
看雪·第六届安全开发者峰会
国产智能网联汽车漏洞挖掘中的几个突破点
马良 绿盟科技 格物实验室 安全研究员
2022 SDC

自我介绍

马良 绿盟科技 格物实验室 安全研究员

十多年嵌入式软、硬件开发经验, 喜欢DIY一些东西

- 2016 - Xpwn：西门子PLC蠕虫演示
- 2018 - 看雪开发者大会：智能设备固件提取的十种方法
- 2018 - 极棒：机器特工挑战赛，关闭激光报警器电源、窃听器放置、气球遮挡摄像头等
- 2018 - JD-HITB：介绍Vocore2模块在安全研究中的应用，提出一种工控设备攻击模型
- 2021 - 极棒《我是极客》：改装电源插座，通过4G用电力猫安全缺陷远程控制内网设备

目 录

概 述

- 常用软硬件
- 固件提取
- 工程模式
- 案例
- IVI(车载信息娱乐系统)
- ADAS(辅助驾驶)

目 录

测车常用工具

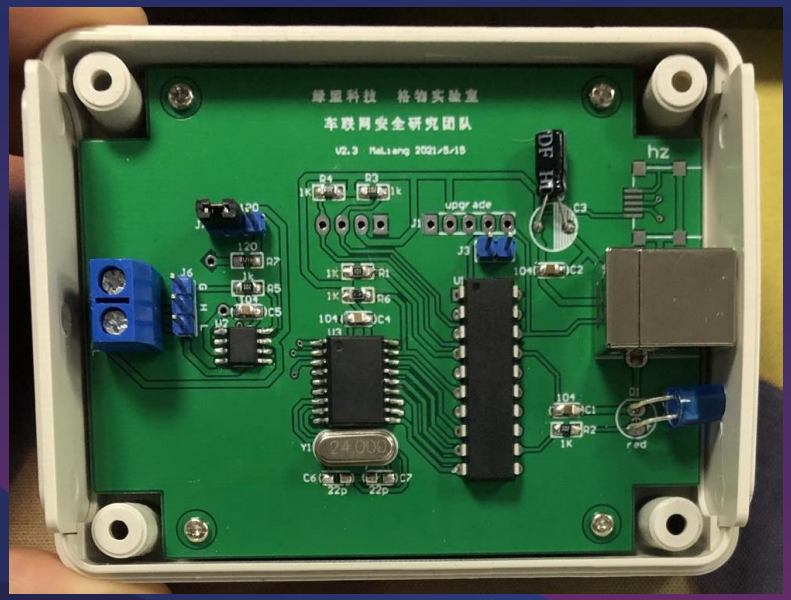
出去测试车，一般要带一些工具，例如：

- 各种接口的USB线
- USB转TTL模块(各种常见电压:、5V/3.3V/1.8V)
- 各种容量的tf卡和读卡器、U盘
- 网络抓包的HUB，车载以太网转换器
- Wi-Fi抓包环境、蓝牙抓包环境
- CAN总线抓包、分析和重放的软件和硬件
- CAN总线Fuzz模块
- HarkRF One with Portapack H2 或 其它SDR
- 调试用的安卓手机(Root、装好各种调试软件)，各种APK分析工具

