IoT安全的To B与To C

王滨　海康威视CSO

IoT设备包括哪些？


工业智能机器人
家用路由器
心脏起搏器
自动驾驶汽车
摄像头
心脏起搏器
手环
各种传感器
智能家居
智能音箱
智能窗帘

公众眼中的IoT安全


央视曝光大量家庭摄像头遭破解，防止隐私泄露做到这几点很重要


搜狐 健康
黑客控制心脏起搏器杀人？ 安全专家称可以实现


滚动
女孩啪啪时戴运动手环 全程被监测 盘点那些被偷偷的尴尬场面[图]


细思极恐，当你的车辆被黑客远程控制


亚马逊旗下智能音箱存在漏洞可被变成窃密的监控工具
正版软件商城

安全研究人员眼中的IoT安全

- 弱口令
- 暴露在互联网上
- 漏洞

ToB：弱口令、漏洞、暴露在互联网上

ToC：弱口令、漏洞

ToC—设备可以不暴露在互联网上

ToB—设备大量暴露在互联网上

- 本身为了应用的需要暴露在互联网上
- 设置不当导致设备暴露在互联网上

IoT设备安全永远的痛--弱口令

用户：安全意识淡薄，亟待提高

厂商：早先的产品存在密码硬编码/未使用更加健全的口令机制

国家信息安全标准委员会（TC260）
《信息安全技术-智能联网设备口令保护指南》

IoT设备安全无法回避的问题—漏洞

ToC安全该怎么做？

ToB安全该怎么做？

- 设备需要开放多种端口
- 用户安全意识普遍不高
- 系统网络环境复杂多样
- 纵深防御很难有效实施
- 历史累积问题堆积如山

- 厂商提供更高产品安全要求
- 为用户提供轻管理的安全防护方案

IoT设备漏洞的几点呼吁

- 目前业界遵循的90天的漏洞披露策略对于无有效升级途径的物联网设备并不适用；
- POC的检测更推荐采用版本检测的方式；
- 用户设置周期性固件更新计划任务，弱口令一定要避免；
- 厂商加强设备的安全设计、开发、测试和应急响应；
- 行业主管机构必须要有强制的检查和通报机制


FREEBUF | FIT
THANKS