OWASP 中国 Open Worldwide Application Security Project

OWASP 中国 | 北京分会 Open Worldwide Application Security Project

网安加社区

探真科技 TensorSecurity

开源网安 SECZONE GROUP

BrainAu 脑动极光 BRAINAU

智能网联汽车网络安全

张海春

2024 OWASP中国安全技术论坛

全球视野下的网络安全趋势

汽车智能化带来巨大网络安全风险

2015年7月

切诺基召回 140 万辆轿车和卡车

黑客从任何接入互联网的地方，远程获取汽车的关键功能操作权限并令所有电子设备宕机。

Jeep

2016年6月

利用 WI-FI 控制三菱欧蓝德

研究人员可以发送的消息关掉汽车的报警器、打开或关闭车灯、控制空调等。

MITSUBISHI MOTORS

2019年10月

奔驰APP在美爆安全漏洞

解锁和启动汽车的应用程序（APP）错误地显示了其他车主的个人隐私信息。

2021年4月

机器学习对抗性攻击 ADAS

黑客通过无人机远程利用零点击漏洞，成功入侵特斯拉信息娱乐系统，还打开了车门和后备箱。

TESLA

2023年

丰田-黑客通过can干扰窃取汽车

三一重工 TBOX MQTT身份验证不足,可篡改车队控制数据和状态数据

蔚来车机存在错误配置和目录遍历漏洞

日产汽车在澳大利亚和新西兰遭遇网络攻击

.....

2015年12月

VOLVO BYD

沃尔沃、比亚迪门锁遥控滚码机制被绕过

遥控滚码机制能够被绕过，用几十元的破解密匙就能无限次打开车门、后备箱。

2017年5月

宝马 330I 2011款格式化字符串 DOS 漏洞

宝马 330i 的蓝牙漏洞会导致多媒体软件崩溃。

2020年2月

TESLA

特斯拉 MODEL X 蓝牙钥匙漏洞

黑客可以通过蓝牙连接重写密钥卡的固件，从密钥卡上解锁代码，然后利用它来偷走 Model X

2022年12月

HONDA The Power of Dreams NISSAN

美国SiriusXM车联网服务漏洞

该漏洞允许黑客远程攻击多家制造商的车辆，包括本田、日产等。只要知道车辆的车辆识别码就可以未经授权解锁、启动、定位和鸣喇叭。

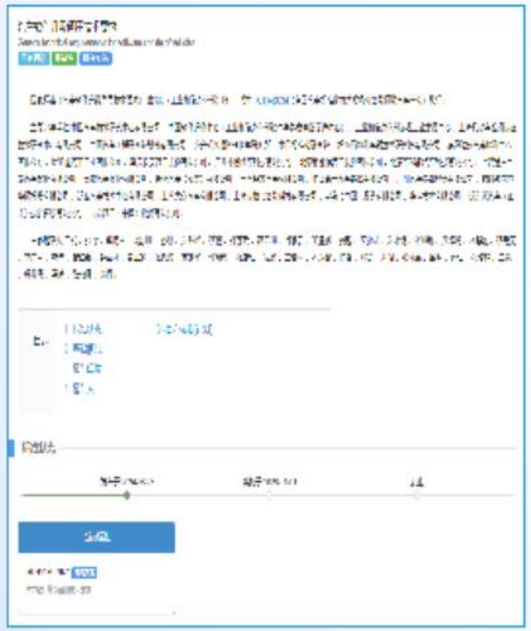
2024-

随着智能网联车辆的普及，未来会有更多潜在风险.....

智能网联汽车+网络安全成为行位风向标

据公安部 2024 年 1 月统计，我国汽车保有量已达 **3.36 亿辆**，全国有 **94** 座城市汽车保有量超过 **100 万辆**。

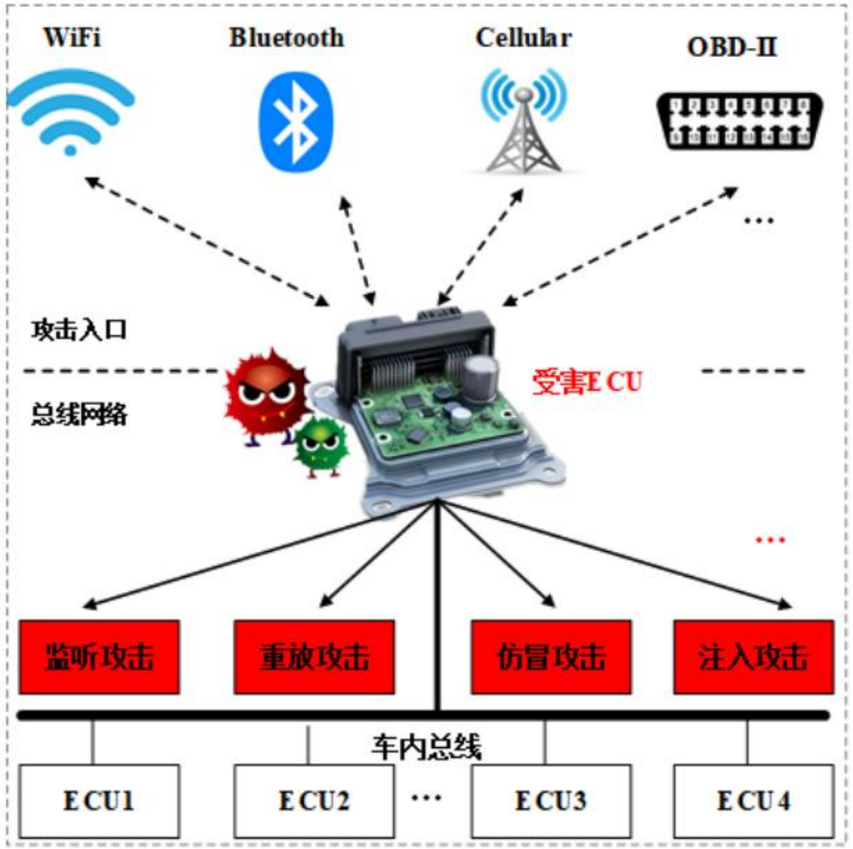
2023 年我国搭载组合驾驶辅助系统的智能网联乘用车新车销售约 **950 万辆**，市场渗透率达 **34.9%**，2023 年上半年市场渗透率提升至**42.4%**，智能网联汽车产业已步入高速发展阶段。