CAN总线收发和Fuzz工具

USBTin

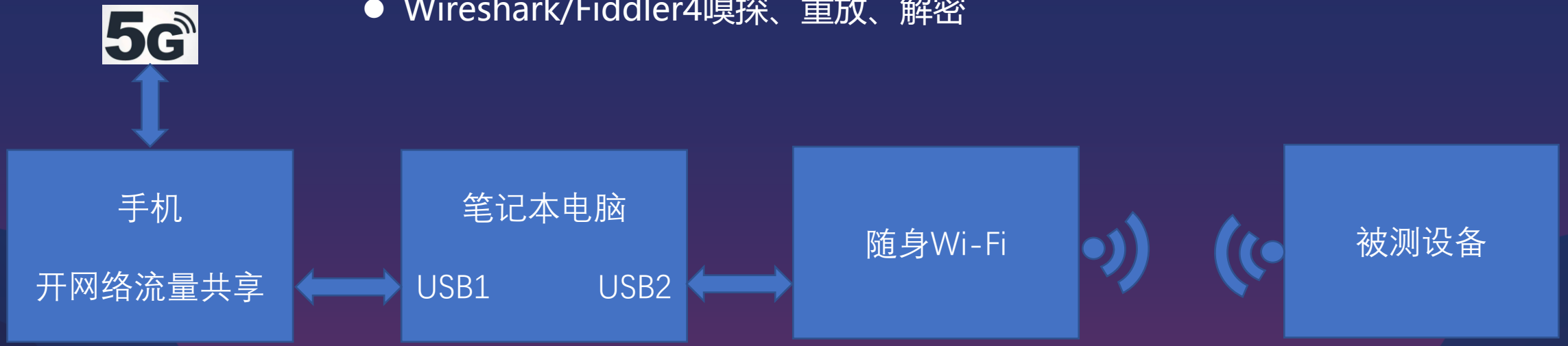
- 软硬件开源(www.fischl.de/usbtin)
- CAN协议探测(USBtinViewer)
- Fuzz工具:CanToolz



Wi-Fi快速抓包环境搭建

受控的可抓包热点，用于各种智能设备测试

- 硬件: 随身Wi-Fi
- 笔记本电脑+手机USB口共享流量
- Wireshark/Fiddler4嗅探、重放、解密



HarkRF One with Portapack H2(SDR)

用于智能设备无线测试

- 无线流量的频段嗅探
- 无线流量的抓取和重放
- GPS的模拟
- 软件: Universal Radio Hacker(URH)

