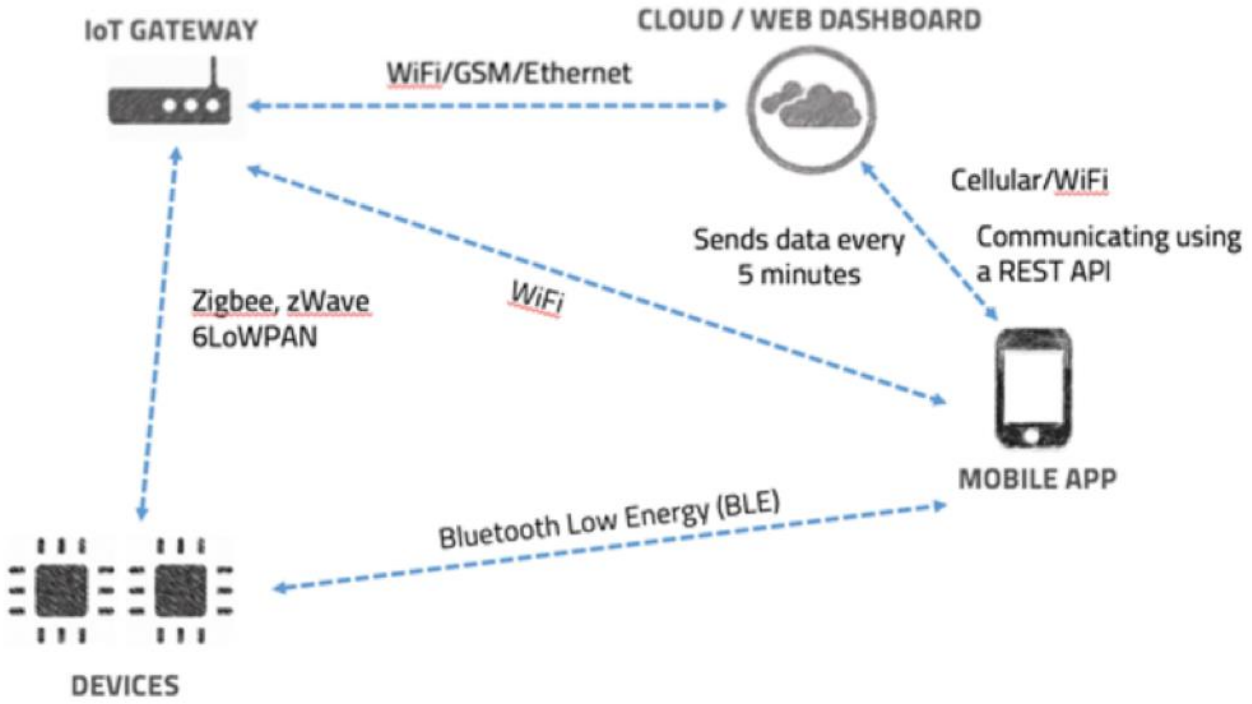
Internet of Thing
安全研究介绍

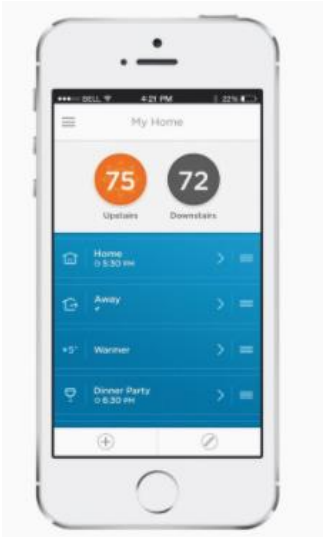
研究对象

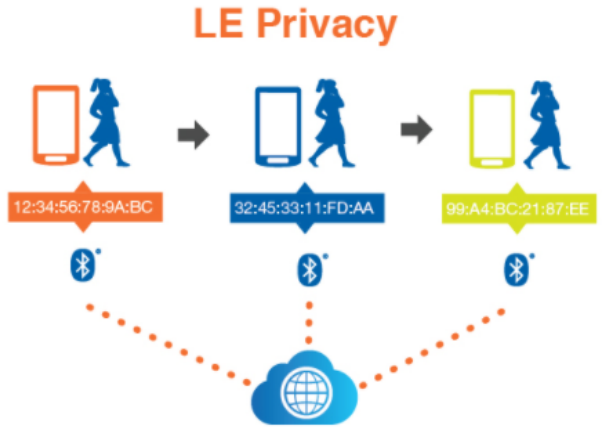
- 嵌入式设备
- 网络通信协议
- 移动终端应用



研究内容

- 设备固件安全分析
- 无线通信协议安全分析
- 移动端应用实现安全分析
- 机密数据泄漏与防护
- 数据追踪与一致性问题





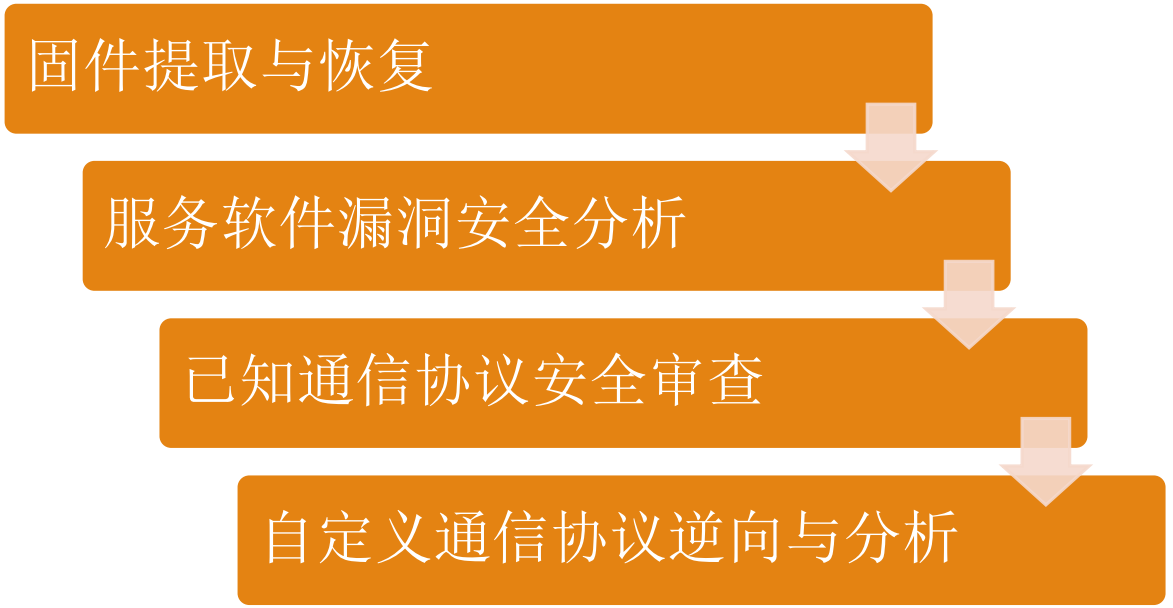
物联网设备固件安全分析

对物联网设备固件逆向，是理解其核心逻辑算法和协议的最重要手段！

- 分析目标
  - 提取并成功解析设备固件代码，**还原其使用的算法、协议**
  - 审计设备中包含的网络服务及其通信协议实现安全性
  - 重点关注**私有自定义通信协议**并分析其安全性

固件安全分析技术要点

- 固件提取技术
  - ✓已知数据格式特征库构建
  - ✓存储器转储
  - ✓数据格式恢复
- 固件分析
  - ✓寻找硬编码的密码，API key，证书
  - ✓网络接口安全分析
  - ✓二进制服务的软件漏洞
    - ✓ 如缓冲区溢出，命令注入，DoS
  - ✓模拟执行固件的执行环境（QEMU ，Unicorn等）

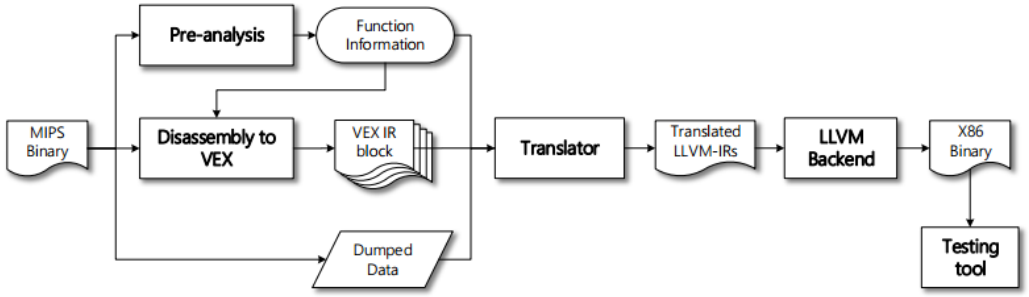


Securecomm 2016

- Security Analysis of Vendor Customized Code in Firmware of Embedded Device
  - **分析嵌入式设备固件中的厂商私有代码部分**
  - 关注其中的安全漏洞，发现了路由器、网络设备等的漏洞
  - 重点关注**私有自定义通信协议**并分析其安全性

CollaborateCom 2016