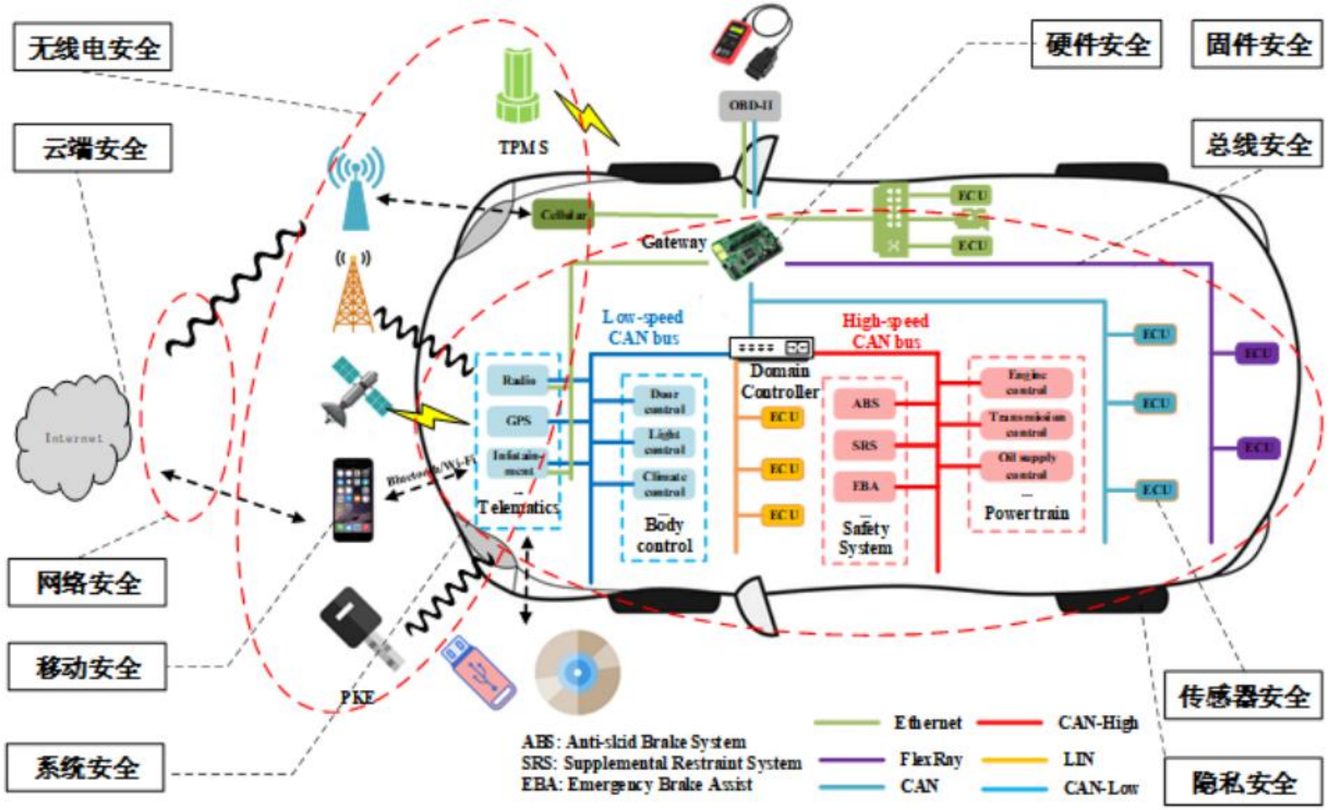


三项强标已落地，助力行业发展

车联网安全直接关系着**人身安全、交通安全、公共安全**乃至**国家安全**

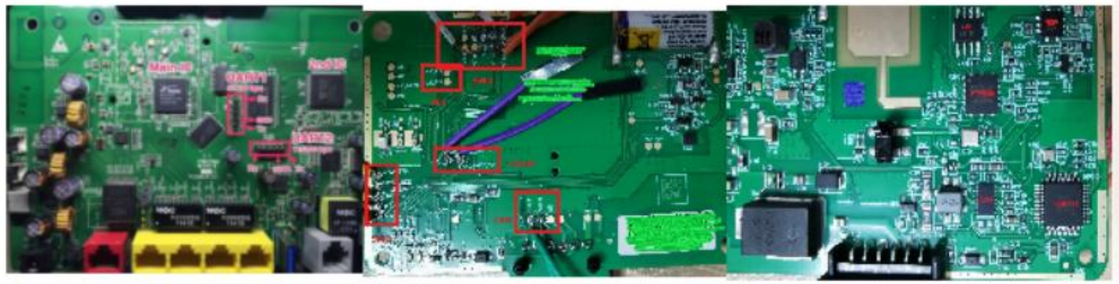
智能网联汽车网络安全全景图





■ 依据从车内到车外、底层到上层、硬件到软件的原则，智能网联汽车攻击模型中的网络安全威胁可分为硬件、固件、总线、系统、无线电、网络、云端、移动、传感器、隐私十个层次。

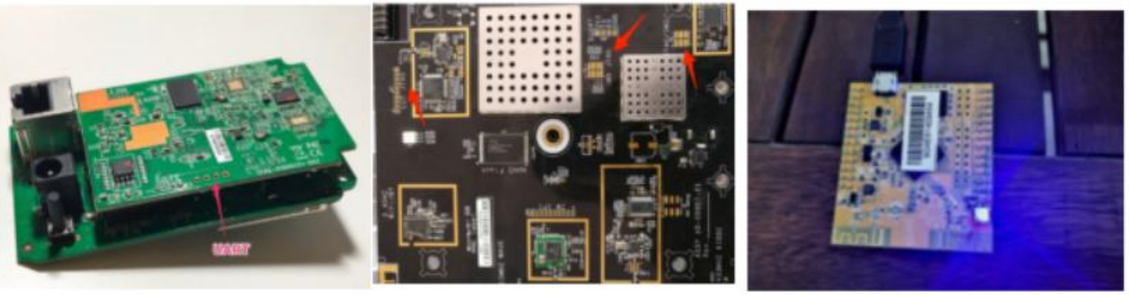
硬件安全



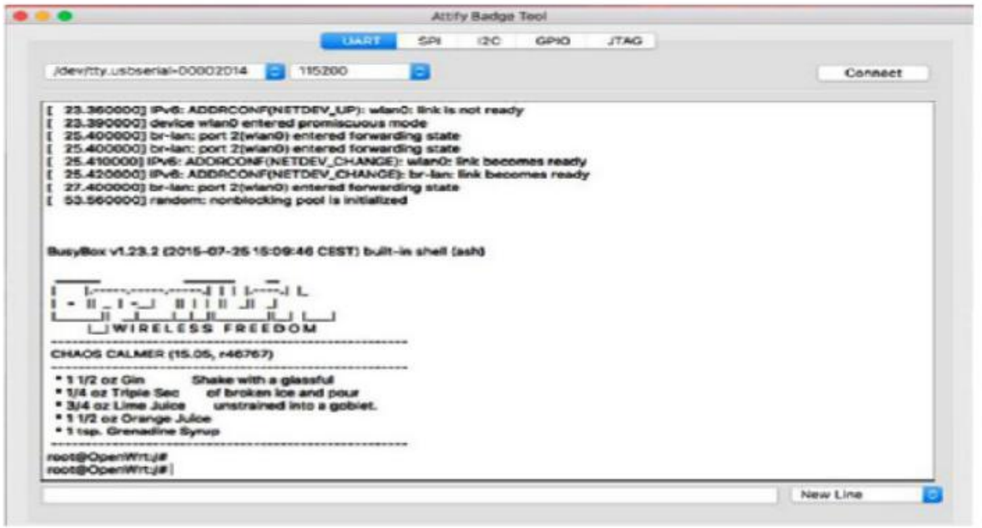
PCB泄露接口信息 PCB泄露协议信息 PCB泄露芯片信息

```
Find Port=0 Device:Vender ID=817910ec
vendor_deivce_id=817910ec
======>>EXIT rtl8192cd_init_one <<======
======>>INSIDE rtl8192cd_init_one <<======
======>>EXIT rtl8192cd_init_one <<======



Probing RTL8186 10/100 NIC-kenel stack size order[2]...

Booting...

********************************************************************************
*
* chip_no chip_id mfr_id dev_id cap_id size_sft dev_size chipSize
* 0000000h 0c22017h 00000c2h 0000020h 0000017h 0000000h 0000017h 0800000h
* blk_size blk_cnt sec_size sec_cnt pageSize page_cnt chip_clk chipName
* 0010000h 0000080h 0001000h 0000800h 0000100h 0000010h 000002dh MX25L6405D
*
********************************************************************************
```