目 录

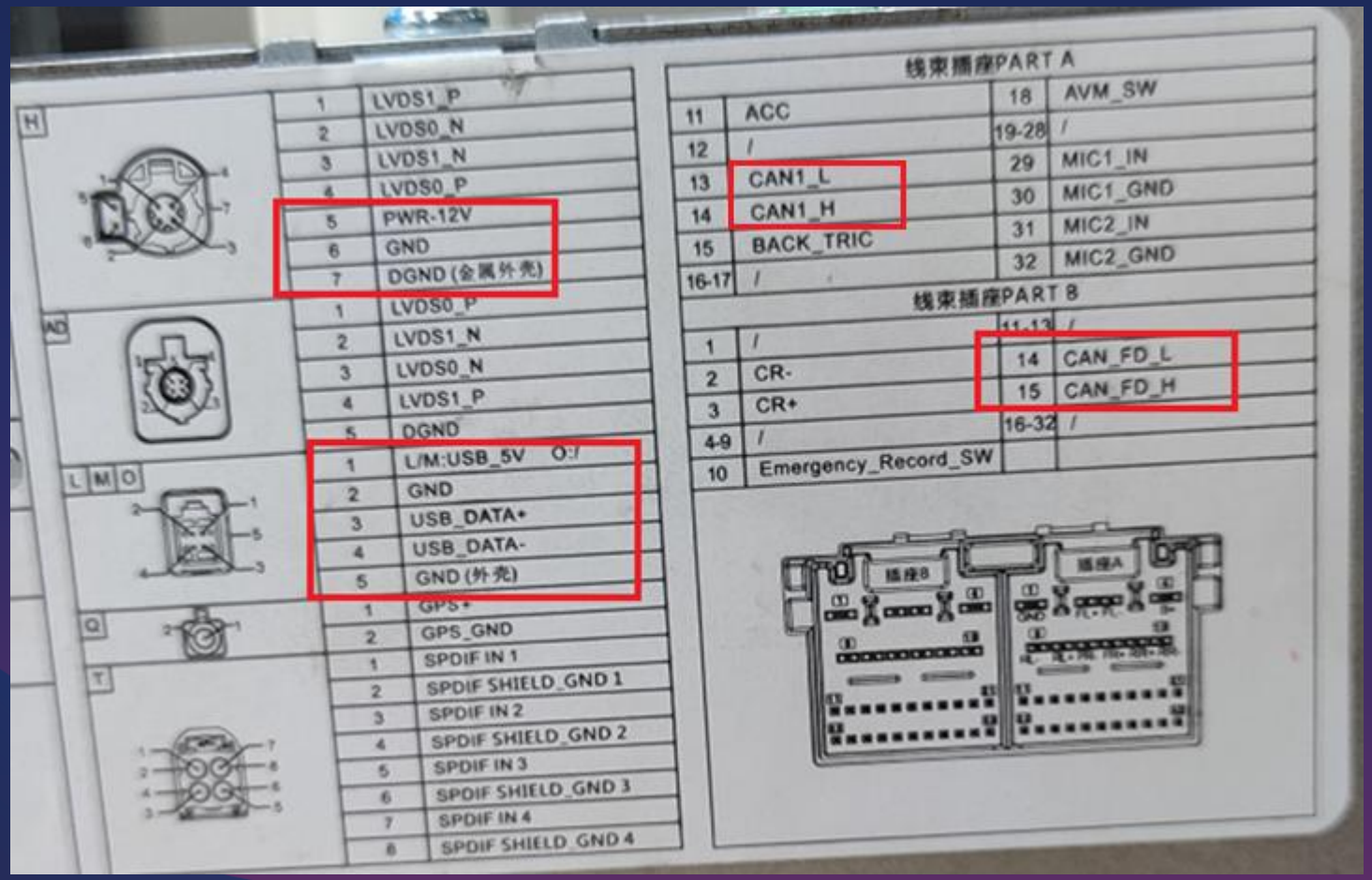
工程模式与固件提取：内容摘要

- 经费预算少，研究车联网，去哪里买车联网部件?
- 如何确定未知电路板的电源引脚、CAN引脚、以太网引脚?
- 车厂是怎么开发、调试和维护的汽车系统的?
- 安全研究员一般怎么进入系统内部?
- 怎么搞到对应车型的固件升级包?
- 进入工程模式有密码，怎么办?
- 固件有哪些常见的风险点?

找研究目标

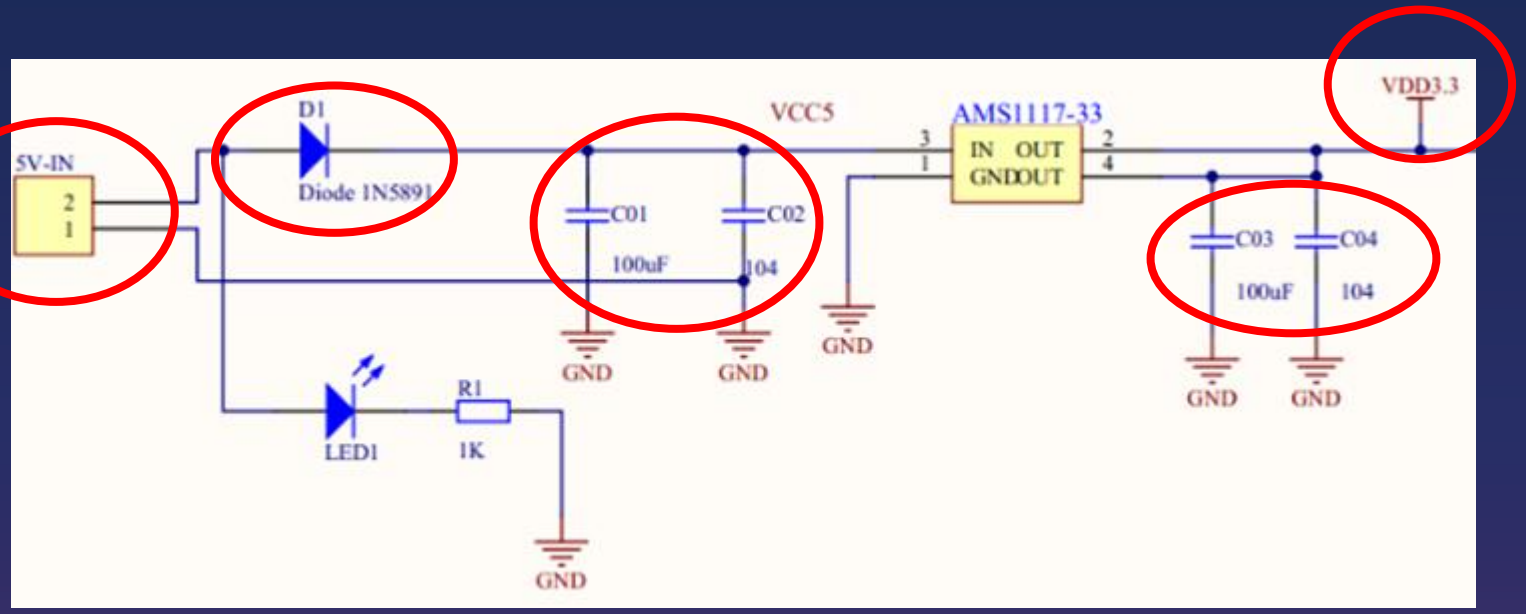
- 买整车
- 租车
- 广州陈田村一日游
- **咸鱼**
- **后装/改装市场**
- 4S店
- 报废车、事故车渠道

