MIDC·2020
小米AIoT安全峰会

车联网安全的攻与防

郑涛　某车联网安全研究负责人

个人介绍

郑涛 网名海盗/haidao

搞WEB安全出身河南人。

混迹过新浪、去哪儿、阿里巴巴。

目前方向在车联网安全领域。

外表因循守旧，内心放荡不羁。

安全的本质是病从“口”入

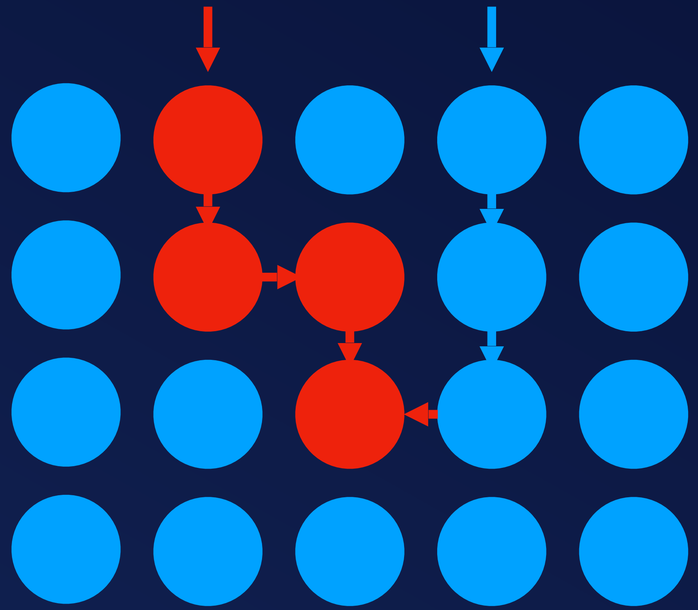
系统处理了预期外的数据，导致偏离了原来的运行轨迹

常规渗透套路

信息收集

漏洞挖掘的战略与战术

阵地战 VS 特种战



手电筒方法论

拓展攻击面与活体调试

挖掘隐藏攻击面

- ★ 键盘鼠标；
- ★ USB网卡；
- ★ IoT设备；

活体调试方法

- ★ 内部调试程序；
- ★ 固件模拟；
- ★ 重写固件；

借东风与打七寸

隐藏业务-内部调试程序

- ★ 拨号盘拉起；
- ★ 加密U盘拉起；
- ★ 远程消息下发拉起。
- ★ 双指或多指操作等。
- ★ 组合键。

显式业务-系统业务逻辑

- ★ 车辆远程控制与交互；
- ★ 系统升级与应用升级；
- ★ 个人网络应用；

实验室建设 - 黑盒流量分析

DNS/路由劫持

- ★ 自动识别域名请求
- ★ 自动劫持
- ★ 自动/手动IP路由劫持

HTTP/HTTPS劫持

- ★ 自动JS执行测试
- ★ 定制相应内容
- ★ 请求与响应修改与记录

自动漏洞检测

- ★ TSP自动扫描
- ★ 网络库漏洞识别

防御的核心是平衡

内视法与核心风险

公司定位 决定核心风险

- ★ 整车厂核心风险是安全PR
- ★ 主机厂核心风险是安全交付
- ★ 服务商核心风险是服务稳定与黑产
- ★ IoT厂商核心风险是用户隐私

团队定位 决定做事范围

- ★ 打阵地战? 打游击战?
- ★ 保障? 研究? 审核?
- ★ 内核? 协议? 基带?

逐级防御

移动安全	WEB安全	通道安全	应用安全	系统安全
个人隐私	管理后台	加密	应用鉴权	安全引导
凭证保存	API 鉴权	验签	端口开放	漏洞缓解
协议安全		防重放	协议安全	开源组件
三方库			三方库	边界防护

脚踏实地

安全运营

团结一切可团结的力量

走可持续发展的道路

SDL

基础安全能力建设

基线安全

编码安全

发布流程卡点

业务安全

架构评审

业务逻辑评审

代码实现审核

MIDC·2020
小米AIoT安全峰会

智能生活
安全护航

Thanks