调试接口泄露启动信息



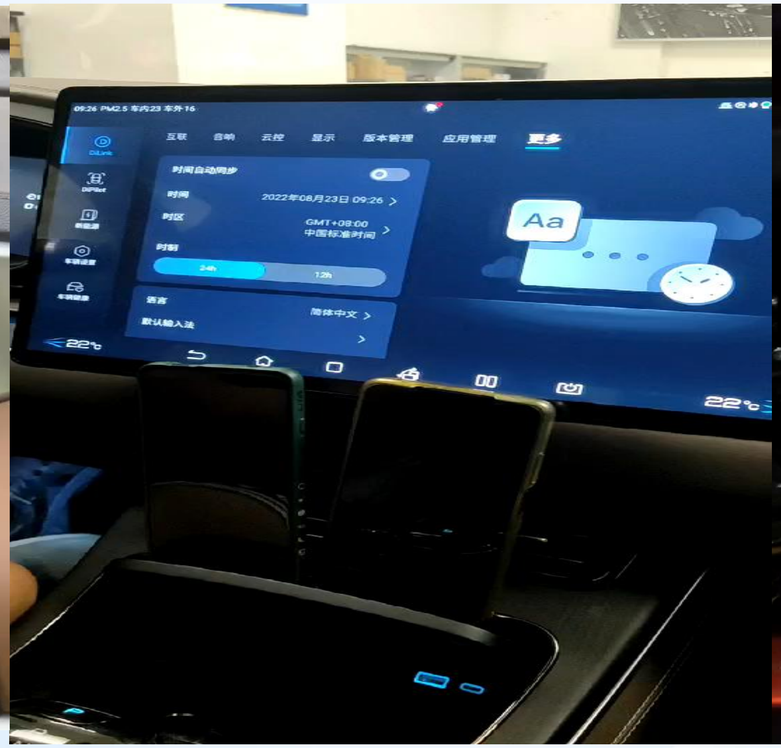
UART调试接口 JTAG调试接口



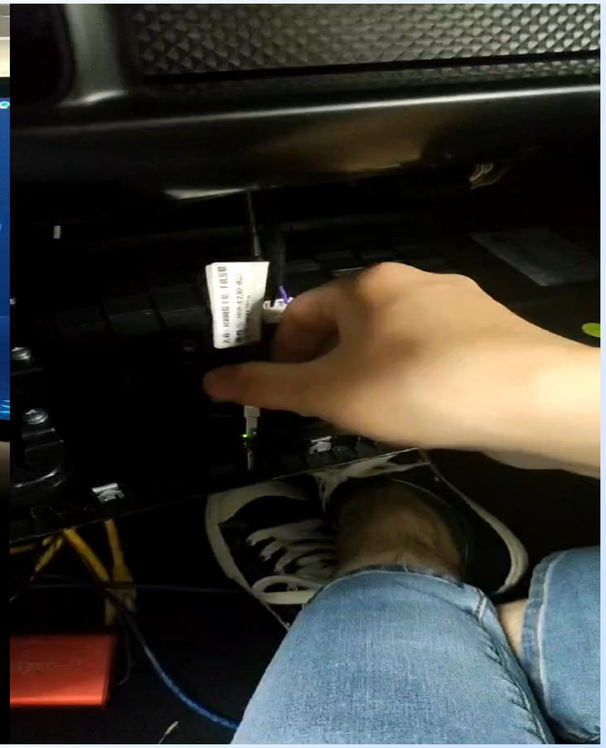
调试接口泄露系统shell

硬件安全

USB车机控制



USB拨号



USB口令爆破

固件安全

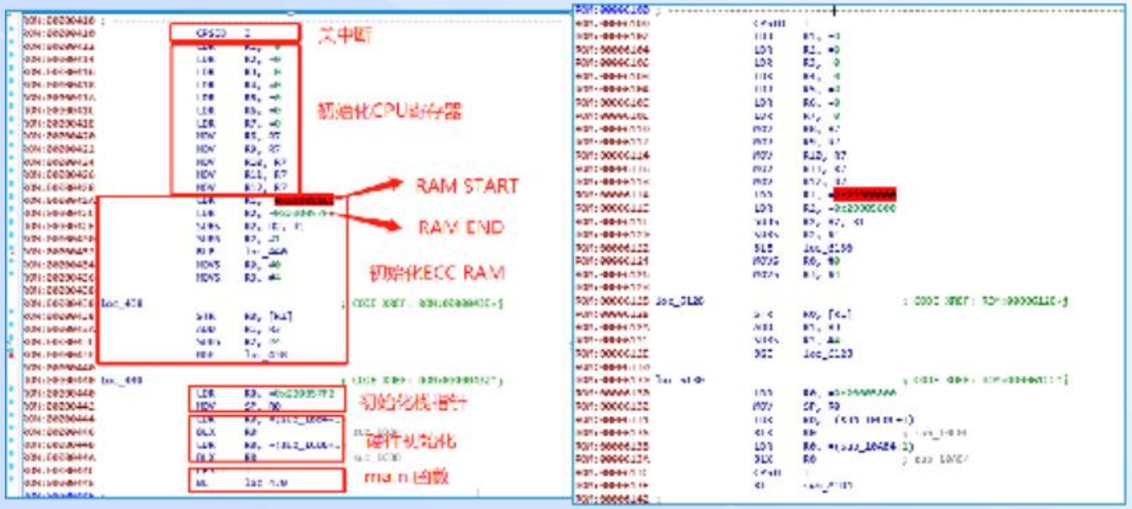
固件泄露

```
oit@ubuntu [01:04:59 AM] [~/lab/firmware]
-> % ~/tools/firmware-mod-kit/unsquashfs_all.sh Dlink_fs
Attempting to extract SquashFS 3.X file system...

Skipping squashfs-2.1-r2 (wrong version)...

Trying ./src/squashfs-3.0/unsquashfs-lzma...
Trying ./src/squashfs-3.0/unsquashfs...
Trying ./src/squashfs-3.0-lzma-damn-small-variant/unsquashfs-lzma... Skipping others/squashfs-2.0-nl
Skipping others/squashfs-2.2-r2-7z (wrong version)...

Trying ./src/others/squashfs-3.0-e2100/unsquashfs-lzma...
Trying ./src/others/squashfs-3.0-e2100/unsquashfs...
Trying ./src/others/squashfs-3.2-r2/unsquashfs...
Trying ./src/others/squashfs-3.2-r2-lzma/squashfs3.2-r2/squashfs-tools/unsquashfs...
created 879 files
created 64 directories
created 111 symlinks
created 0 devices
created 0 fifos
File system sucessfully extracted!
MKFS="./src/others/squashfs-3.2-r2-lzma/squashfs3.2-r2/squashfs-tools/mksquashfs"
oit@ubuntu [01:05:10 AM] [~/lab/firmware]
-> % ls squashfs-root
bin  dev  etc  home  htdocs  lib  mnt  proc  sbin  sys  tmp  usr  var  www
```

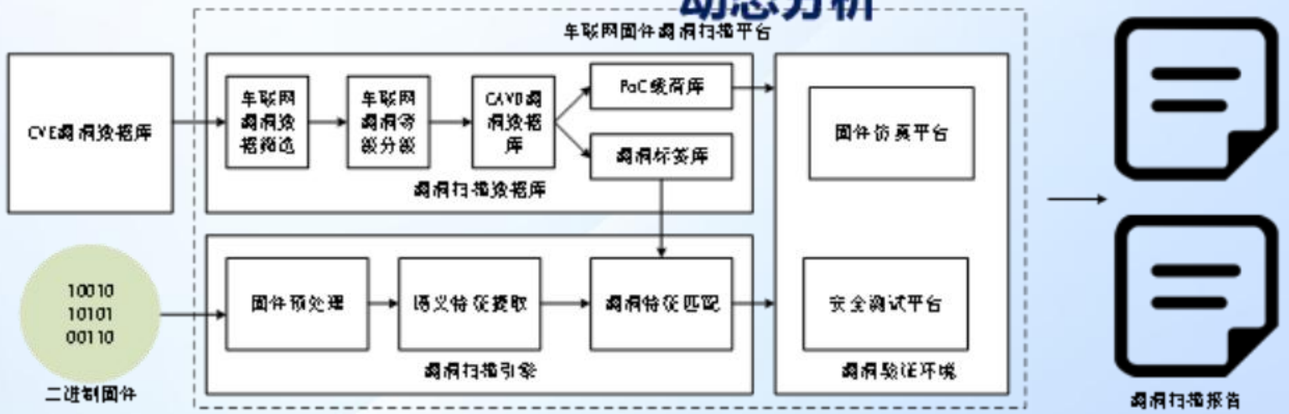
静态分析

```
~/Downloads/_dvrf.bin.extracted/squashfs-root » which qemu-mipsel-static
/usr/bin/qemu-mipsel-static
~/Downloads/_dvrf.bin.extracted/squashfs-root » sudo cp /usr/bin/qemu-mipsel-static .
~/Downloads/_dvrf.bin.extracted/squashfs-root » sudo chroot . ./qemu-mipsel-static ./bin/busybox
BusyBox v1.7.2 (2016-03-09 22:33:37 CST) multi-call binary
Copyright (C) 1998-2006  Erik Andersen, Rob Landley, and others.
Licensed under GPLv2.  See source distribution for full notice.

Usage: busybox [function] [arguments]...
   or: [function] [arguments]...

        BusyBox is a multi-call binary that combines many common Unix
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use and BusyBox
        will act like whatever it was invoked as!

Currently defined functions:
        [, [[, addgroup, adduser, arp, basename, cat, chgrp, chmod, chown, clear, cp, cut, delgroup,
        deluser, df, dirname, dmesg, du, echo, egrep, env, expr, false, fdisk, fgrep, find, free,
        fsck.minix, getty, grep, halt, head, hostid, id, ifconfig, insmod, kill, killall, klogd,
        less, ln, logger, login, logread, ls, lsmod, mkdir, mkfifo, mkfs.minix, mknod, more,
        mount, msh, mv, netstat, passwd, ping, ping6, pivot_root, poweroff, printf, ps, pwd,
        rdate, reboot, reset, rm, rmdir, rmmod, route, sh, sleep, su, sulogin, swapoff, swapon,
        sysctl, syslogd, tail, telnet, telnetd, test, top, touch, true, umount, uname, uptime,
        usleep, wget, xargs, yes
```

