汽车TBOX安全性分析与测试

TBOX是什么

- 现代汽车进入车联网时代，简单来说就是实现以车辆、人、服务器为节点组成的网络，TBOX是一种车载智能终端，用来实现对车辆的远程信息提取和远程控制
- **方式：**内置、OBD
- **功能：**ECU的远程监控和远程控制
- **代表：**现代bluelink
  GM on-star
  snap-on
  Verizon Wireless

TBOX是什么

- STM32F103
- 256MB Flash
- GPS
- 2G/GPRS
- G-Sensor

- 通信方式：
- 2G/GPRS
- USB 端口
- OBD 接口

安全问题

- 近年来TBOX正在迅速成为汽车行业中的标准组件，然而由于汽车的信息安全性漏洞导致的汽车攻击事件屡有发生，人们对于TBOX的安全性问题非常关注
- Rapid7破解bluelink
- Kamkar破解on-star
- Miller 破解UConnect

- 本PPT主要对TBOX的安全性问题及其检测进行分析，简单介绍了TBOX的一些漏洞和攻击方法，包括存储安全、接口安全、CAN总线访问安全等等

车辆攻击

攻击方式

驻车状态：

- CAN总线
- Flash
- USB debug 端口

可以通过物理访问TBOX，直接与汽车网络通信

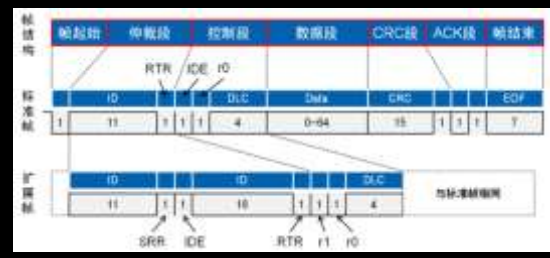
行车状态:

- SMS
- 2G/3G/4G

无法访问TBOX，甚至不知道地理位置

CAN总线

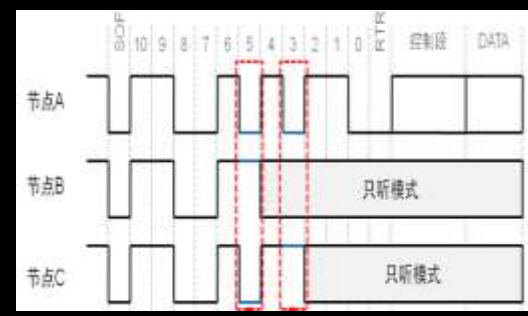
- 汽车内ECU通信网络
- 标准/扩展CAN数据格式
- 标识符
- CAN总线的安全漏洞：
  - 多主站性
  - 广播性
  - 仲裁机制
  - 错误处理机制




```
0x378 0x00 0x00 0x46 0x00 0xff 0x00 0x80 0x00 0x08 Standard Data
0x623 0x00 0x00 0x00 0x00 0x0e 0x04 0x31 0x1a 0x08 Standard Data
0x2e9 0x84 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x08 Standard Data
0x310 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x08 Standard Data
0x0fa 0x00 0x00 0x25 0x00 0x00 0x53 0x00 0x00 0x08 Standard Data
0x270 0x04 0x00 0x00 0x00 0xfe 0x00 0x00 0x79 0x08 Standard Data
0x430 0x00 0x00 0x7b 0x22 0x5c 0x41 0x7d 0x06 0x08 Standard Data
0x2e9 0x84 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x08 Standard Data
0x310 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x08 Standard Data
0x0fa 0x00 0x00 0x25 0x00 0x00 0x53 0x00 0x00 0x08 Standard Data
0x270 0x04 0x00 0x00 0x00 0xfe 0x00 0x00 0x79 0x08 Standard Data
```

CAN总线

- 非破坏性逐位仲裁
- 按位对标识符进行仲裁，各节点在向总线发送电平的同时，也对总线上的电平读取，并与自身发送的电平进行比较，如果电平相同继续发送下一位，不同则停止发送退出总线竞争，直到总线上只剩下一个节点发送的电平，竞争结束，优先级高的获得总线控制权



