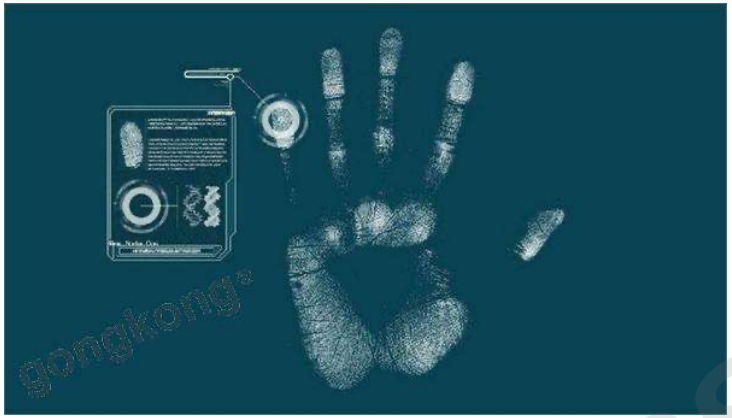

视网膜识别技术



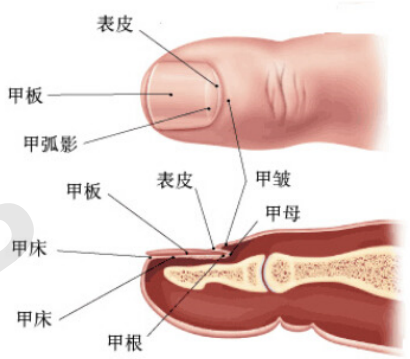

手型识别技术

静脉识别技术

# 生理特征——其他



掌纹识别技术




甲床识别技术

DNA识别技术

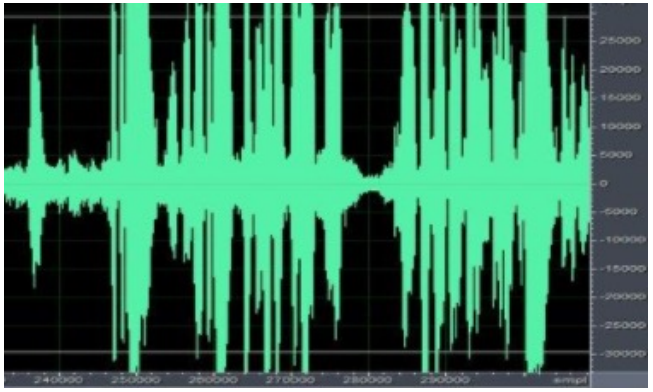
耳廓识别技术

# 物联网生物认证——行为特征

- 声纹：由于每个人发声使用的**发声器官**（声带、嘴、鼻腔和嘴唇）的形状和大小的差异，以及地域和说话方式的影响，个体的声音特征不相同。
- **声纹识别：**基于个体发声器官的差异性，利用声音的差异来进行身份识别。



Q: 声纹是一种典型的行为特征，为什么不是生理特征?



声音波形图

# 行为特征——声纹

- **声纹识别四个环节：**
  1. **声纹采集：**使用音频采集设备（麦克风）将声波转换为电信号；
  2. **预处理：**采集获得为模拟信号，需要转换为数字信号；
  3. **特征提取：**音频特征主要有时域特征（短时平均幅值、短时过零率等）、频域特征（傅里叶变换）、梅尔倒谱系数等；
  4. **匹配决策：**在决策时，输入相应的待确认目标声纹模型以及已确认声纹模型，输出匹配分数。

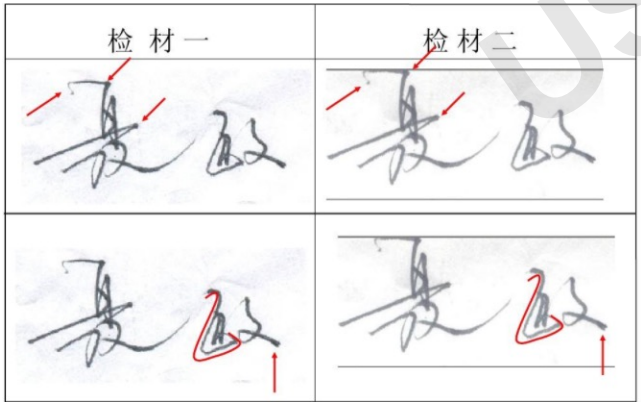
# 行为特征——声纹

- **优势：**
  - 蕴含声纹特征的语音获取方便、自然，具有较高用户友好度
  - 获取语音的识别成本低廉、方法简单
  - 适合远程身份确认，提取声纹后就可以通过网络实现远程登录
  - 声纹辨认和确认的算法复杂度低
  - 和语音识别等方案结合，可以提高准确率
- **缺点：**
  - 但是由于生理（例如年龄）、病理（例如感冒）、心理（例如情绪状态）、环境（例如不同的麦克风和信道）等，每个人的语音声学特征具有**变异性**，不是绝对一成不变的。

# 行为特征——签名

## 基于静态签名

- 原理：对其特征点进行分析匹配以确认真实性。
- 缺点：易于伪造。



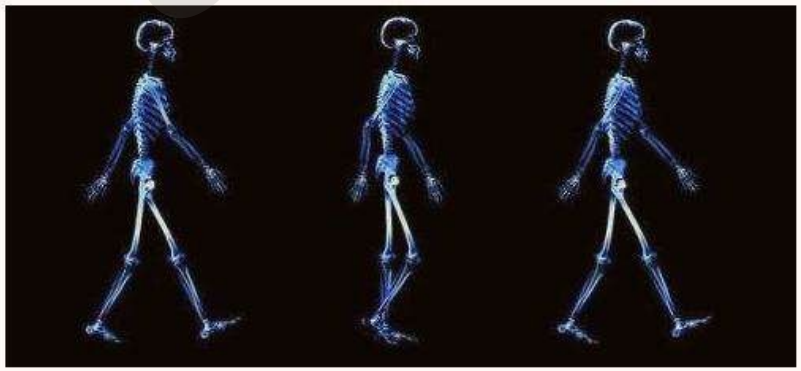

示例：静态签名检测

## 基于动态签名

- 原理：通过检测用户书写时的力度、笔画顺序等特征
- 优点：攻击者无法通过简单地查看先前写过的信息来收集有关如何编写签名的信息。
- 缺点：用户友好型较差。

# 行为特征——步态

- **定义**：
  - 通过人类的行走步态差异进行身份识别的方法。
- **原理**：
  - 人类的走路姿势由身体的肌肉力量、肌腱、骨骼等决定，人为很难长期刻意改变自己的走路姿势。

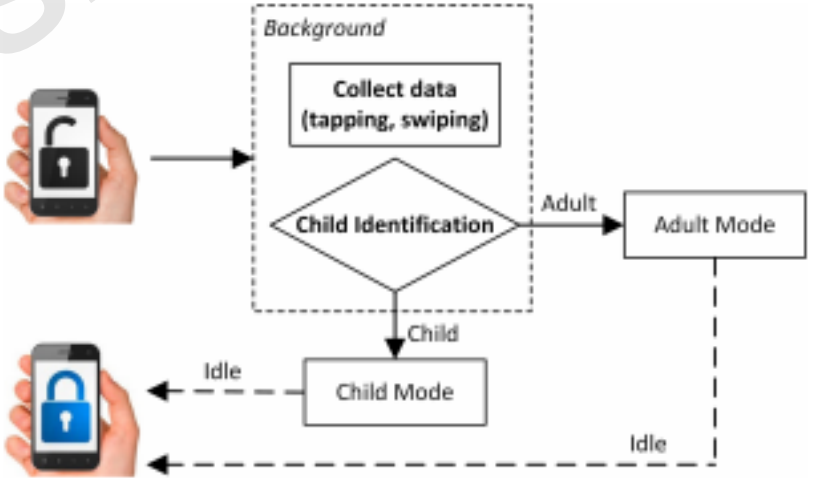


示例：人行走时的步态

# 新兴方法——iCare

- **群体行为特征识别**：如用户年龄分布、疾病预测诊断等。
- **技术原理**：儿童和成人用户操作手机的方式不同。如按压、滑动等动作特征不同，通过屏幕传感器、加速度、陀螺仪的数据反映出来。
- 应用场景：智能设备权限控制、身份识别、疾病预测等。