某车 IVI 接口定义



- 电源
- USB
- CAN

智能设备的电源原理图



- 输入是5V电源
- D1作用是防止电源反接。
- C01、C02是电源输入滤波电容；
- C03、C04是输出滤波电容。
- VDD3.3是3.3V电源

没官方资料，找电源引脚的办法

- 电源电压一般是12V，也可向卖家确认
- 万用表先找到“地” --- GND

  电路板上的“地”一般都是连在一起的

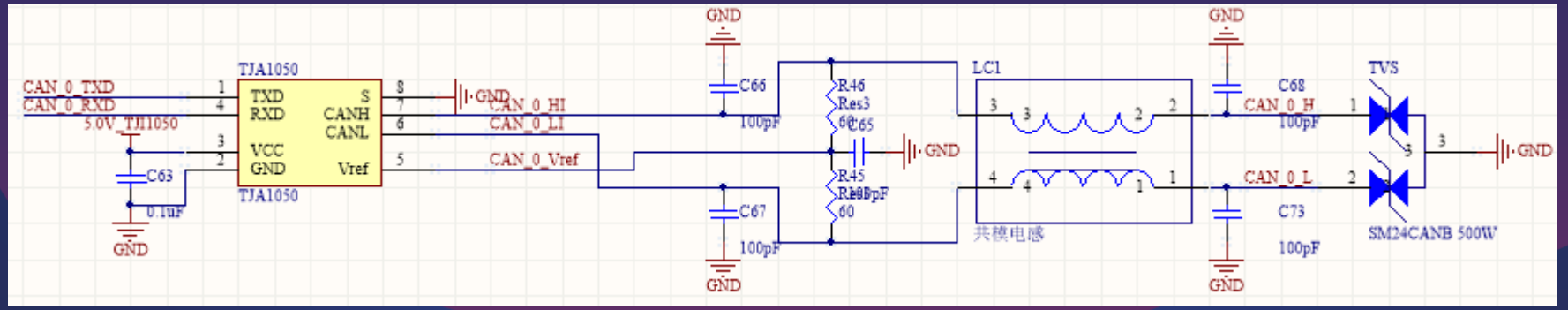
  “地”一般和大块铜皮相连

  CPU旁边的小电容一般有一端接“地”

  每个芯片都要接“地”
- 一般有大电容且集中的地方是电源电路
- **“地”和VCC一般走线比较粗**
- VCC可能经过一个大的二极管（防接反）
- VCC经过稳压等芯片转换成其它电压(可查手册确认)
- 金属外壳的接插件一般外壳焊在板子上的一般都是GND