CAN总线

- DOS攻击：
- 最高优先级标识符
  - 发送000ID
- 篡改TBOX发送的数据
  - 错误计数器累计增加
  - 超过256时总线关闭

名称	帧ID	帧类型	帧格式	DLC	数据	帧计数
接收	391	DATA	STANDARD	8	40 00 00 00 00 10 38 C2	8191
接收	2E9	DATA	STANDARD	8	84 00 00 00 00 00 00 00	16384
接收	310	DATA	STANDARD	8	00 00 00 00 00 00 00 00	16351
接收	0FA	DATA	STANDARD	8	13 28 2E 00 00 2F 00 00	16957
接收	2C0	DATA	STANDARD	8	8C 4E 13 AF FE 00 00 80	16351
接收	2C0	DATA	STANDARD	8	47 04 17 96 49 70 F7 CD	16350
接收	370	DATA	STANDARD	8	47 56 00 18 4E 00 00 00	16350
接收	370	DATA	STANDARD	8	80 00 53 00 FF 00 80 00	16349
接收	430	DATA	STANDARD	8	00 00 0F 02 46 41 78 06	7980
接收	398	DATA	STANDARD	8	03 00 00 00 00 00 00 00	1638
接收	31C	DATA	STANDARD	8	80 00 00 00 00 00 00 00	331
接收	623	DATA	STANDARD	8	80 00 00 00 00 0E 04 31 1A	168
接收	706	DATA	STANDARD	8	07 0C 09 02 01 3D E8 00	81
发送成功	000	DATA	STANDARD	8	8A 26 00 00 00 00 00 00	888704

CAN总线

- TBOX接入方式：
- 直接作为一个节点接入CAN网络
- 集成在汽车网关中
- 通过OBD接口接入汽车网络

- 三种方式虽然不同，但都可以实现CAN数据的接收和发送，进而进行数据篡改和重放攻击

- 重放攻击：
  - 数据采集
  - 定位ID
  - 数据解析
  - 重放

- 以上是CAN总线逆向的流程，找到对应攻击的数据后设置数据域进行重放，此过程中还可能需要配置滚动计数和校验和

CAN总线

- 车门

CAN总线

- ABS报警和安全气囊

存储安全：Flash读取

- 找到文件系统布局
- 拆焊Flash
- 设计Flash读取仿真环境
- 分区读取数据

Flash数据中包含了公钥、私钥和认证信息，这对于后面的远程攻击有重要作用

接口安全：USB Debug

- 连接USB接口之后设置它的子网和IP地址
- 利用USB网络可以调取网络服务和SSH服务
- SMS 短信发送接口获取SIM号码

通过这些接口可以获取SIM芯片信息、GPS信息和TBOX设备参数，还可以修改TBOX的配置

远程攻击

- 非双向认证
  - 带恶意代码的更新文件
  - 2G伪基站
- 未使用NAT
  - SSH Key 登录
  - 获取用户软件权限

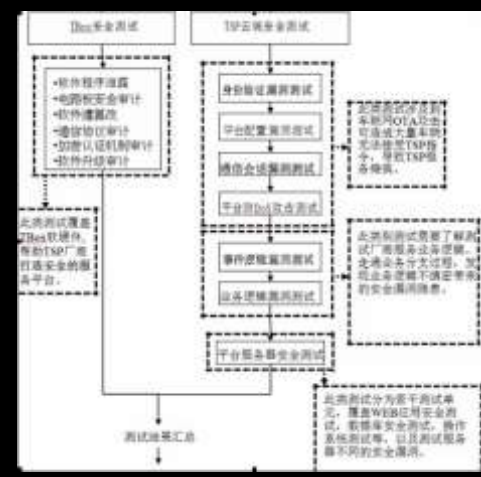
远程攻击

- 远程更新攻击：
- 利用SMS启动更新响应
- 设备向服务器请求更新文件
- 利用恶意服务器传输包含恶意命令的UpdateFile.txt

- 远程更新攻击很具有威胁，因为它可能提供一种机制来获取反向shell和命令解析方法, 从而实现任意访问
- 攻击成功后可以设置触发条件，在触发后执行清除、更改、重置等命令操作

安全检测

- TBox测试项目:
- (1)软件程序安全测试
- (2) 硬件电路安全测试
- (3)总线安全检测
- (4)更新安全检测
- (5)加密认证机制测试



(1)软件程序泄露

- 最小权限检测/权限分离：
  - 用户模式
  - 内核模式
- 最小功能检测：
  - 系统软件
  - 第三方软件
  - 后门攻击

(2)硬件电路安全测试

- 电路板安全审计
- 恶意代码植入
- 反汇编防护
- 安全芯片

(3)总线安全检测

- TBOX与总线是否进行通信隔离
- CAN网络侵入检测/网络异常
- DOS安全检测
- CAN网络数据安全检测：
  - 数据篡改
  - 重放攻击

(4)更新安全检测

- 更新文件完整性检测
- 是否进行身份验证保证真实性
- 是否进行强加密的服务器身份验证

(5)加密认证机制

- 是否进行身份验证
- 本地验证与通信验证的独立性
- 身份验证机制检测：
  - 数字签名
  - 消息认证码
- 关键数据是否加密与加密算法

谢谢！