Q：群体行为特征识别更难还是更简单？



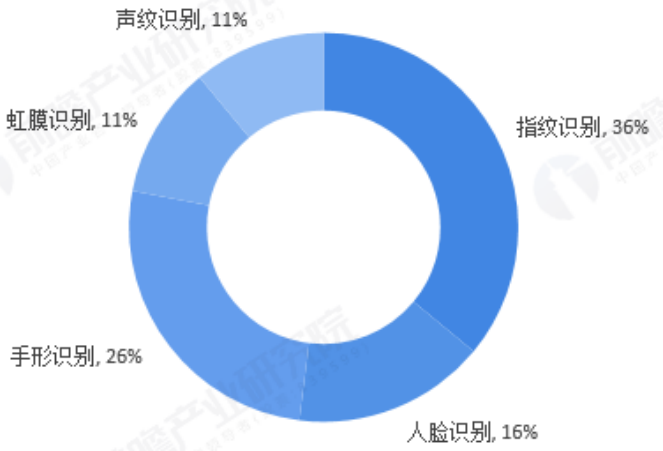



Ref: Xiaopeng Li, Sharaf Malebary, Xianshan Qu, Xiaoyu Ji, Yushi Cheng, and Wenyuan Xu. 2018. iCare: Automatic and User-friendly Child Identification on Smartphones. ACM HotMobile '18

# 生物认证应用及发展趋势

- 指纹识别技术最成熟且成本较低，应用范围广泛，普及率较高；手形识别作为与指纹识别关联性较大的技术，市场占比为其次；而技术难度更大的人脸识别、声纹识别、虹膜识别分别占比随后。
- 我国生物识别产业还有一个高速增长期。预计到2023年，中国生物识别行业的市场规模将达到379亿元。

北京地铁大兴机场线“刷掌”乘车




各类生物认证方法市场识别

# 生物认证发展面临问题

- **标准化和统一认证**
  - 目前系统的各方大多独立使用自己的算法、传感器和认证模式
- **数据存储安全**
  - 随着生物特征技术的应用，生物特征欺诈带来安全隐患
- **消费者隐私**
  - 个人生物特征数据具有唯一性和不可修改性，如果泄露会导致严峻的后果
- **通用性**
  - 对于某些特殊人士（例如残障人士）而言，有部分生物识别特征可能难以获取，这阻碍了这类人群获得服务。

# Discussion

- **生物认证需要用到各类传感器获取并提取生物特征，会导致哪些安全问题?**
- **Sensor oversensing, feature overfeeding, model overlearning and privacy leakage**

# 4.3 物联网设备指纹认证技术

# 物联网设备指纹认证技术

- **设备指纹定义**
  - 一种**唯一标识出该设备特征的设备标识**，如软件版本号、硬件信号特征等指纹信息

- **设备指纹构成**
  - 通常由**单种**或**多种**设备特征信息构成，其包含的特征信息越多，安全性越高

- **设备指纹认证技术**
  - 使用设备指纹作为物联网设备标识，对设备进行识别和认证的技术，可以用来做设备接入认证或者设备配对

# 物联网设备认证技术

- **设备指纹认证技术**
  - **软件指纹**
    - 浏览器信息
    - 设备网络行为
    - 设备软件环境
    - ……
  - **硬件指纹**
    - **外设单元**
    - **通讯单元**
    - **计算单元**
    - ……

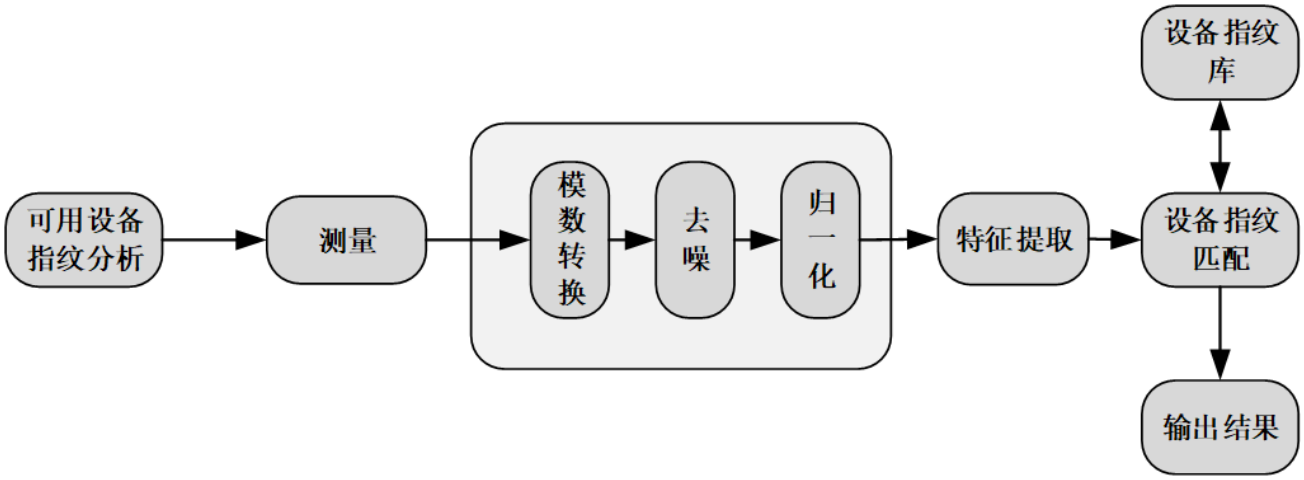
- **基于软件指纹的设备认证技术**：软件指纹来自于设备ID、MAC地址等


示例：路由器标签上的MAC地址

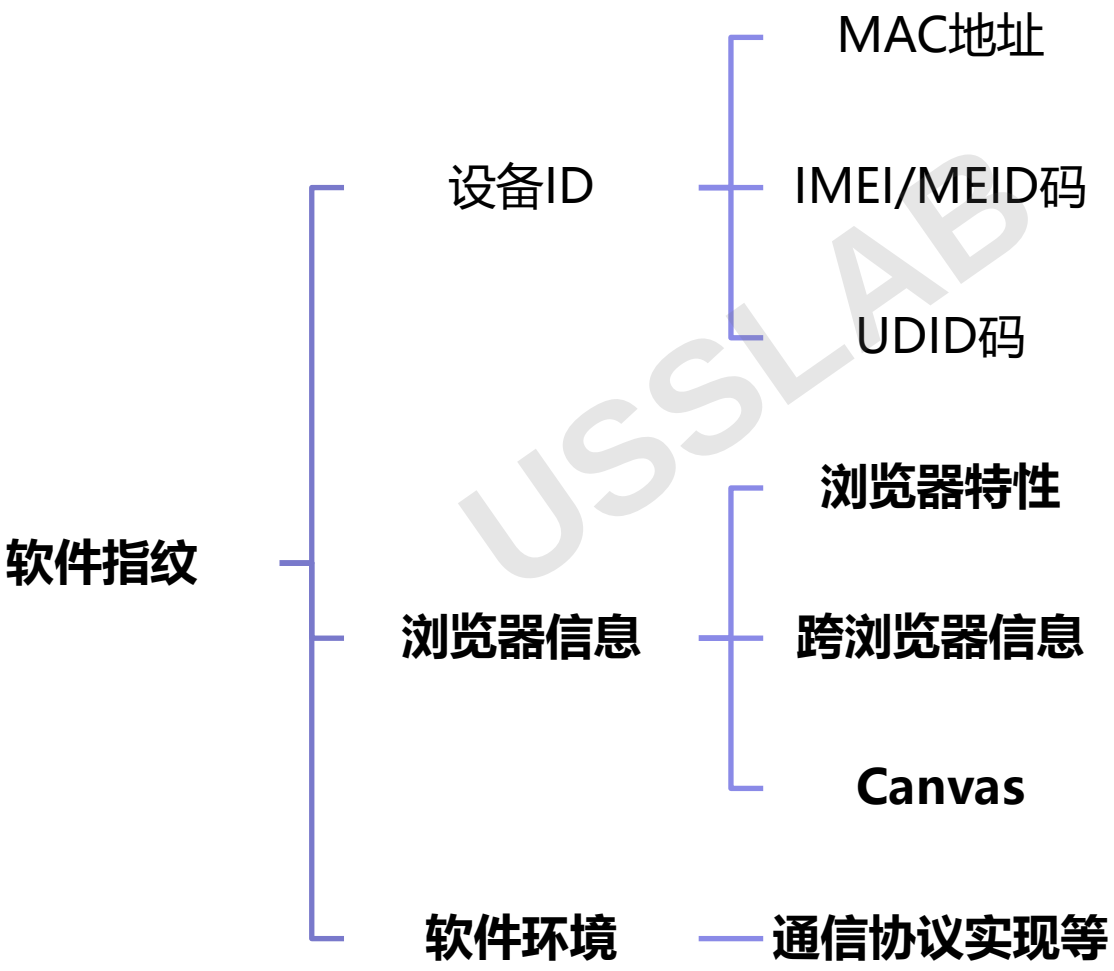
- **基于硬件指纹的设备认证技术：**硬件在制造过程中存在细微差异，可形成硬件指纹，例如传感器非线性、射频信号特征、晶振偏移等。