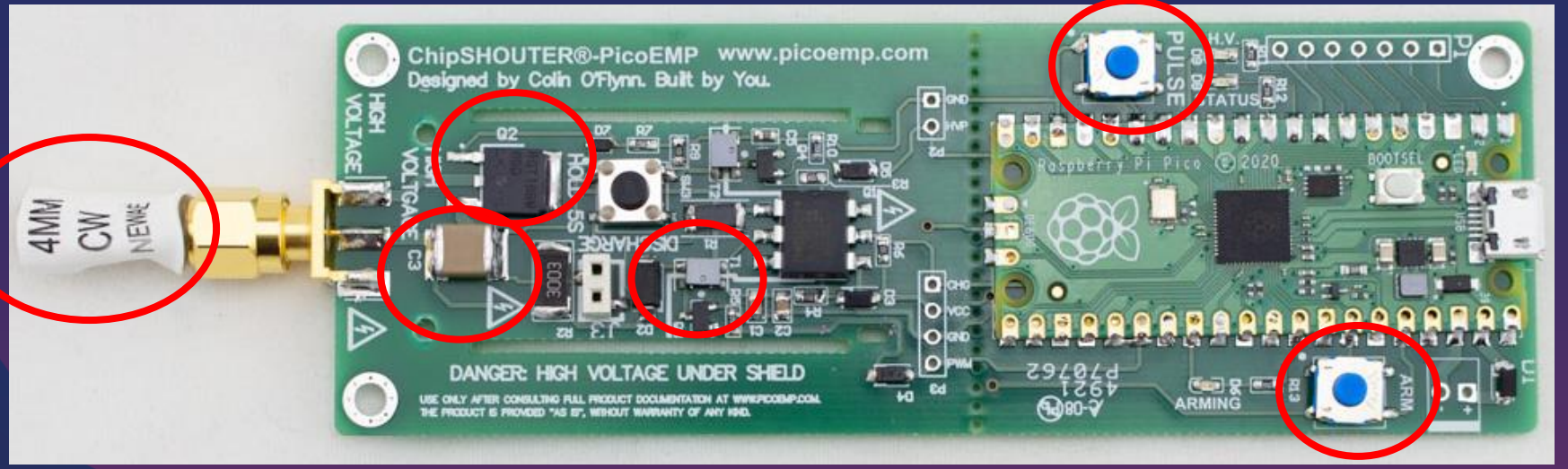
没官方资料，找电路通信引脚的办法

- CAN管脚一般通过电感和CAN控制芯片连接
- 以太网引脚一般和以太网PHY芯片连接
- 查找对应芯片的手册，知道芯片功能
- 如果看不清芯片型号，可以用手机微距镜头拍摄
- 如果手机没有微距镜头，可以买外置微距镜头
- 观察芯片标识: 也可买专门的电子显微镜



固件提取中，破解芯片保护或绕过登陆的方法

- 《智能设备漏洞挖掘中的几个突破点》，发现大家感兴趣的是固件提取方法
- 电压故障注入:《敲开芯片内存保护的最后一扇门》付鹏飞
- 电磁故障注入：PicoEMP(github.com/newaetech/chipshouter-picoemp)



电磁故障注入场景

汽车工程模式

汽车内置的一种模式。用在开发、生产测试、维护等场合。进入可能要密码，功能如下:

- 可以开调试模式（例如：打开安卓系统的ADB shell)
- 导出一些内部日志(一般导出到U盘)
- 查看和修改汽车的一些参数配置
- 汽车仪表的自我诊断
- 进行本地升级操作

以下是某款车工程模式菜单:

另一款汽车的工程模式

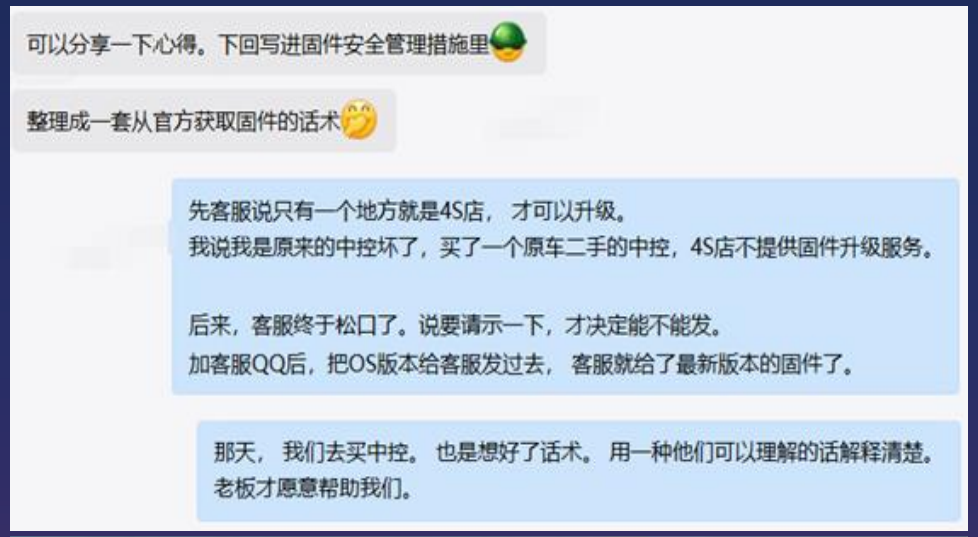
工程模式本身不是漏洞，是我们进入汽车内部继续研究的一个途径。

如何进入汽车工程模式

获取当前研究车型的工程模式，有很多种方法，例如:

- 厂家官网文档(一般较少提及)
- 尝试 在安卓：系统->版本信息 多次点击版本号
- 如果工程模式有密码, 逆向固件获取密码
- 搜索引擎查找工程模式和进入密码
- 淘宝/咸鱼搜索车型对应固件
- 找厂家客服，社工获取
- 找上游的系统软件开发商客服，社工
- 4S店获取

社工客服拿到汽车升级包和工程模式进入方法



通过逆向汽车升级包发现工程模式密码

```
/* access modifiers changed from: private */
public TextView yb;
private boolean yc;
private final a yd = new a(this, (byte) 0);

/* access modifiers changed from: private */
public /* synthetic */ void m(View view) {
    if (this.xY.getText().toString().trim().equals("*#18[redacted]")) {
        dismiss();
    } else {
        this.yb.setVisibility(0);
        this.yd.sendEmptyMessageDelayed(0, 1500);
    }
    this.yc = true;
}
```

```
code:ERROR.NO_ERROR,msg:a}))},function(b){log.D(d,
in zxqaccount =  "+Util.inspect(a));var c=a.expiryTime,f=(
yTimeStamp= "+Util.inspect(f)),log.D(d,
kZxqToken#Local Login zxqToken Expired !"),e({errorcode:ER
)}var c=new HttpsAgent,d=global.TAG;this.zxqLogin=functio
(function(g,h){var i={token:global.token.getActiveToken(),
if("17000000009"===a&&"72hs[redacted]===b){var j=new ZXQAccou
0000009",is_owner:0,user_id:0xe8d4a51002,args:{account_typ
ype:"tb",mobile:"",user_id:"1",user_name:"test",login_stat
urn g(a)})}if("17000000008"===a&&"72hsh7[redacted]===b){var k
ser_name:"17000000008",is_owner:0,user_id:0xe8d4a51003,arg
i_accounts:[{type:"tb",mobile:"",user_id:"1",user_name:"tes
nction(a){return g(a)})}c.post("/user/1.0/login",i).then(
)),b.err_resp)return f={errorcode:ErrorConvertor.getError(
```

进入原生安卓模式

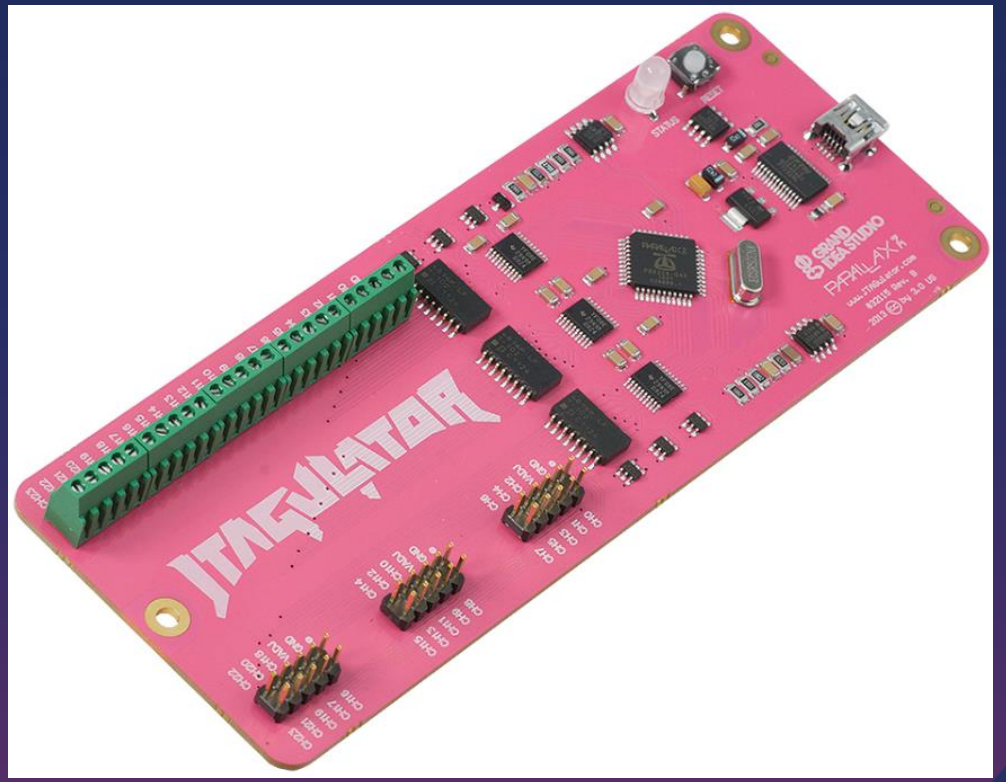
极少汽车还可进入原生安卓模式，看到更多的系统内容，例如:

- 有时会有内部测试软件，正式界面中未启用
- 权限比较高，更方便调试。
- **找可以控制车运动状态的应用软件，分析和提取通讯协议**
- 容易找到危及行驶安全的风险点
- 也可安装抓包和安全测试软件

硬件调试接口的寻找

进入工程模式以后，调试接口一般有以下几种:

- 电路板上的调试串口
- USB专用调试口
- 插U盘的USB口，其处于从模式(SLAVE)
- TF卡可能导出调试日志或其它信息
- Wi-Fi/网口尝试连adb服务
- 硬件串口和JTAG口探测工具JTAGulator



常用的adb 命令

IVI和ADAS进后，一般是安卓系统，以下是常用adb命令:

- adb devices
- adb connect ip:5555
- adb shell (或adb -s 123456789ABCDEF shell)
- adb logcat
- adb install Root.apk # 安装应用
- adb pull /data/local/temp/test.pcap d:\ # 复制 安卓文件 到 电脑
- adb push “C:\Users\ml\Root.apk” /mnt/sdcard/ # 复制 电脑文件 到 安卓

启动网络adb调试

打开网络调试

- # setprop service.adb.tcp.port 5555
- # stop adbd
- # start adbd

关闭网络调试

- #stop adbd
- #setprop service.adb.tcp.port -1
- #start adbd

```
$ adb root
adbd is already running as root

$ adb remount rw,remount/
remount succeeded

$ adb remount -o rw,remount /
remount succeeded

$ adb push logservice.sh /bin/
logservice.sh: 1 file pushed, 0 skipped 0.1 MB/s(2265 bytes in 0.031s)

$ adb reboot

$ adb connect 192.168.1.105:5555
already connected to 192.168.1.105:5555

$ adb shell
car:/ $
```

固件提取

IVI和ADAS进去以后，一般是安卓系统，以下是常用固件提取命令:

- ps –aux
- netstat -atnp
- df -h

第一种方法提取固件

- dd if=/dev/mtd0 of=/tmp/SD0/mtd0.bin

第二种方法提取固件(有遗漏或文件系统不好解压缩)。

- tar -cvpf /mnt/SD0/root.tar / --exclude="sys" --exclude="proc" --exclude="tmp"

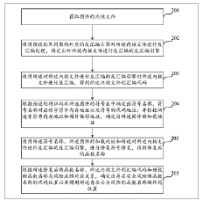
固件的文件拆解与符号表恢复

- 固件中一些文件系统的拆解：熟悉常见嵌入式文件系统；编程解决问题
- 几种高效恢复固件符号表的方法

一种固件安全分析的方法及装置 在申—实审

Firmware security analysis method and device

申请号：202010732659.1 申请日：2020-07-27



CN202010732659
CN111881455A

微信扫码查看/分享专利

摘要：本发明提供了一种固件安全分析的方法及装置，该方法包括获取固件的内核文件，使用预设的不同架构对应的反汇编引擎对所述内核文件进行反汇编处理，确定出反汇编引擎，得到内核文件的汇编代码，根据预设的特征码从固件的符号表中确定出符号名称、字符串内存地址以及代码地址，确定出固件的加载地址，进行符号修复，得到修复后的函数名称，确定出存在安全风险的函数名称的代码位置以及调用函数名称的代码位置。通过对固件进行反汇编的方式得到固件的汇编代码，进而再依据预设的函数名称与风险点的对应关系，可以快速的确定出固件的汇编代码中存在安全风险的函数名称的位置，从而实现了在无需测试设备的情况下，快速的识别测试设备的安全风险点。