动态分析



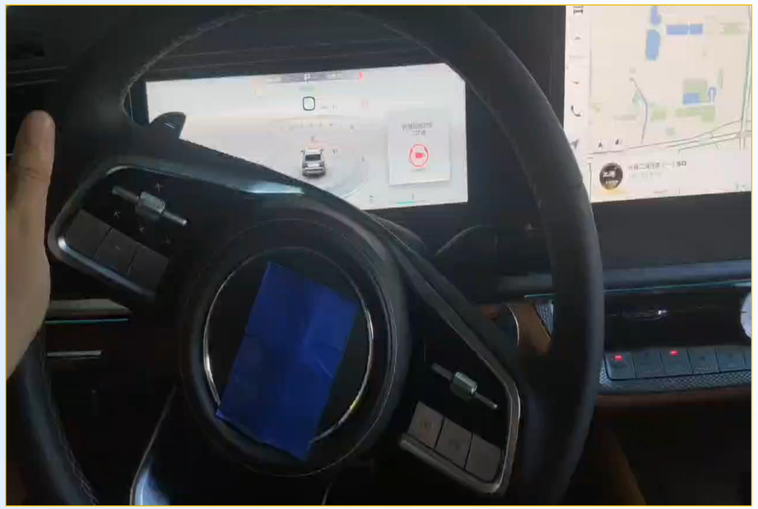
逆向分析

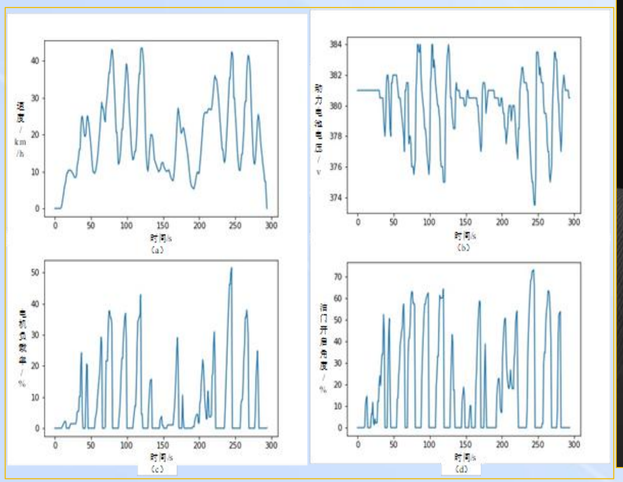


自动化分析

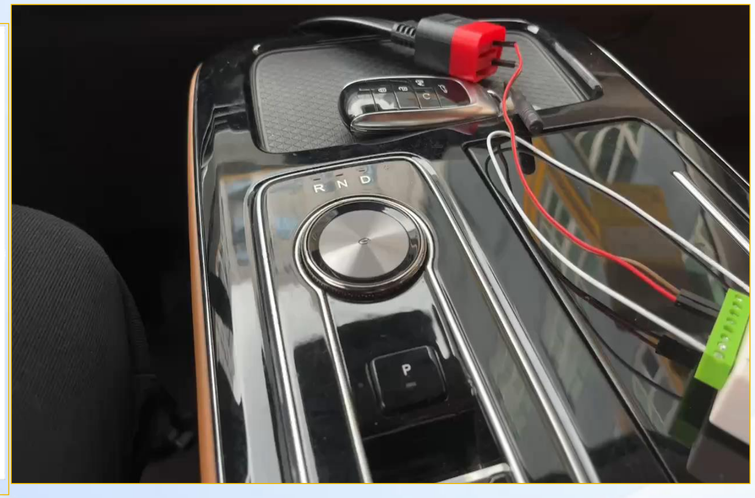
总线安全

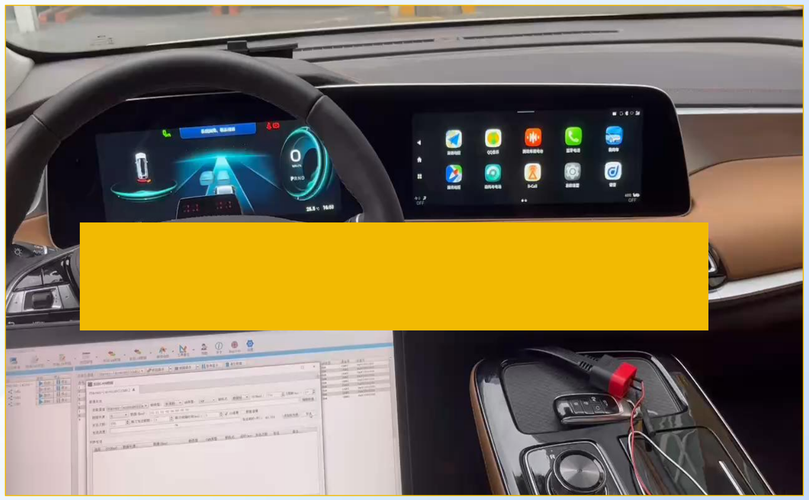
非诊断CAN总线车辆控制





诊断CAN总线数据读取





诊断CAN总线车辆控制

总线安全

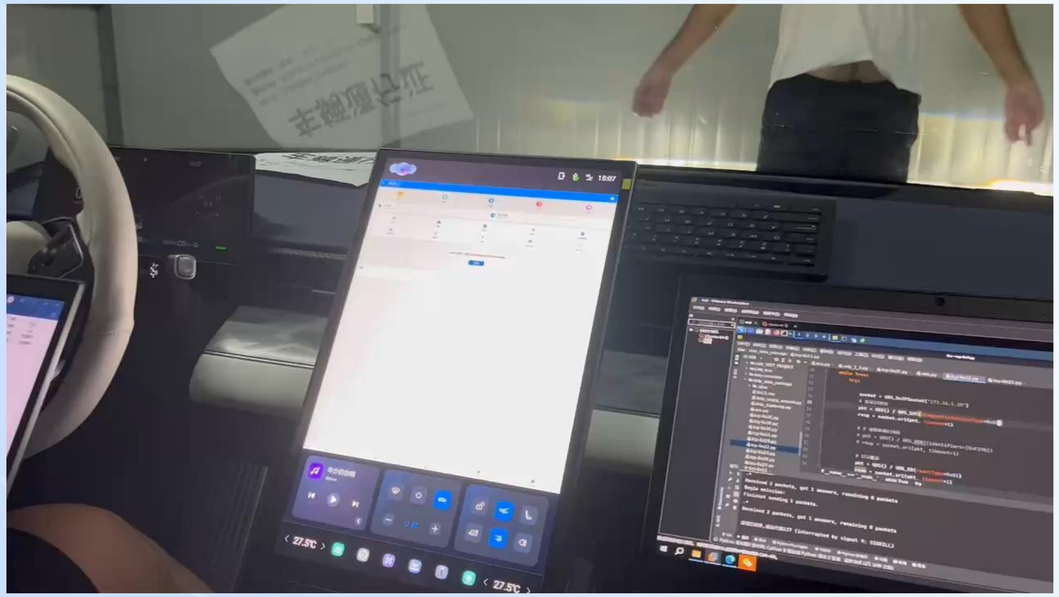

远光灯失效
掉线攻击前
掉线攻击后


左转向灯失效
掉线攻击前
掉线攻击后


左转向灯异常
右转向灯异常


远光灯异常
安全带指示灯异常

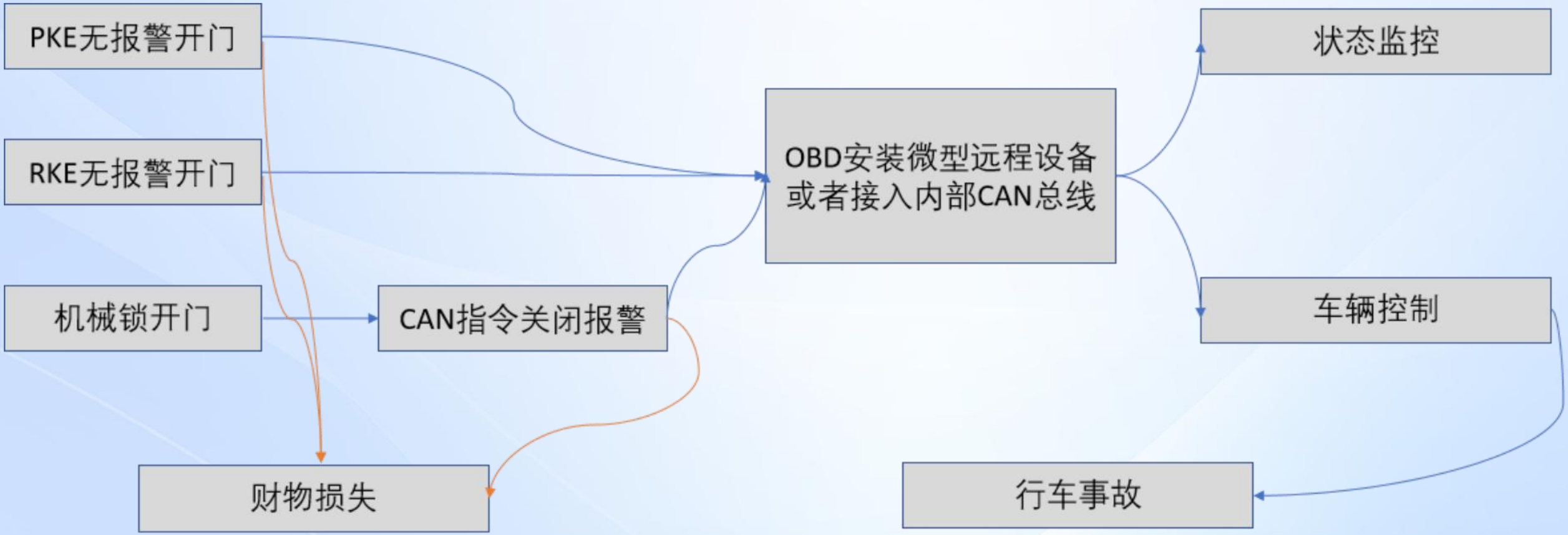
总线安全



DoIP车辆远程控制

DoIP车辆远程断网

总线安全

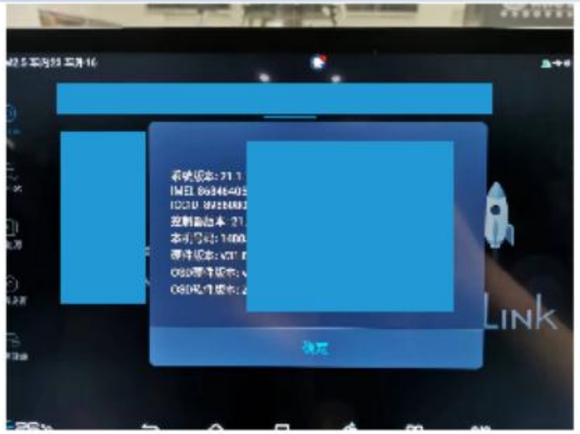


实现概率非常大的具有严重后果的攻击链条

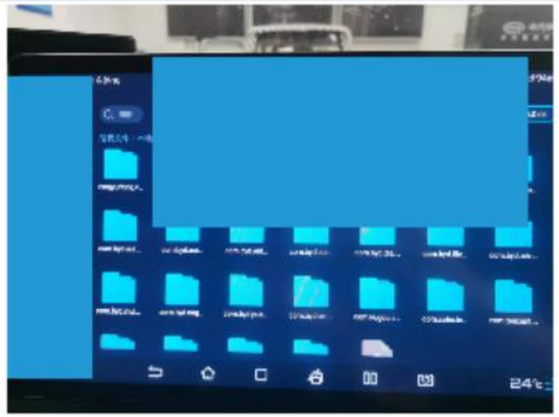
系统安全

- 启动与运行
  Startup and running
- 服务与漏洞
  Services and vulnerabilities
- 访问控制
  Access contorl
- 系统审计
  System audit
- 数据备份
  data backup
- 敏感信息
  Sensitive data
- 应用程序
  Application
- 浏览器/OTA
  Browser/OTA
- 防火墙
  firewall
- 代码及数据
  Code and data