# 设备指纹提取方法

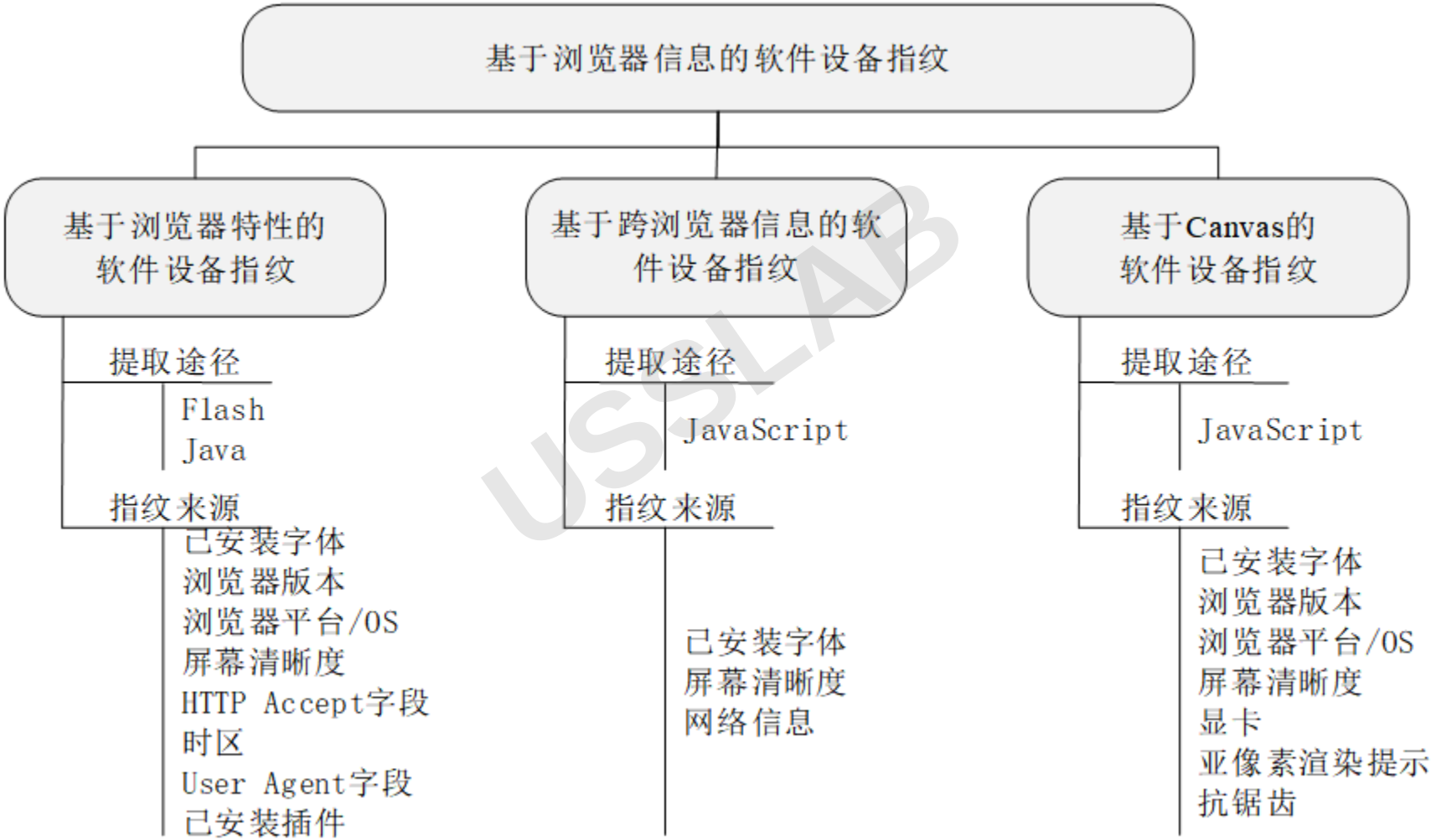
- 设备指纹提取主要包括四个步骤：
  1. **分析来源**：根据应用场景和终端设备特点，分析当前设备可用的设备指纹来源，如软件信息、硬件模块等，选择适用于当前认证环境的设备指纹；
  2. **收集信号**：根据选定的设备指纹来源，通过设备的 API接口或外置测量设备收集可用的设备指纹数字或者物理信号；
  3. **信号处理**：对收集到的设备指纹数字或物理信号进行信号处理，通常包括模数转换、去噪、归一化等；
  4. **提取特征**：从预处理后的可观测信号中提取可以标识设备身份的特征。



# 物联网设备认证技术——软件指纹



# 软件指纹——浏览器信息



# 软件指纹——软件环境

- **原理**
  - 互联网通讯协议标准中存在一些可自由选择和配置的参数及选项，不同的操作系统在实现过程中存在**细微差别**，从而构造基于软件环境的设备指纹。
- **方法**：
  - 被动探测设备操作系统，分析侦测到的数据包，提取相关特征如WS、TTL、DF、ToS、TL等，从而判断目标设备的操作系统。
  - 随着终端设备操作系统种类及版本数量的增加，不同版本之间差异缩小，该方法的准确度易受影响。

- WS(Window Size) : **TCP 数据包头中的窗口值**。Windows 会话会改变该值，在 Unix系统中则保持不变。
- TTL( Time To Live) : 数据包在网络传输过程中的生存时间。若 TTL 值为128，则一般为Window 操作系统。
- DF( Don`t Fragment) : 不分片标记位，大多数操作系统设置该项为缺省值。
- ToS(Type of Service) :服务类型。
- TL(Total Length) : 总长度，是指包括 IP 包头的数据包长度。

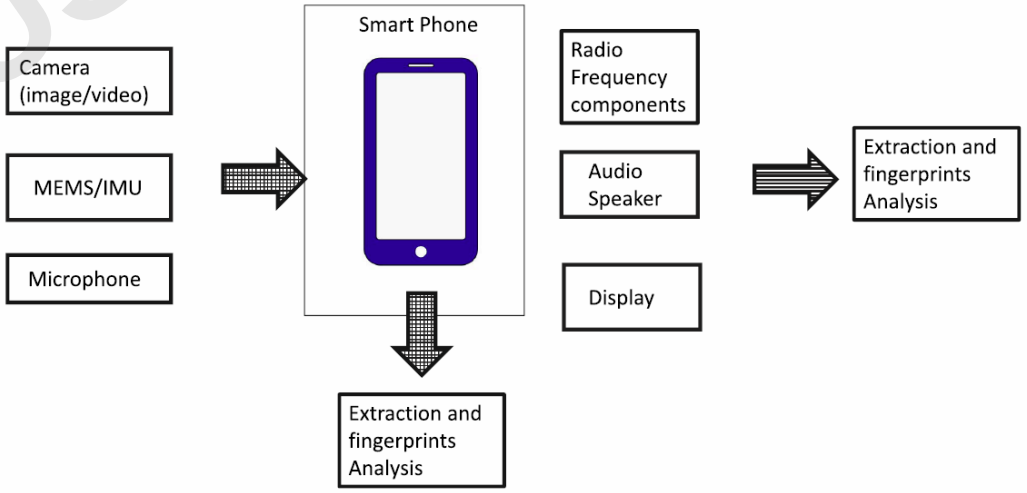
# 软件设备指纹对比

| 软件设备指纹类别 | 具体来源 | 适用对象 | 标识特征（指纹） | 提取方法 | 特点 |
|---|---|---|---|---|---|
| 浏览器信息 | 浏览器特性 | 具有浏览器且启用Java或Flash插件的终端设备 | 浏览器版本，已安装字体，浏览器平台/OS等 | 浏览器插件Java或Flash | 依赖浏览器插件获取，无法区分具有相同软硬件设置的终端设备 |
| | 跨浏览器信息 | 具有浏览器的终端设备 | | JavaScript引擎 | 不依赖浏览器插件获取，无法区分具有相同软硬件设置的终端设备 |
| | Canvas | 具有显示功能的终端设备 | 操作系统，浏览器版本，显卡，已安装字体等 | HTML5 <canvas> 元素 | 最常见的设备指纹识别技术之一，无法区分具有相同软硬件设置的终端设备 |
| 软件环境 | 软件环境 | 具有通信功能的终端设备 | 数据包特征值或Banner（旗帜信息）等 | 被动嗅探 | 易被终端设备的安全策略屏蔽，精度受限于终端设备操作系统种类及版本数量的增加 |

# 物联网设备认证技术——硬件指纹

- **硬件指纹原理：**终端设备的硬件模块在制造过程中，由于生产制造工艺限制，导致即便是同一型号的硬件模块也存在细微差异。这些差异可以体现在硬件模块的输出或者其他相关信号，从而作为硬件设备指纹的来源。
- 由于硬件指纹是硬件的本征差异，相比于软件设备指纹，硬件指纹不易被篡改，不易随时间或用户操作改变。

