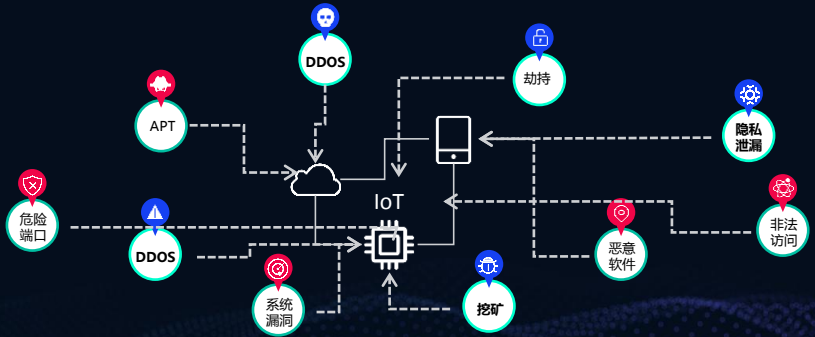
IOT安全实践：高效协议分析

骇极CEO Zenia

为什么需要关注IoT安全

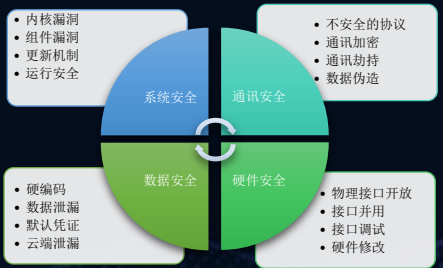
为什么要关注IoT安全

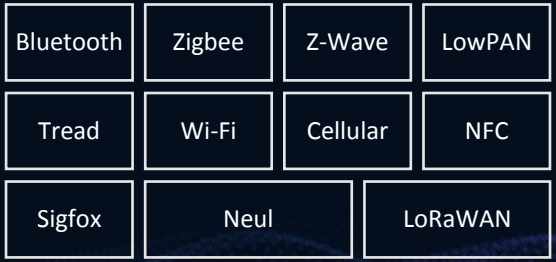
- 2016年10月，美国最主要的DNS服务商Dyn遭遇了来自超过1000万台IoT设备的DDos攻击，瘫痪了大半个美国的网络
- 2017年3月，一款智能玩具CloudPets泄漏了200多万条儿童与父母的录音和80多万账户
- 2018年5月， Z-Wave降级攻击导致1亿多物联网设备被黑客攻击
- 2018年11月，CarsBlues蓝牙漏洞 影响全球数千万辆汽车


DDOS
劫持
APT
隐私
泄漏
危险
端口
IoT
非法
访问
DDOS
恶意
软件
系统
漏洞
挖矿

IoT安全需要关注哪些内容

IoT安全需要关注哪些内容




Bluetooth
Zigbee
Z-Wave
LowPAN
Tread
Wi-Fi
Cellular
NFC
Sigfox
Neul
LoRaWAN

通讯上层协议

- 传统文本协议（HTTP、FTP、Telnet等）
  - 优势：开发资源丰富、易于实现具体功能
  - 劣势：攻击门槛低、大量在代码上的实现漏洞被移植到设备上
- 工业协议（Modbus、CAN等，二进制协议居多）
  - 优势：协议成熟，通信效率高
  - 劣势：扩展性差，缺乏可靠的安全设计
- 自定义协议（BLE、TCP/UDP应用层，二进制协议居多）
  - 优势：灵活多变、封闭协议难以被公开资料解析
  - 劣势：许多自定义协议同样缺乏安全设计

为什么关注协议安全

- 协议是通讯的基础
- 伪造通讯数据需要理解协议
- 协议引发的安全问题普遍

IoT攻击基础路径：协议逆向

为什么要进行协议逆向

- 可以理解协议的格式，提取数据中的信息
- 发现协议中的控制字段，尝试发现漏洞点和滥用设备功能
- 解析数据中的特定区域，尝试注入畸形数据以发现未知漏洞

协议逆向方法

- 对数据的关键信息（如IP、端口、连接、文本关键字等）进行过滤
- 根据对应操作（如开关灯），对比数据中的相应变化，定位功能
- 人工跟踪数据交互流程，标记不同条数据的逻辑关系

人工逆向的优劣

优势：

- 灵活性
- 精确性

劣势：

- 需要过滤大量无用数据
- 反复分析字节变化，找到变化特征
- 报文间关联提取耗时耗力
- 程序受到加固/保护情况下难以直接跟踪

如何高效进行协议逆向

《人科进化图》 复旦大学 - 李辉教授绘制

关于进化树

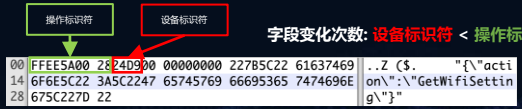
在进化系统中，影响生物特征变化巨大的基因（例如控制肺叶和腮体征变化等）其基因多样性变化率远远小于在功能和体征上引起较小变化的基因

同样这种统计特征出现在一些IoT协议中，例如设备标识符这类决定设备唯一性的字段（基因）在一堆协议数据中基本保持不变，其变化率远远小于那些控制数据字段，例如温度，亮度等操作数据

字段变化次数: 设备标识符 < 操作标识符 < 数据字段

自定义协议示例

- 协议数据会包含一个特定的操作标识字段
- 协议为连接的设备分发标识符，该标识符会反复出现在之后的报文中
- 协议数据会包含一个数据字段，其中可能包含某一个具体的操作命令或者需要传输的数据



字段变化次数: 设备标识符 < 操作标识符 < 数据字段

某智能网关获取Wi-Fi配置指令

聚类分析

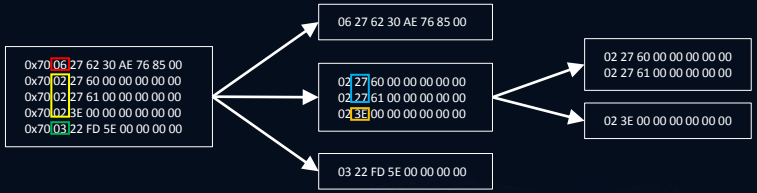
- 获取数据集（数据包）
- 聚类分析

  使用贝叶斯/最大似然法构建一个以**元操作**或**设备标识符**为根节点的进化树，使得被视为同一物种（某一个操作）的报文集中在某个叶子节点上，从而完成聚类

- 提取标识符

  同一操作的数据进行比对，操作标识可能出现在公共序列中
  对所有操作的报文进行比对，设备标识可能出现在公共序列中

聚类示例



通过对二进制数据字节进行特征提取，建立协议的报文格式模型

建立状态机


类1
70 00 B9 00 F1 42 09
初始化
类2
A5 24 A2 01 95 00 C2
类3
BE 39 80 01 8A 47 7D
操作状态转换
类4
B2 69 00 01 11 58 00
类5
DA 4F 19 01 09 00 00

解决了什么？

解决了什么？

- 噪声信号被聚类，可以定向的分析有用数据
- 可以快速标识出变化字节
- 通过状态机有效识别出信号的关联关系，避免在繁杂的数据中寻找关联

更高效的IoT安全测试

- 提升对未知协议的安全测试能力

  IoT领域存在大量非文本的二进制自定义协议

- IoT数量快速增长，满足大量安全检测需求

  基于机器的逆向技术有效的提升了效率

- 自动化FUZZ平台的构建

  基于协议格式的精确FUZZ是发现漏洞的有效途径


FREEBUF | FIT
THANKS