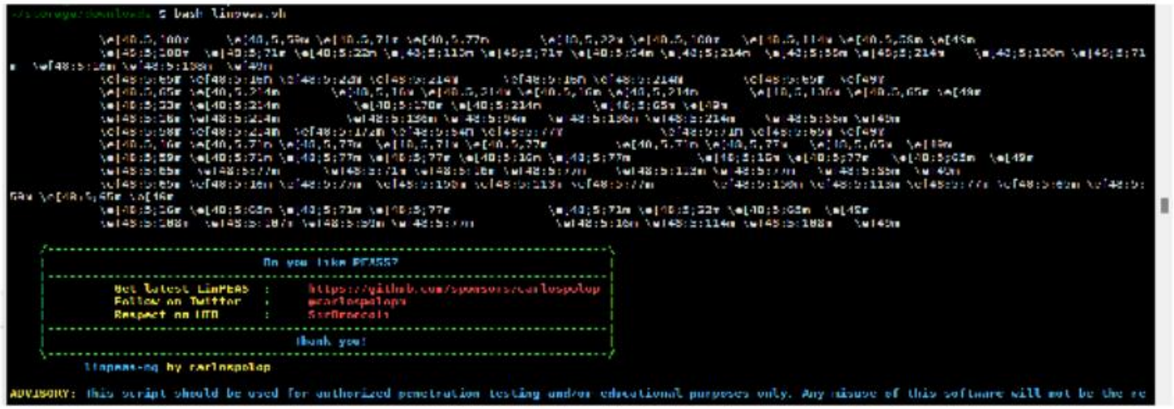
系统安全



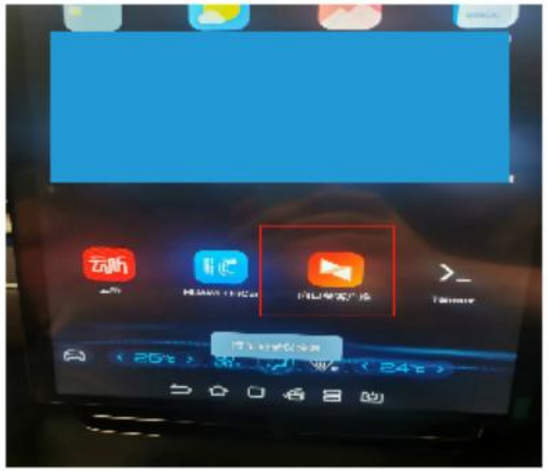
信息泄露



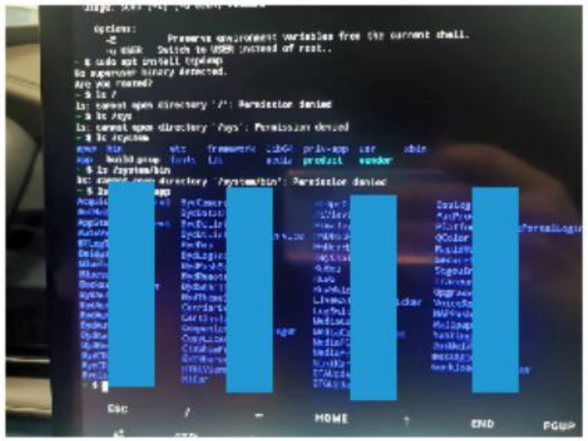
文件操作



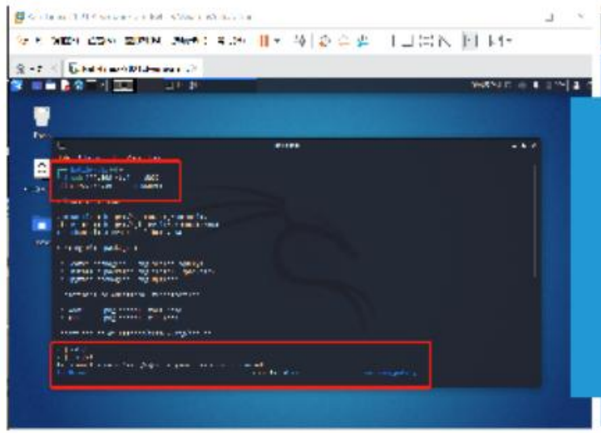
脚本文件执行



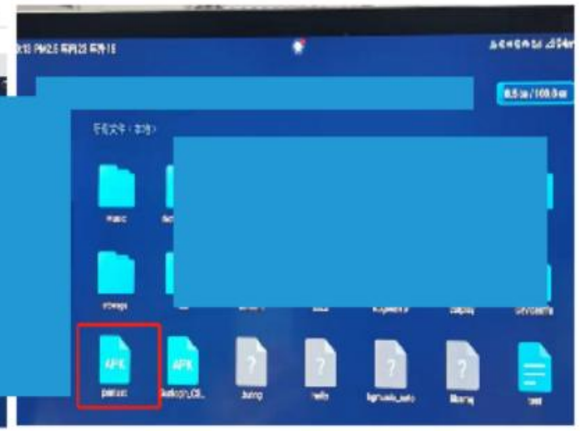
恶意APP安装



本地shell

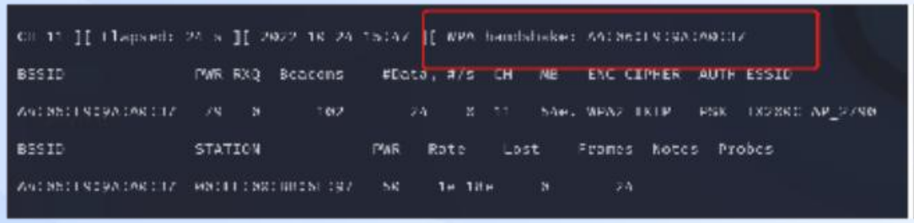


远程shell 1

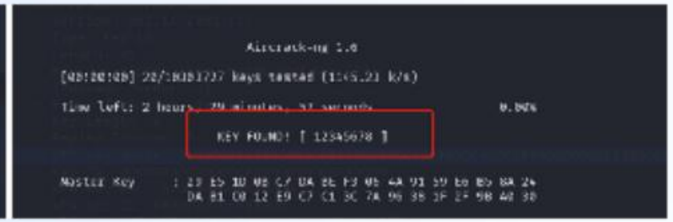


恶意文件检测

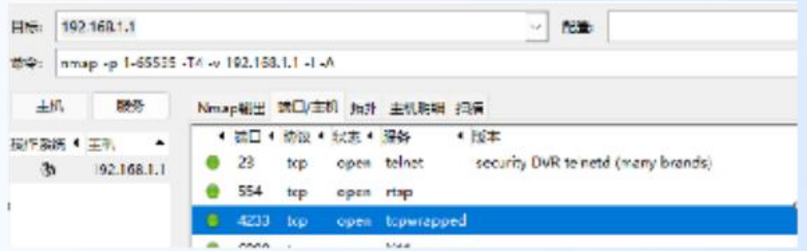
系统安全



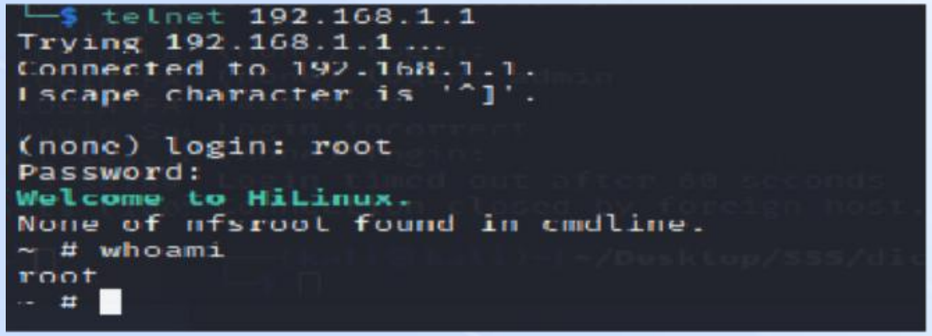