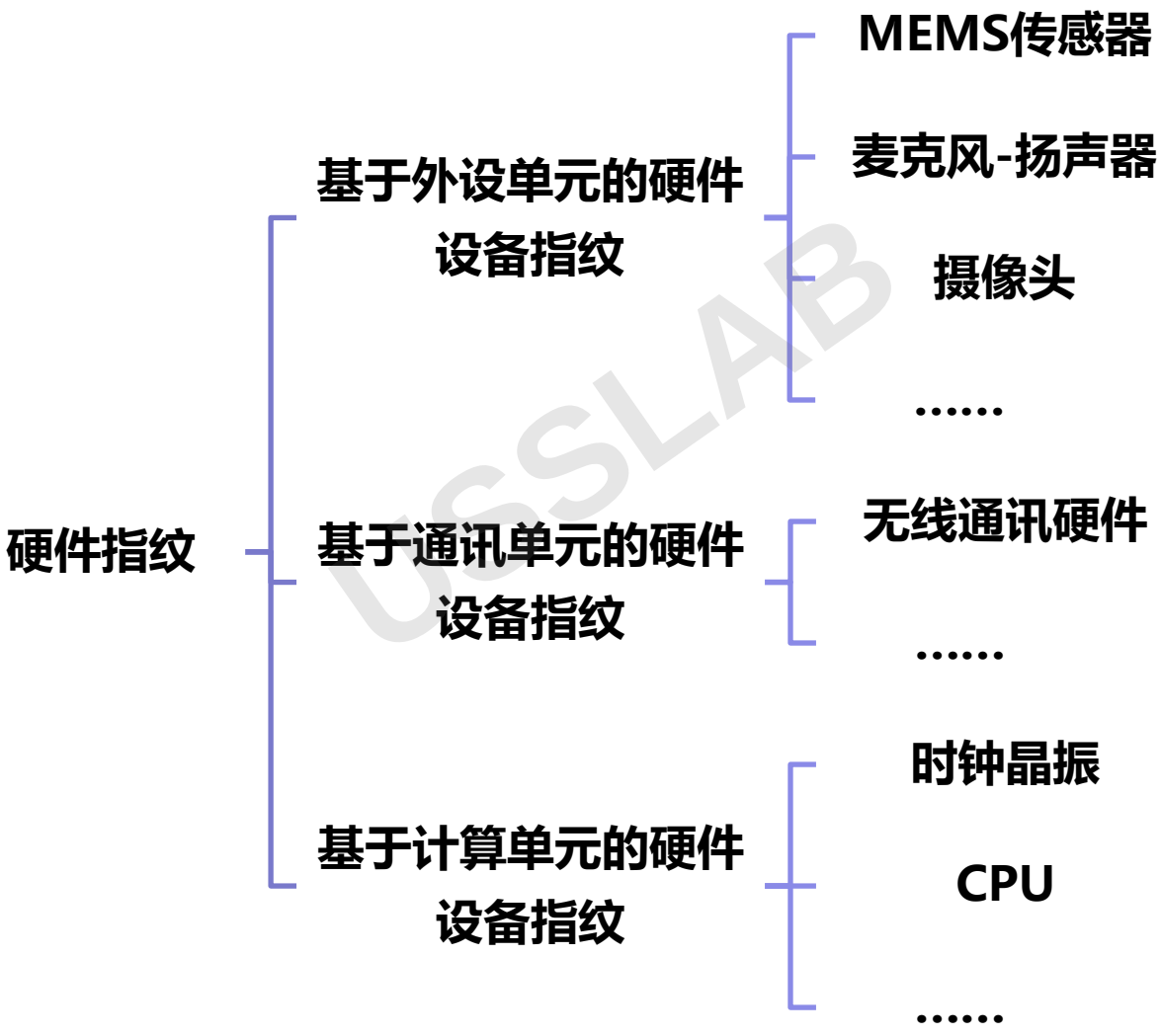
示例：智能手机硬件设备中各个模块都存在的硬件指纹





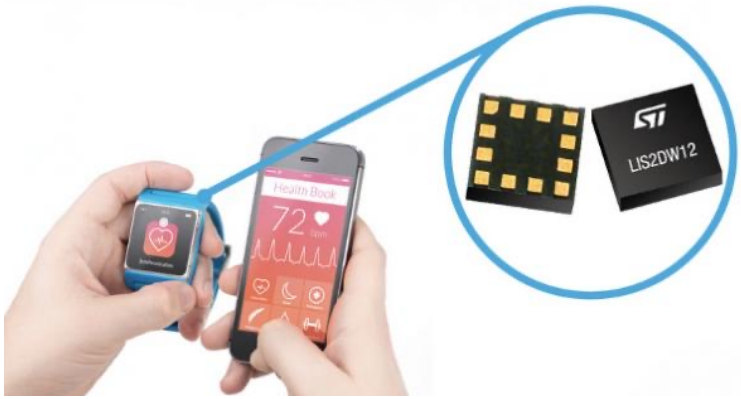

Baldini G, Steri G. A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components[J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1761-1789.

# 物联网设备认证技术——硬件指纹



# 硬件设备指纹——外设单元

- **MEMS传感器**：微型电子机械系统（Microelectro Mechanical Systems，MEMS），是集微传感器、微执行器、微机械机构、信号处理和控制电路、高性能电子集成器件、接口、通信和电源等于一体的微型器件或系统，利用的是传统的半导体工艺和材料，具有小体积、低成本、集成化等特点，广泛应用于各类智能设备，尤其是体积受限的设备。
- 举例：加速度计，麦克风、陀螺仪、磁力计等。

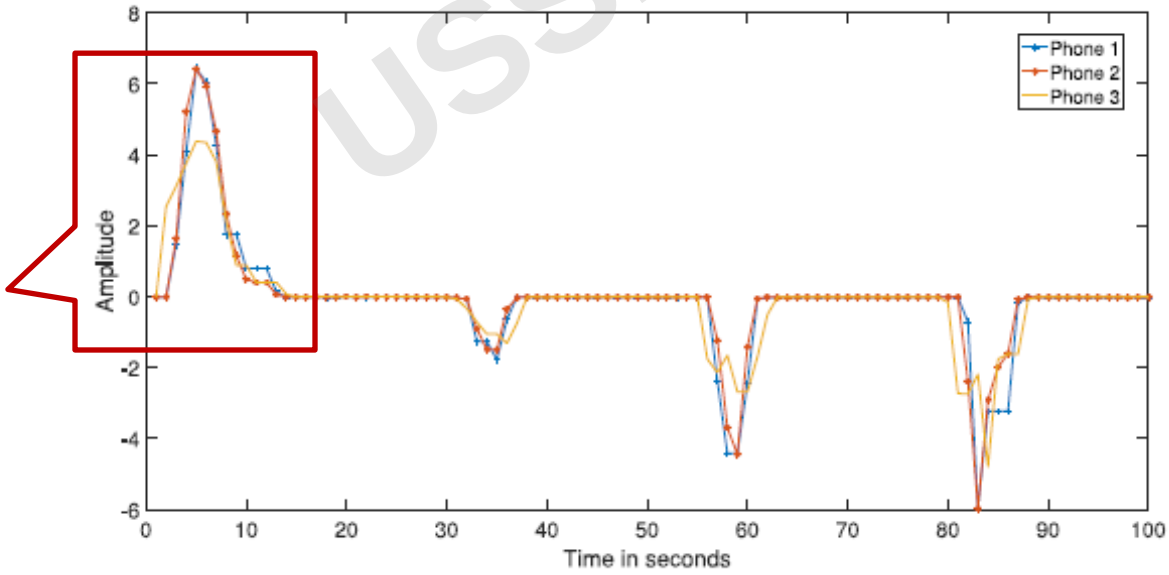



智能手环中的MEMS加速度计

# 基于外设单元的硬件设备指纹

- **MEMS传感器硬件指纹来源**
  - 由于MEMS传感器在制造过程中受到工艺精度的限制，即便是同一型号的不同传感器个体，其硬件电路也存在细微差异。
  - 传感器在相同激励输入下，输出结果存在差异。

3 个 MEMS 传感器对同一个加速度的测量差异




同一型号不同设备的陀螺仪对特定刺激的响应

# 基于外设单元的硬件设备指纹

- **MEMS传感器硬件指纹**

  - MEMS传感器硬件指纹可以是单个MEMS传感器或者包括多个MEMS传感器组合进行构造

  - 优点：MEMS传感器应用范围十分广泛，且调用MEMS传感器无需特殊权限，可在用户无感知的情况下实现设备认证

  - MEMS传感器如加速度传感器等都是低敏感权限传感器

# 基于外设单元的硬件设备指纹

- **案例1：麦克风 - 扬声器 硬件指纹**
  - 智能设备通常集成麦克风和扬声器MEMS传感器，主要特性为其对应的频率响应
- **方法：**
  - 分析麦克风-扬声器音频电路对标准刺激（例如标准音调）的响应
  - 提取特定音频特征，如梅尔频率倒频谱MFCC
  - 构造基于麦克风-扬声器硬件指纹，用于智能设备认证。