- Security Testing of Software on Embedded Devices Using x86 Platform
  - **通过二进制代码翻译来增强嵌入式设备固件代码分析**
  - 将MIPS代码翻译成x86代码进行分析
  - 可以将成熟的代码分析技术引入到嵌入式设备代码分析上



Securecomm 2016

- Security Analysis of Vendor Customized Code in Firmware of Embedded Device
  - **分析嵌入式设备固件中的厂商私有代码部分**
  - 关注其中的安全漏洞，发现了路由器、网络设备等的漏洞
  - 重点关注**私有自定义通信协议**并分析其安全性

IoT SP @ CCS 2017

- Smart Solution, Poor Protection: An Empirical Study of Security and Privacy Issues in Developing and Deploying Smart Home devices
  - **分析智能家居部署过程中的安全问题**
  - 关注其中的安全漏洞，发现了京东微联设备的漏洞
  - 重点关注**京东微联协议**并分析其安全性

WiSec 2018

- Passwords in the Air: Harvesting Wi-Fi Credentials from SmartCfg Provisioning
  - **分析SmartCFG配网方案的安全问题**
  - 分析了8类SmartCFG解决方案，60余款智能家居设备
  - 关注其中的Wi-Fi password泄漏问题，发现了大量智能家居设备的漏洞

智能门锁分析

当前主流的智能门锁安全问题

- 小猪短租：中间人攻击
- 夏洛克：直接嗅探和开锁
- Keylocker：直接嗅探和开锁
- Xxx：

智能电视安全分析

三款智能电视测试

- 海信
- 微鲸
- 模卡
- 安全问题
  - 漏洞未修复
  - 权限管理存在问题