Wi-Fi握手数据



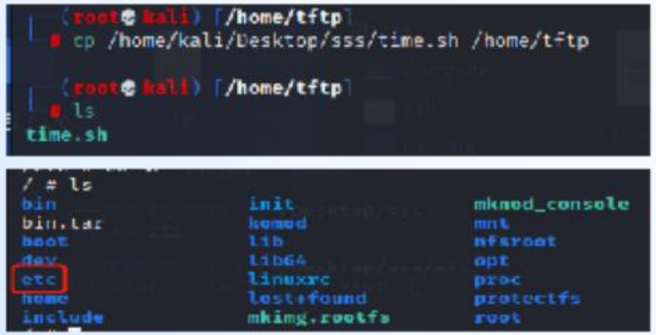
Wi-Fi口令



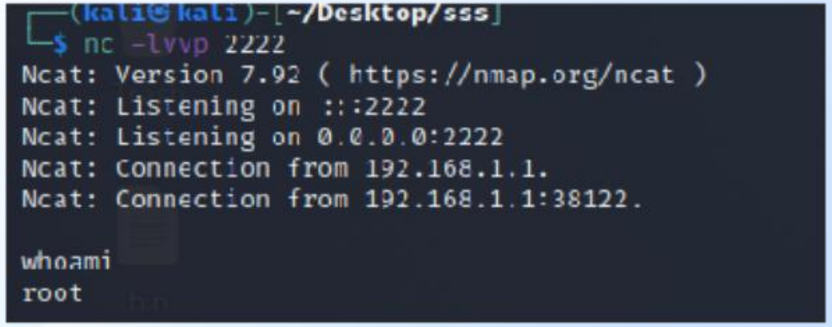
端口扫描



Root权限



文件上传下载



反弹shell

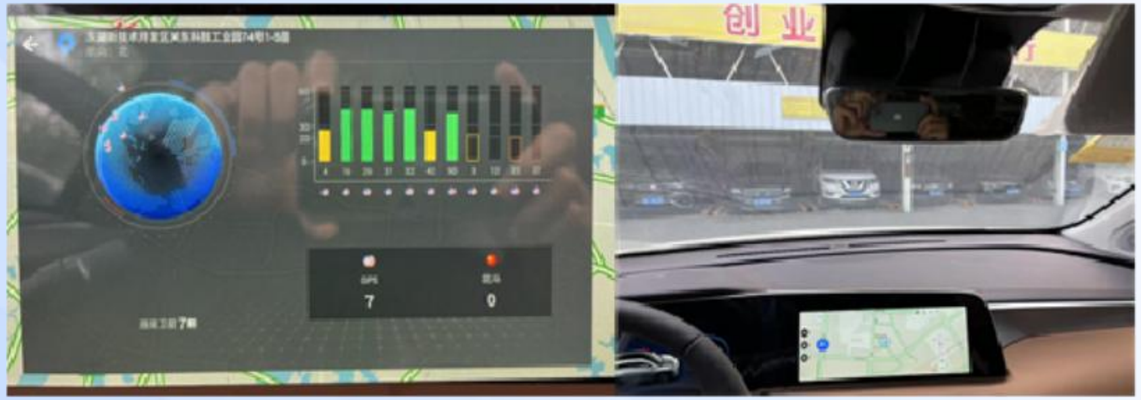
传感器安全

- 车载摄像头
Camera
- 激光雷达
Lidar
- 超声雷达
Ultrasonic radar
- 毫米波雷达
Millimeter wave radar
- GPS/北斗
GPS/Beidou
- TPMS

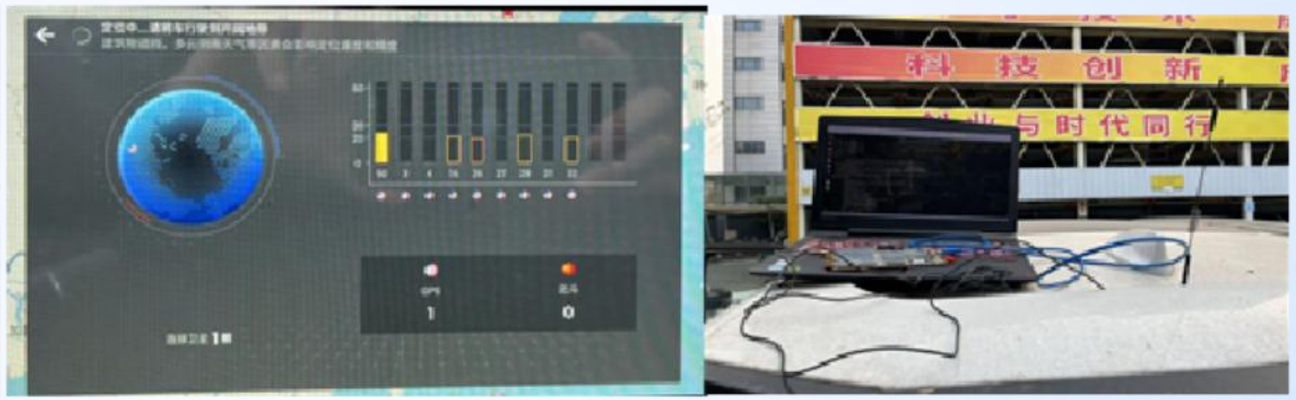
- 干扰测试
Disturbance test
- 失效测试
Failure test
- 欺骗测试
Spoof test
- 重放测试
Replay test
- 传输安全
Transmission security
- …