Q：如果利用超声波调制信号作为输入，是否也可以？





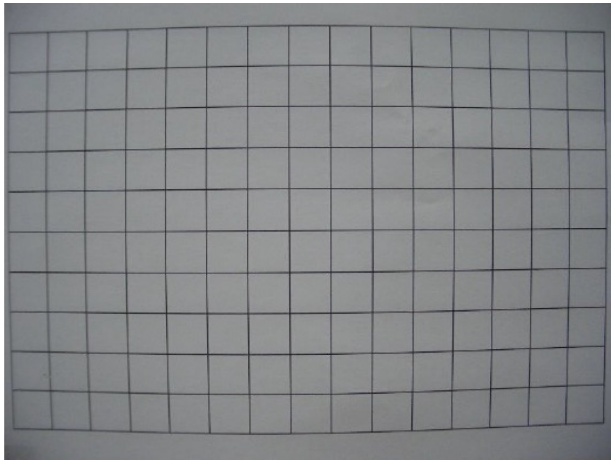


Xinyan Zhou, Xiaoyu Ji, etc, “NAuth: Secure Face-to-Face Device Authentication via Nonlinearity”, IEEE INFOCOM 2019

# 基于外设单元的硬件设备指纹

- **案例2：摄像头传感器硬件指纹**
  - 表现：互补金属氧化物半导体（CMOS）传感器和后续图像处理会引起**图像伪像**，例如图像畸变
  - 指纹来源：
    1. 镜头（Lens）
    2. 色彩过滤阵列（Color Filter Array）
    3. 传感器（Sensor）
    4. 压缩算法（Compression Algorithm）
    5. 综合差异
  - 应用：设备认证和图像溯源。

智能手机摄像头结构



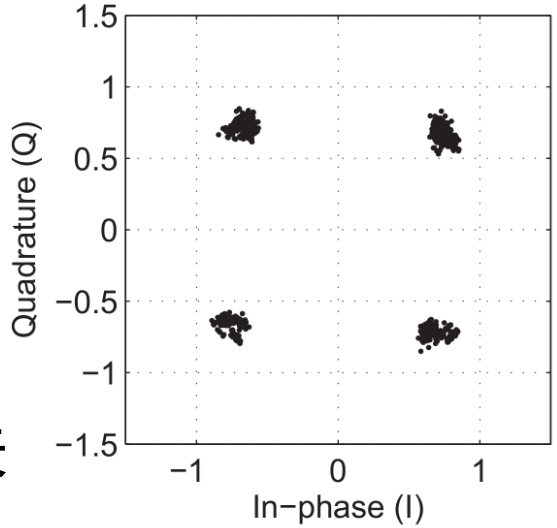
图像畸变

# 外设单元硬件设备指纹对比

| 硬件模块类别 | 具体来源 | 适用对象 | 标识特征（指纹） | 提取方法 | 特点 |
| --- | --- | --- | --- | --- | --- |
| 外设单元 | MEMS传感器 | 具有MEMS传感器的终端设备 | 输出数据偏差 | API读取传感器读数 | 访问无需用户权限，非所有终端设备均配备 |
| | 麦克风-扬声器 | 具有麦克风、扬声器的终端设备 | 麦克风-扬声器频率响应 | 或者目标麦克风采集或目标扬声器播放的音频 | 访问需要用户权限，易受环境噪声影响，非所有终端设备均配备 |
| | 摄像头 | 具有摄像头的终端设备 | 图像伪像 | 获取目标摄像头采集的图片或视频 | 访问需要用户需要权限，非所有终端设备均配备，存在隐私安全问题 |

# 基于通讯单元的硬件设备指纹

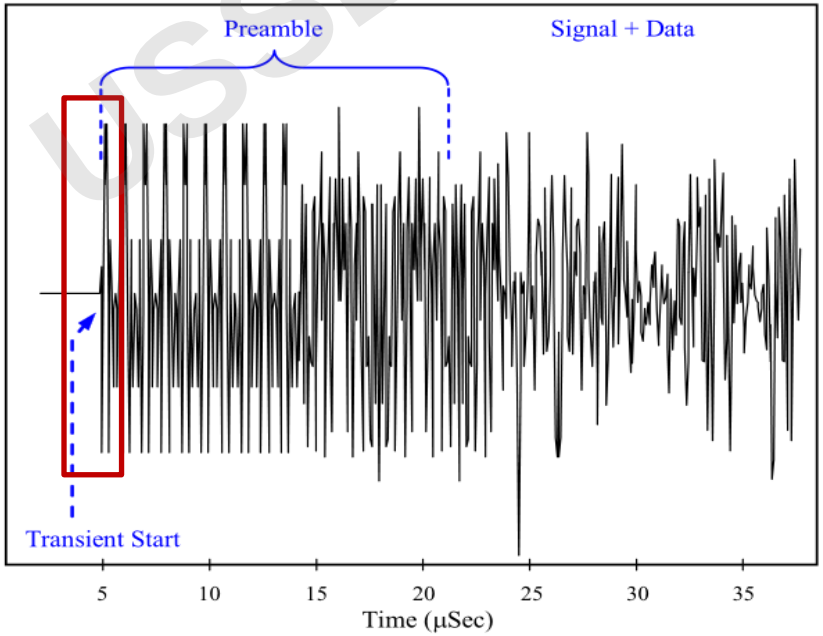
- **定义：**
  - 从无线通信信号提取“**射频指纹**”（Radio Frequency Fingerprint）
  - **来源：**由于通信硬件（发射机、接收机等）制造差异，导致的射频信号存在差异，每个无线设备有不同的射频指纹
- **分类：**
  - **瞬态**信号射频指纹技术
  - **稳态**信号射频指纹技术
- **要求：**指纹信号与通信数据内容无关




信号调制误差作为指纹

# 瞬态信号射频指纹技术

- **瞬态信号：**发射机功率**从零到达额定功率**时发送的信号部分，不承载任何数据信息，只与发射机硬件特征相关，具有**数据独立性**。其持续时间极为短暂，一般在纳秒级。
- **瞬态信号指纹：**根据发射机**开启/关闭过程中的瞬态信号**提取设备射频指纹的技术。



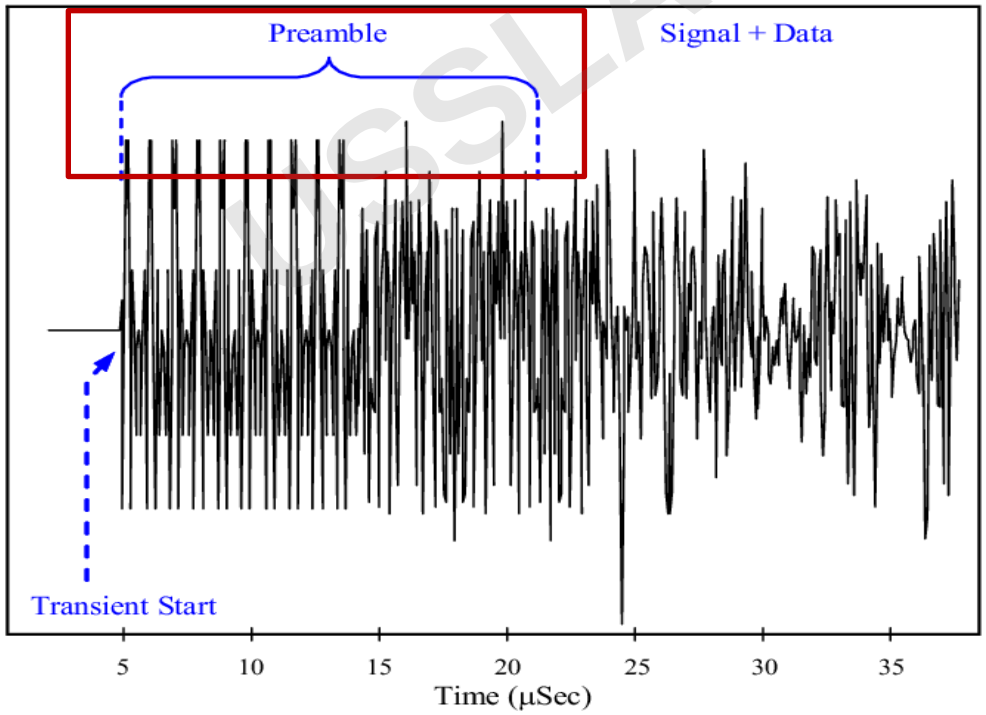





Ref: Suski, W.C., etc., “Using Spectral Fingerprints to Improve Wireless Network Security”, IEEE GLOBECOM, 2008

# 稳态信号射频指纹技术

- **稳态信号：发射机到达额定功率之后的信号状态**
- 稳态之后，信号会随数据变化。因此，射频指纹需要从相同数据包部分获取，例如数据包前导码（preamble）
- **稳态信号指纹：**利用**稳态信号**进行射频指纹提取和识别的技术






Ref: Suski, W.C., etc., “Using Spectral Fingerprints to Improve Wireless Network Security”, IEEE GLOBECOM, 2008

# 射频指纹应用场景——无线充电安全

- 如何检测公用无线充电板是否可信?