Abstract: The invention provides a firmware security analysis method and device, and the method comprises the steps: obtaining a kernel file of firmware, carrying out disassembly of the kernel file through preset disassembly engines corresponding to different architectures, determining a disassembly engine, and obtaining an assembly code of the kernel file, and determining a symbol name, a character stringmemory address and a code address from a symbol table of the firmware according to a preset feature code, determining a loading address of the firmware, performing symbol repair to obtain a repaired function name, and determining a code position of the function name with a security risk and a code position of a calling function name. According to the method, the firmware assembly code is obtainedby disassembling the firmware, and the position of the function name with the security risk in the firmware assembly code can be quickly determined according to a corresponding relationship between the preset function name and the risk point, so that the security risk of the firmware assembly code can be quickly determined without test equipment, and the security risk point of the test equipment can be identified rapidly.

申请人： 绿盟科技集团股份有限公司 北京神州绿盟科技有限公司

Applicant: NSFOCUS TECH GROUP CO LTD; NSFOCUS INFORMATION TECH CO

地址： 100089 北京市海淀区北洼路4号益泰大厦三层

发明(设计)人： 陈杰 马良 高剑 李东宏 田泽夏 潘雨晨 史龙安

Inventor: CHEN JIE; MA LIANG; GAO JIAN; LI DONGHONG; TIAN ZEXIA; PAN YUCHEN; SHI LONG'AN

一种基于字符串签名的函数识别方法

专利申请审查表

■ 文档编号		■ 密级	商业秘密
■ 版本编号		■ 日期	2022-7-6
■ 适用性声明	本模板用于专利申请中技术方案的撰写，是内部评审依据和专利代理机构的撰写依据。		

一、 基本信息

发明名称	一种基于字符串签名的函数识别方法
发明人	魏凡
部门、组	格物实验室
应用产品 、 适用领域	物联网设备固件中二进制文件的自动化函数识别

《一种高效识别VxWorks库函数的方法》（撰写中）

固件风险点

进入系统后台，一般会查看系统风险点，例如：

- 运行了哪些进程
- 开启了哪些端口
- 有没有厂家开发人员留下的调试手段/后门
- 和哪些云端的主机通讯
- 应用商店使用抓包
- App使用抓包
- 远程控制App抓包、尝试了解业务
- 模块与模块之间的通讯协议逆向

目 录

采用不安全的通讯协议

危害：

- 如果协议没有加密保护，在传输过程中容易被篡改
- 通过简单的抓包，就可获取登录用户名和密码

案例：

- 中间人攻击：本来安装一个应用商店的软件，结果安装了替换后的软件
- 抓包发现某应用商店用了FTP协议。抓包获取用户名和密码，进入App商店云端可增删改应用商店的所有apk包

采用不安全的通讯协议(续)

- 抓取协议和逆向App
- 找到可修改行车状态的指令，搞清了汽车内部的通信协议。
- 发送指令，可以实时修改汽车运行状态，从而影响行车安全

密钥保存不当

下面的密钥保存方案是不安全的：虽然采用了一些加密手段。

- 固件中保存云端密钥等登录凭据
- App中保存云端密钥等登录凭据

案例：

- 某系统内部配置文件加密。逆向其so文件后，找到了加密的密钥和算法
  解密后，发现很多系统内部的密钥和口令，甚至可以登录到云端
- 某安卓App，密钥保存不当，导致可进入云端，看到用户上传的身份证等隐私内容

总结

对厂商来说，要综合考虑的东西很多，修复周期长，任重而道远

- 软件供应商团队可能已经解散, 或不再维护
- 车型较老，漏洞可能不准备修复
- 遗留问题多，牵一发而动全身
- 有的漏洞无法远程修复

- 由于时间有限，本次只是讲了几个常见的案例。但引发的后果挺严重

谢 谢