南京大学
NANJING UNIVERSITY

物联网与隐私

殷亚凤
智能软件与工程学院
苏州校区南雍楼东区225
yafeng@nju.edu.cn，https://yafengnju.github.io/

物联网与隐私

- **基于传感器的隐私泄露**
- 基于流量的隐私泄露
- 物联网安全隐私防护

传感器的分类

隐私敏感的传感器

- 摄像头、麦克风等
- 能轻易地窃取人们的隐私，被严加看护

Google眼镜

Hololens

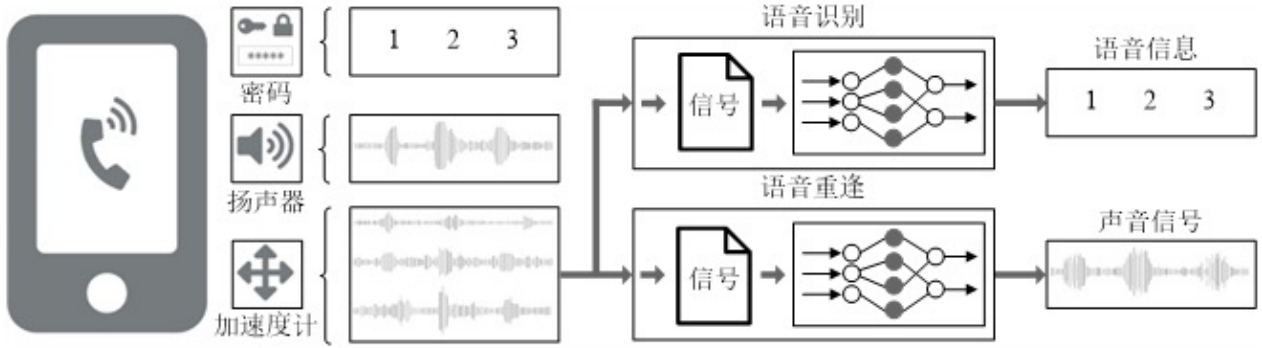
小米手环

传感器的分类

隐私不敏感的传感器

- 加速度、陀螺仪
- 看似提供信息不多，容易对其放松警惕，但经过特殊设计，也能窃取到很多隐私信息

典型的隐私泄露案例: 密码盗窃 轨迹泄露 语音窃听



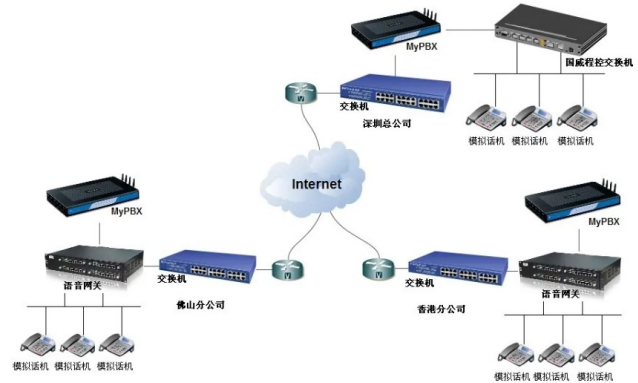
使用传感器窃取用户的隐私

物联网与隐私

- 基于传感器的隐私泄露
- **基于流量的隐私泄露**
- 物联网安全隐私防护

基于流量的隐私泄露

网络加密语音通话VoIP并非牢不可破



基于流量的隐私泄露

智能家居

- 使用WiFi接入互联网
- 嗅探网络空间中物联网常用协议的信号，推测智能家居的运转情况
- 捕捉空间中智能家具信号，通过神经网络处理信号，推断各设备的工作情况，推测用户的活动情况

物联网与隐私

- 基于传感器的隐私泄露
- 基于流量的隐私泄露
- **物联网安全隐私防护**

物联网隐私安全防护手段

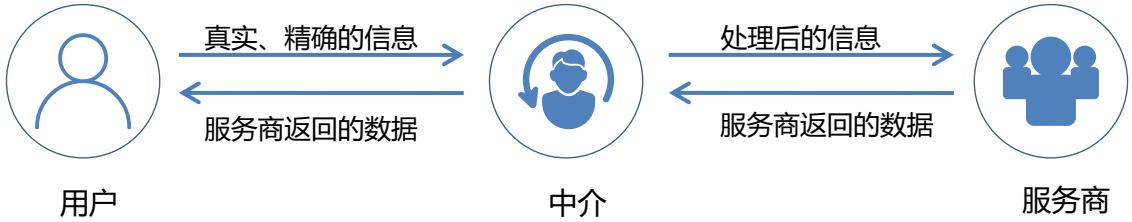
身份匿名

将数据中的真实身份信息替换为一个匿名的代号，隐藏位置信息中的“身份”

服务商能利用位置信息提供服务，但无法推断用户身份

常用技术

- K匿名：引入可信中介，让用户发布的信息和另外k-1个用户的信息变得不可分辨



保护位置隐私的手段

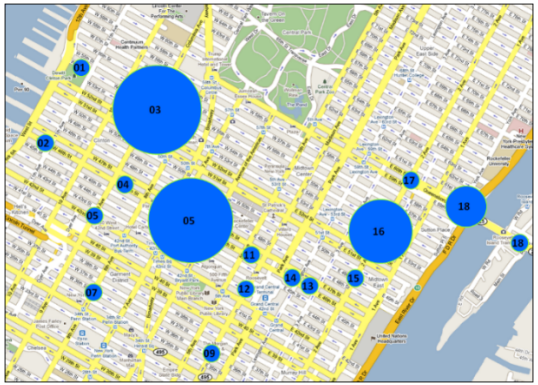
数据混淆

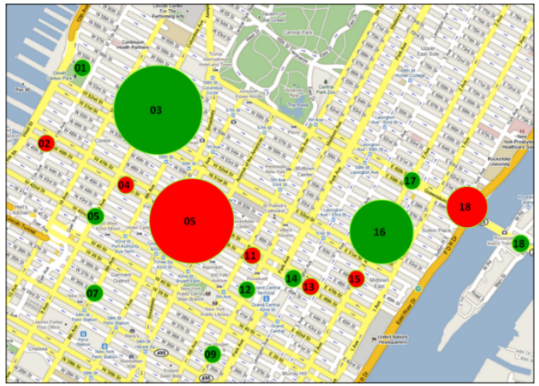
基本思想

- 通过对数据进行混淆，避免攻击者得知用户的精确信息

三种方法（以位置隐私为例）

- 模糊范围：降低位置信息的精度，从精确位置到区域
- 声东击西：偏离精确位置
- 含糊其辞：引入模糊语义词汇，例如“附近”





保护位置隐私的手段

从感知数据的特点出发

通过主动检测手段找出或干扰攻击者预先放置的物理嗅探设备或软件

- 摄像头：频闪灯光
- 网络摄像头：分析网络流量
- 无线嗅探装置：主动发射数据

提问

Q & A

殷亚凤
智能软件与工程学院
苏州校区南雍楼东区225
yafeng@nju.edu.cn，https://yafengnju.github.io/

南京大学 NANJING UNIVERSITY