(a) Wireless charger in restaurants.


(b) Wireless charger in airports.

(c) Wireless charger in coffee shops.

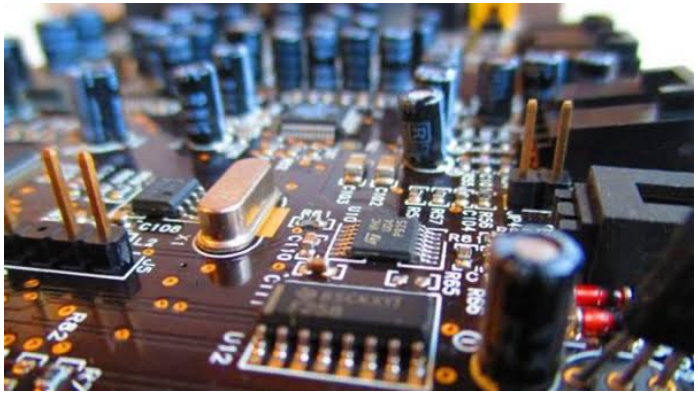
(d) Wireless charger in hotels.

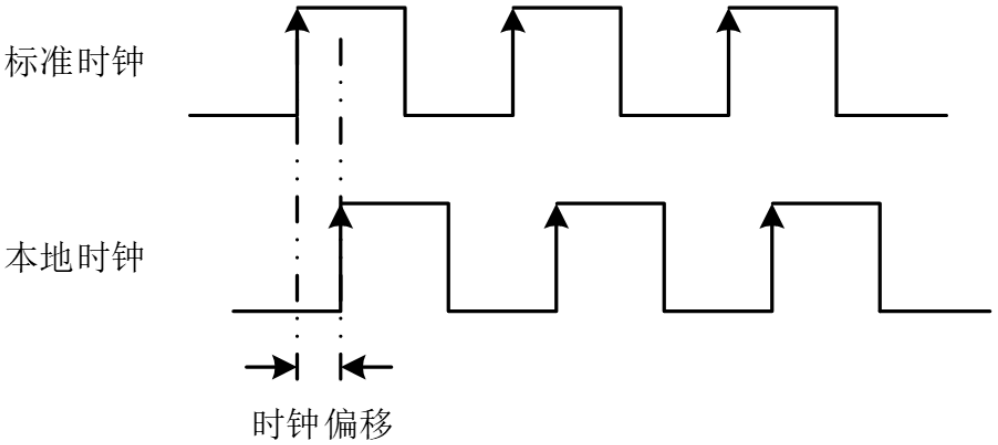
Jiayu Zhang, Xiaoyu Ji, etc., Who Is Charging My Phone? Identifying Wireless Chargers via Fingerprinting, in IEEE Internet of Things Journal, 2020

# 基于计算单元的硬件设备指纹

## 时钟晶振硬件指纹

- 晶振在生产过程中存在的差异性导致设备的本地时钟相对于标准时钟存在细微的**时钟偏移**（Clock Skew）
- 经过长时间的积累，智能设备本地时钟相对于标准时钟的偏移速率则称为设备的**时钟偏移率**（Clock Skewness）
- 时钟偏移率是一个由设备硬件系统决定的**常量**，与设备的位置、IP 地址、网络拓扑和测量时刻均无关

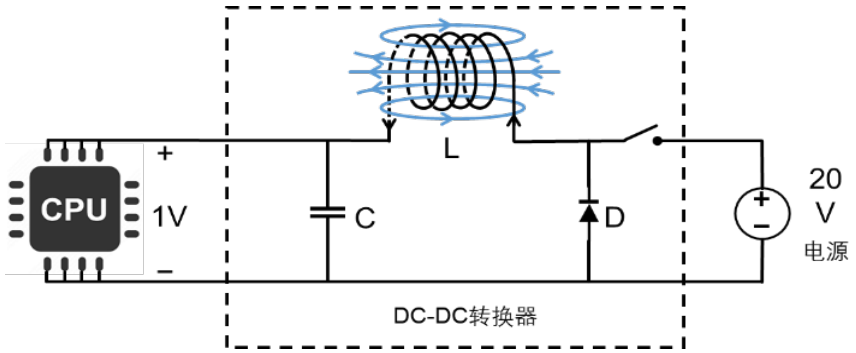




# 基于计算单元的硬件设备指纹

- **中央处理器（CPU）硬件指纹**
  - 不同型号的CPU，其**硬件结构和参数规格**存在差异；
  - 即使是相同型号的CPU，由于制造过程中由工艺限制引入**缺陷**，其硬件电路也存在细微差异，如CMOS管的差异。
  - 通过测量CPU在数据计算过程中的信号差异，例如CPU辐射的**电磁信号**，可以构造基于CPU的硬件设备指纹。
- CPU硬件指纹优势：普适性高

**应用场景：**假设支付宝登陆账户和密码丢失了，如何阻止账户在用户非授权手机上登录?




CPU模块硬件指纹原理



Yushi Cheng, Xiaoyu Ji, etc., "DeMiCPU: Device Fingerprinting with Magnetic Signals Radiated by CPU“, in ACM CCS 2019

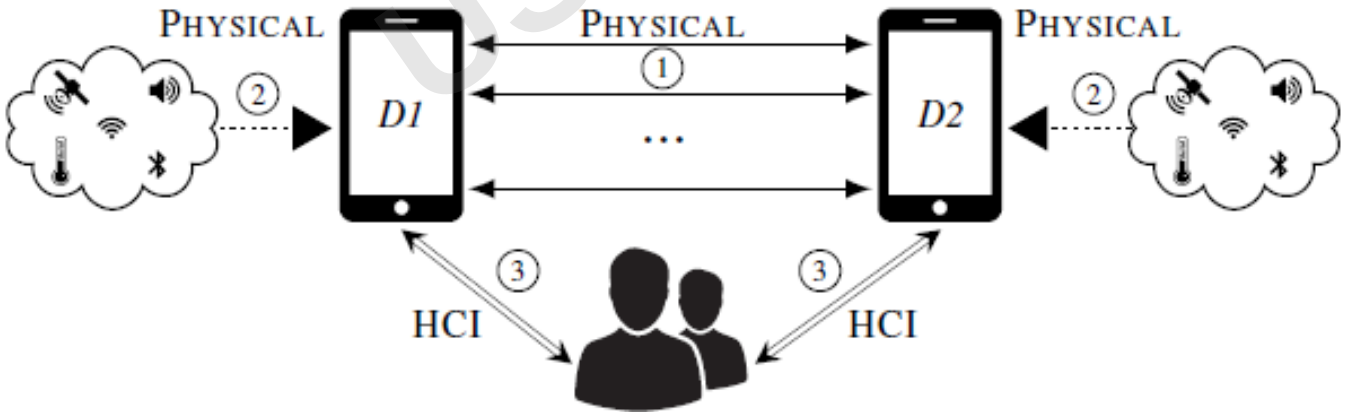
# 基于计算单元的硬件设备指纹

| 硬件模块类别 | 具体来源 | 适用对象 | 标识特征（指纹） | 提取方法 | 特点 |
| --- | --- | --- | --- | --- | --- |
| 计算单元 | 时钟晶振 | 绝大多数终端设备 | 时钟晶振偏移率 | 获取网络数据包 | 终端设备基本均配备 |
| | CPU | 绝大多数终端设备 | 电磁辐射时频域特征 | 获取CPU电磁辐射 | • 终端设备基本均配备，不受设备内部环境影响<br>• 需要额外采集设备 |

# 4.4 物联网设备配对技术

# 物联网认证——设备配对技术

- **设备配对（device paring）**：在不存在先验知识的两个设备间，利用**共同知识**来完成对彼此认证的操作
- 共同知识：包括使用物理时空信号和人机交互。
  - 物理时空信号：声音、图像、射频信号等；
  - 人机交互：利用人为输入数字信息，如蓝牙的PIN码。




Fomichev M, Álvarez F, Steinmetzer D, et al. Survey and systematization of secure device pairing[J]. IEEE Communications Surveys & Tutorials, 2017, 20(1): 517-550.