传感器	信号	范围	场景
GPS/北斗	微波	全球	定位
TPMS	微波	短距离	胎压监测
激光雷达	激光	中距离	碰撞避免、行人探测
超声雷达	超声波	短距离	停车辅助
毫米波雷达	毫米波	长距离	碰撞避免、自动巡航
摄像头	可见光	短距离	交通信号探测、车道探测、障碍探测

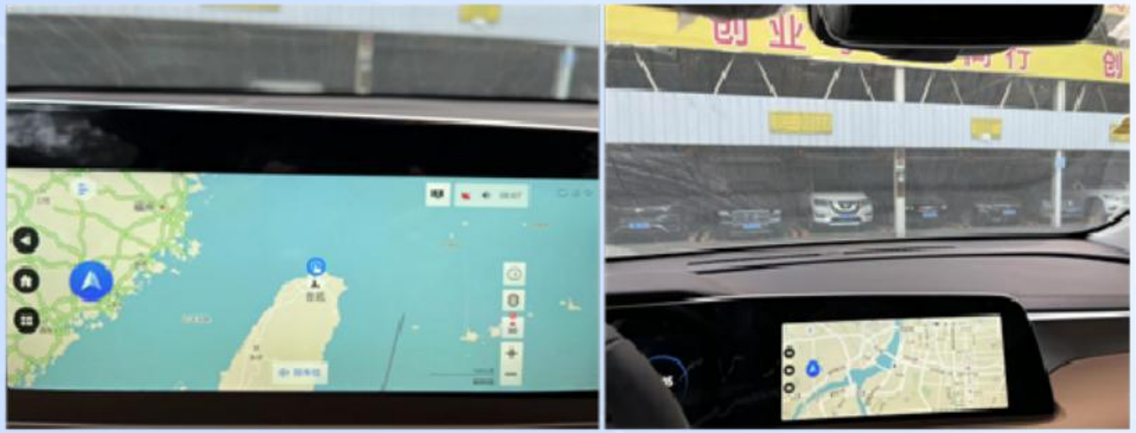
传感器安全



正常定位-园区



攻击过程中受到干扰-重新搜星



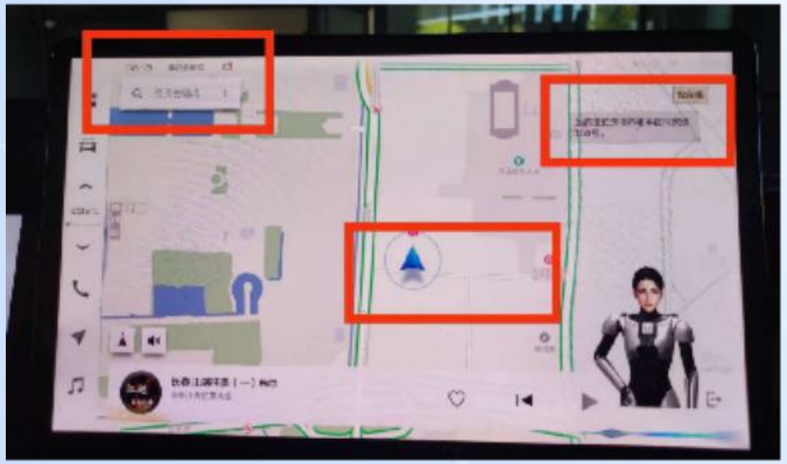
欺骗成功-台北

欺骗成功-时间系统

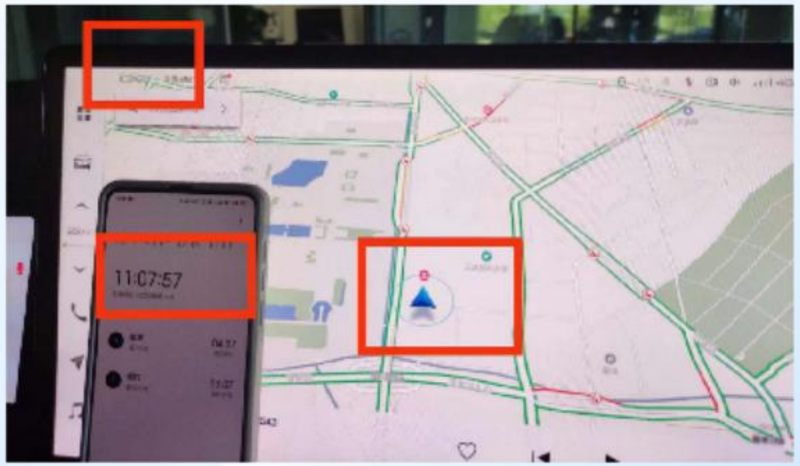
传感器安全

欺骗成功

错误导航

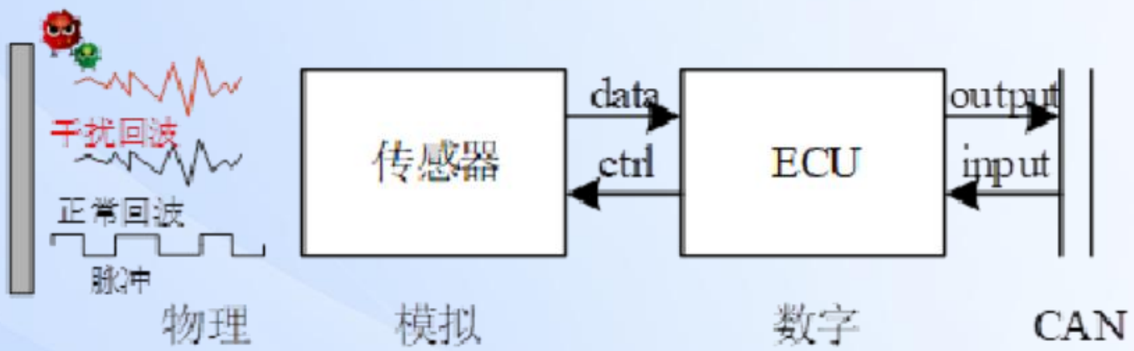


关闭后仍有效果

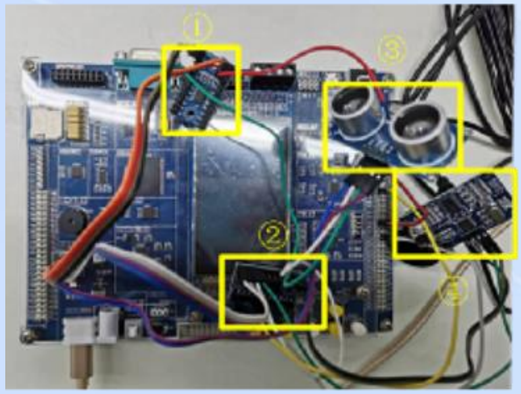


时间系统

传感器安全



攻击原理



超声波测量数据24.07cm
echo0
超声波测量数据23.50cm
echo0
超声波测量数据23.78cm
echo0
超声波测量数据23.79cm
echo0
超声波测量数据23.79cm
echo0
超声波测量数据23.78cm
echo0
超声波测量数据23.79cm

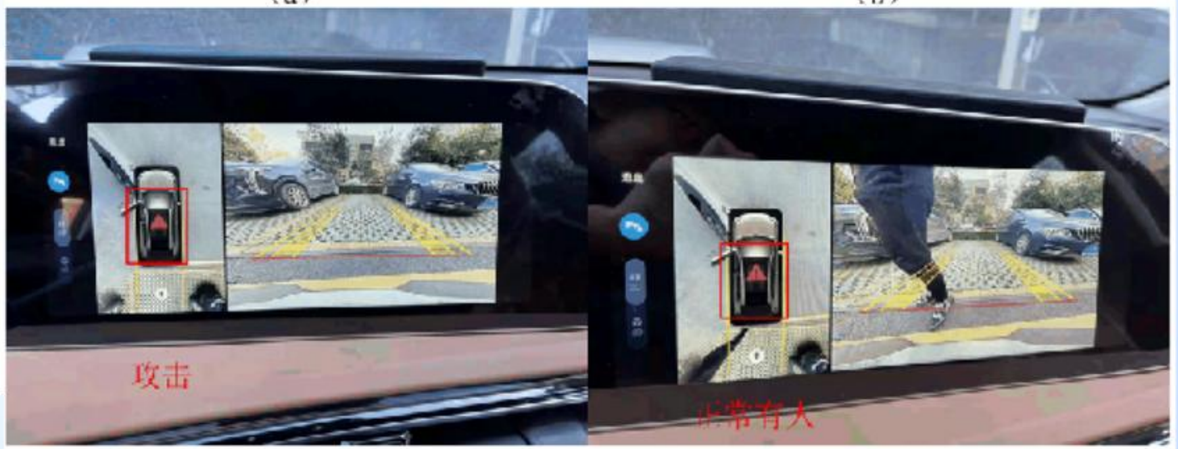
无干扰下测距稳定

jamming!
echo0
超声波测量数据4.53cm
jamming!
echo0
超声波测量数据1.24cm
jamming!
echo0
超声波测量数据4.83cm
jamming!
echo0
超声波测量数据6.31cm
jamming!
echo0