# 物联网认证——设备配对技术

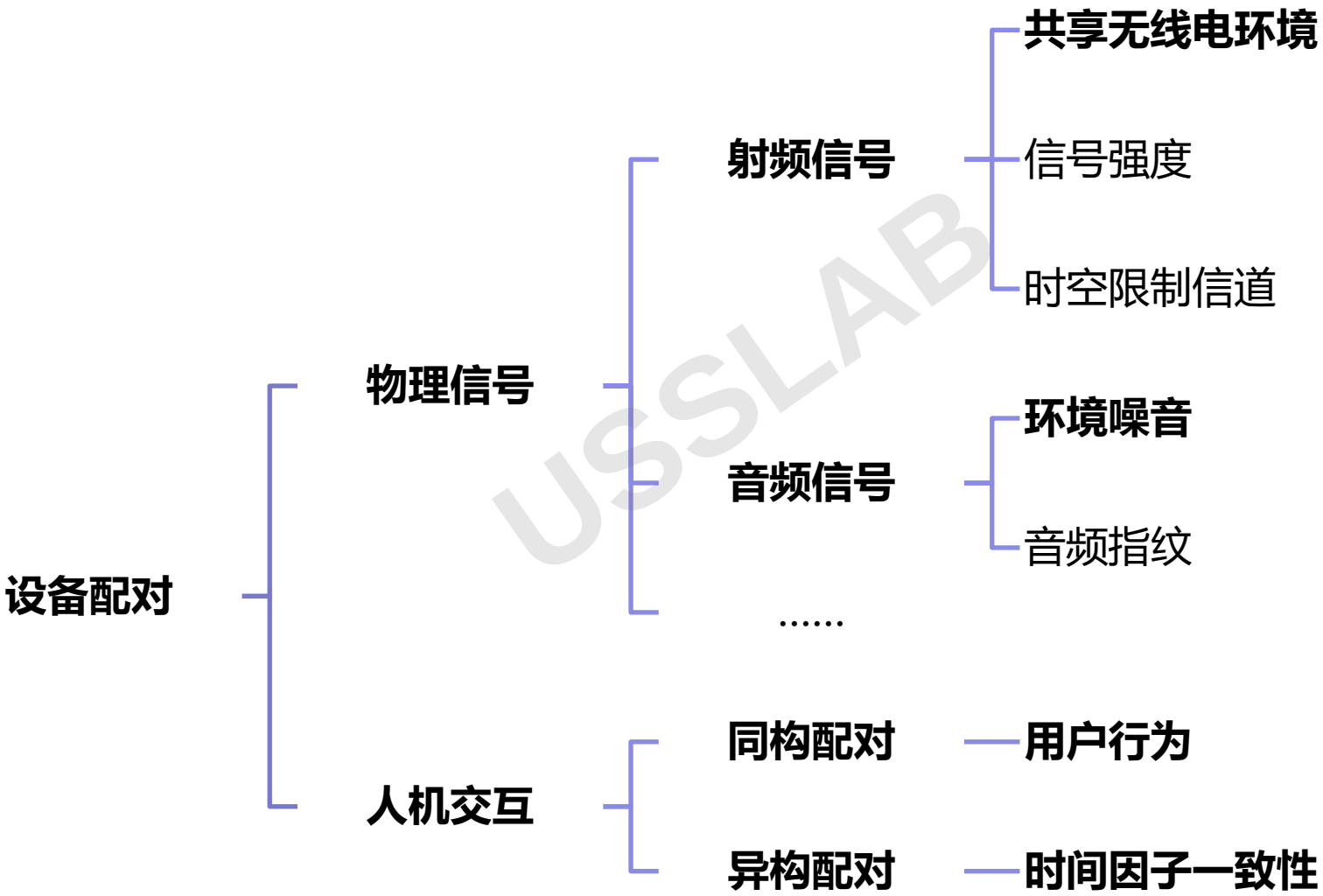
- **设备配对（device paring）**：在不存在先验知识的两个设备间，利用**共同知识**来完成对彼此认证的操作
- 共同知识：包括使用物理时空信号和人机交互。
  - 物理时空信号：声音、图像、射频信号等；
  - 人机交互：利用人为输入数字信息，如蓝牙的PIN码。



- 为什么要设备配对
  - 无需复杂的用户参与、计算成本较低
- **举例：**如何在第一次进入酒店房间以后，屋内的人可以自动连接屋里WiFi?

Fomichev M, Álvarez F, Steinmetzer D, et al. Survey and systematization of secure device pairing[J]. IEEE Communications Surveys & Tutorials, 2017, 20(1): 517-550.

# 设备配对技术

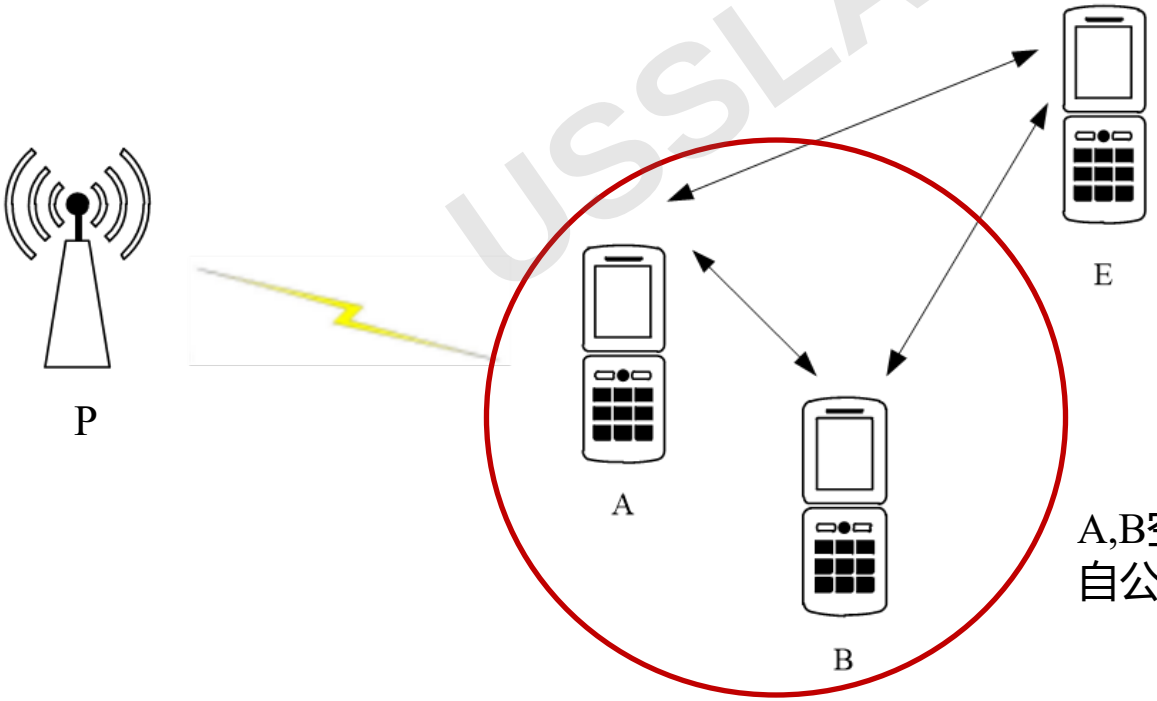


# 基于射频信号的设备配对

- **原理**:
  - 使用设备**共享的无线电环境**作为物理接近度的依据，从而验证两个设备的共存位置
- **方法**:
  - 被认证双方从共同的无线电环境动态特征中提取**相同的信号**来进行**邻近设备的配对**
- **优点**:
  - 具有很强的鲁棒性
  - 不需要其他附加硬件完成通讯
  - 不需要用户参与来验证身份验证过程的有效性

# 基于射频信号的设备配对

- **举例**:
  - Alice和Bob由于地理位置接近，来自Peter的信号在A和B出相似；
  - 攻击者（Eve）不在A/B附近，无法提取相同的信号密钥



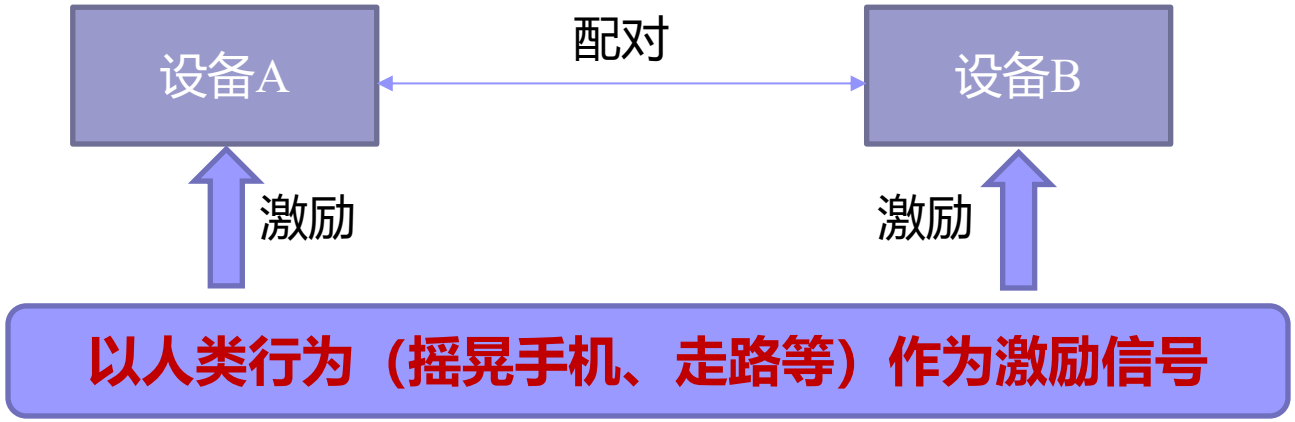

A,B空间相近，导致来自公共源P的信号相似

# 基于声音信号的设备配对

- **原理**:
  - 利用设备**麦克风**获取**环境噪音**，完成设备配对
- **方法**:
  - 两个设备分别通过麦克风记录环境噪音，比较两个噪音是否相同或者相似，完成两个设备的配对
- **优点**:
  - 麦克风在多种设备上均有普及。

# 基于人机交互产生激励进行配对

- 如果环境中没有可以用来配对的信息，则需要通过人机交互方式产生
- **人机交互方式**：如走路、摇晃、点击等操作，对两个需要进行配对的设备产生相同的激励信号
- 接收激励信号的传感器：
  - 基于**同构传感器**的设备配对，如都使用麦克风；
  - 基于**异构传感器**的设备配对，如A使用麦克风，B使用加速度计。



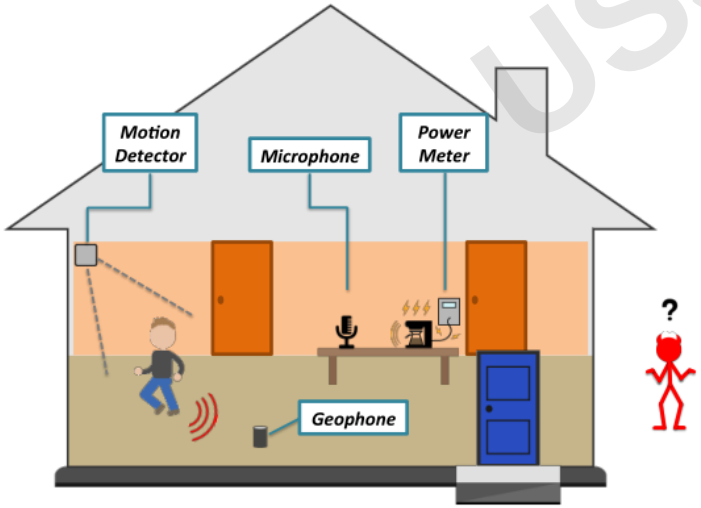
# 同构传感器设备配对

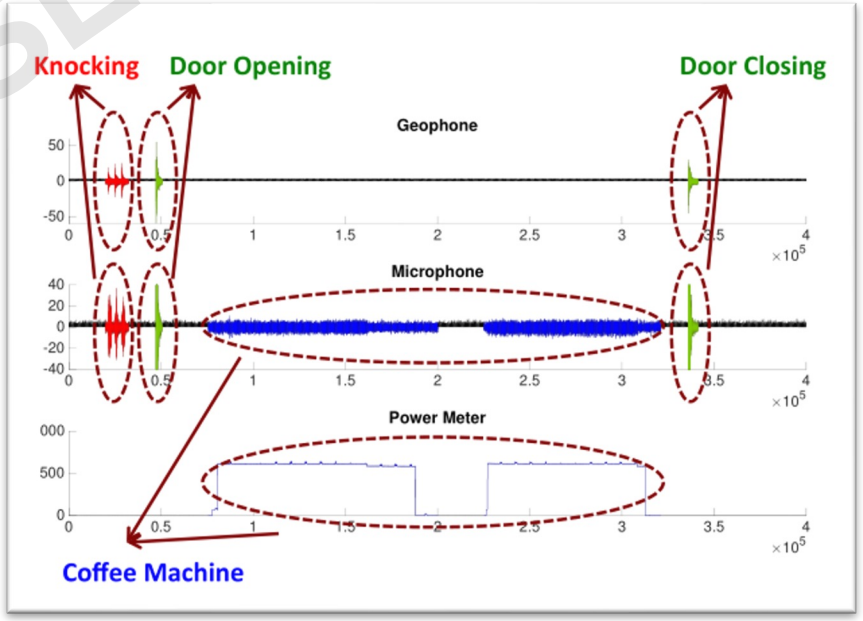
- **方法**：
  - 通过用户的行为如走路、摇动设备等对两个设备同时产生影响，认证双方通过**共同感知**到的动作作为共享知识，完成设备配对。
- **原理**：
  - 基于**相同类型**的传感器如加速度计、陀螺仪、麦克风等，并进行数据匹配从而完成设备配对。
- **优点**：
  - **不受环境限制**：除了环境中射频、音频信号之外，人可以作为信号产生的来源。
  - **信息熵更大**：人执行的单个活动片段可组成一系列事件。例如，烹饪早餐活动可以包括由同一用户执行的多个传感器事件，打开冰箱，然后取出煎锅，然后打开炉子。

**Q：如果被认证双方没有同样类型的传感器怎么办？**

# 异构传感器设备配对

- **原理：**
  - 利用人或者环境作为共同信号发生源，基于不同传感器对同一事件感知相似性，如时间长度等，用于异构传感器设备配对。
  - 案例：咖啡机、冰箱、手机等具有不同传感器的物联网设备配对



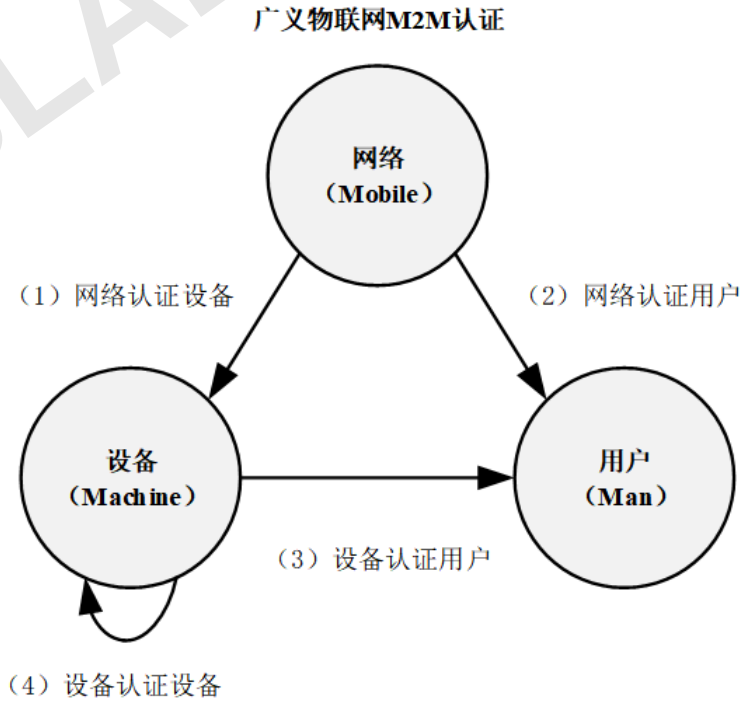





Ref: Jun Han, etc., “Do you feel what I hear? Enabling autonomous IoT device pairing using different sensor types”, IEEE S&P 2019

# 本章总结

- **物联网**:
  - 特点：轻量级、多安全等级、跨平台的特点需要新的认证方式
- **物联网认证三要素：**
  - 网络（Mobile）
  - 设备（Machine）
  - 用户（Man）
- **物联网生物认证技术**
  - 常用生物认证技术
- **物联网设备指纹认证技术**
  - 常见硬件指纹认证



# 一千个人有一千条密码？

- **密码设置偏好排名**

| | 中文 | 英文 |
|---|---|---|
| 1 | 123456(2.17%) | 123456 (0.88%) |
| 2 | 123456789(0.65%) | 12345(0.24%) |
| 3 | 111111(0.59%) | 123456789(0.23%) |
| 4 | 12345678(0.39%) | password(0.18%) |
| 5 | 000000(0.34%) | iloveyou(0.15%) |

- **中文拼音/英文单词密码偏好排名**

| | 中文拼音 | 英文单词 |
|---|---|---|
| 1 | woaini (1.47%) | password (1.28%) |
| 2 | li (1.06%) | iloveyou (0.98%) |
| 3 | wang (0.97%) | love (0.76%) |
| 4 | tianya (0.89%) | angel (0.59%) |
| 5 | zhang (0.84%) | monkey (0.45%) |

# 密码偏好设置特点

- 在相似的强度下，中文密码包含更多的纯数字（>50%）的密码。
- 就像英文密码中的英文单词一样，中文密码中也会出现中文拼音（10%-15%）。