干扰下测距不稳定

攻击设备与实验室结果

(a) (b)



(c) (d)

实车测试结果

传感器安全

正常测距105cm

无人仍然测距32cm

有人却无法测距

测距不精准5cm

传感器安全

攻击原理

胎压精确控制

攻击过程

温度精确控制

传感器安全

正常情况下识别出限速40

无目标攻击下无法识别出限速40

错误识别成限速60

先正常识别为40后错误识别为60

无线电安全

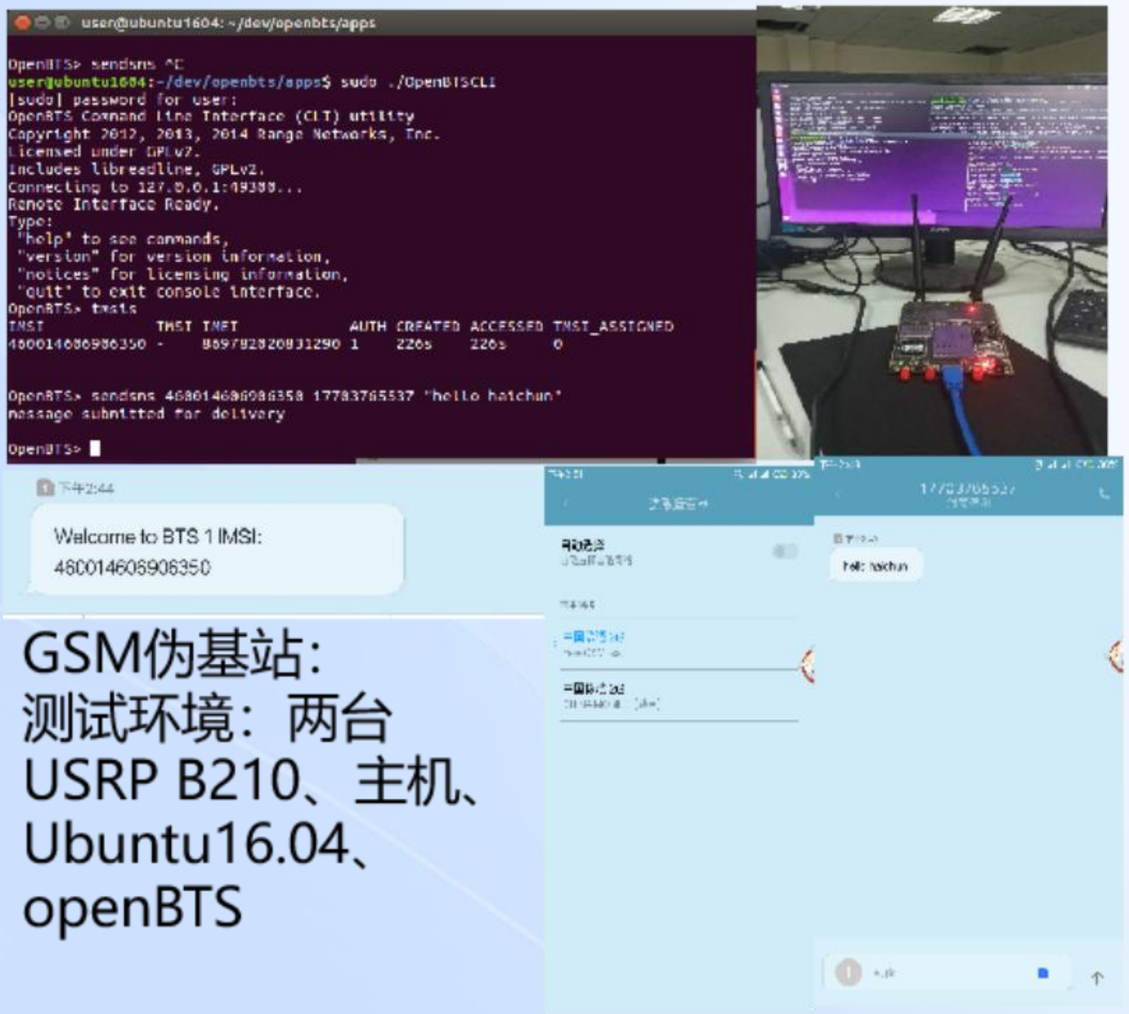
- WiFi
- Bluetooth
- Beidou
- GSM/LTE/5G
- RFID
- NFC
- ETC
- GPS
- TPMS
- PKE

- 设备扫描/复制/嗅探/发送
  Device scan/copy/sniff/send
- 加密/认证/完整性
  Encryption/Authentication/Integrity
- DoS/信道干扰
  DoS/channel interference
- 重放/碰撞
  Replay/collision
- 协议分析/模糊测试
  Protocol analysis/fuzzing

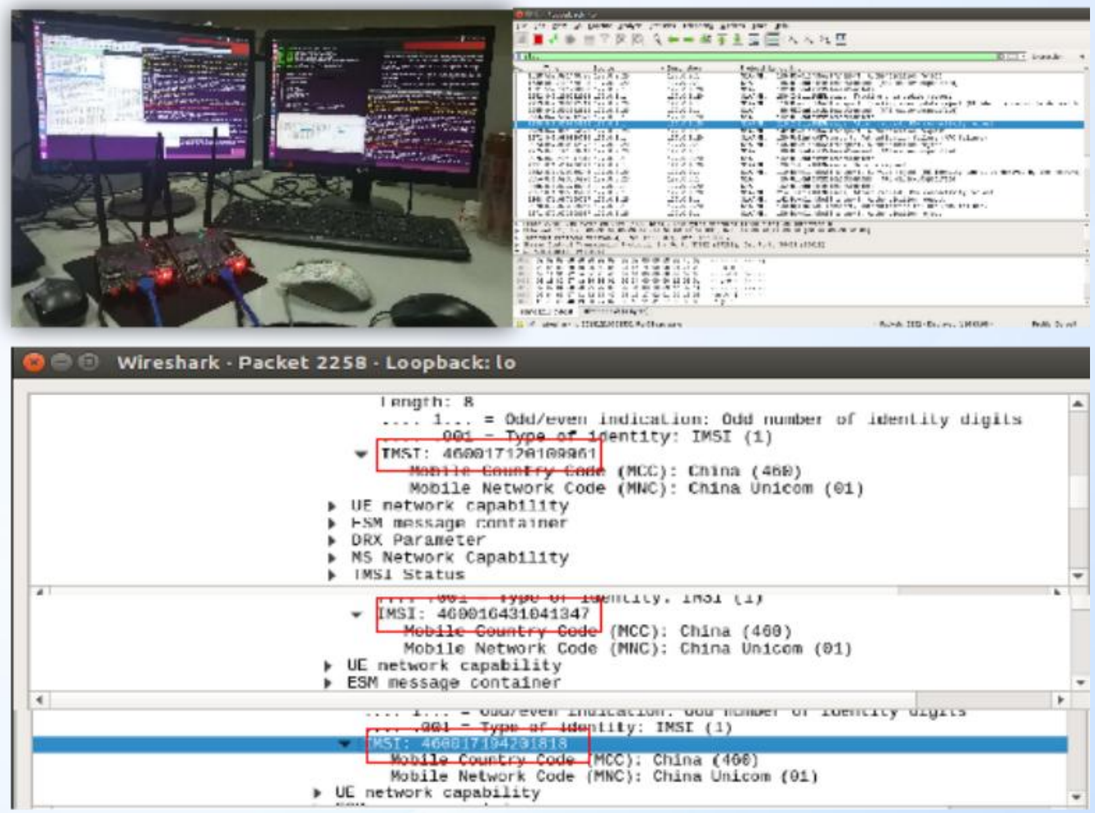
无线电安全

Wi-Fi拒绝服务

无线电安全

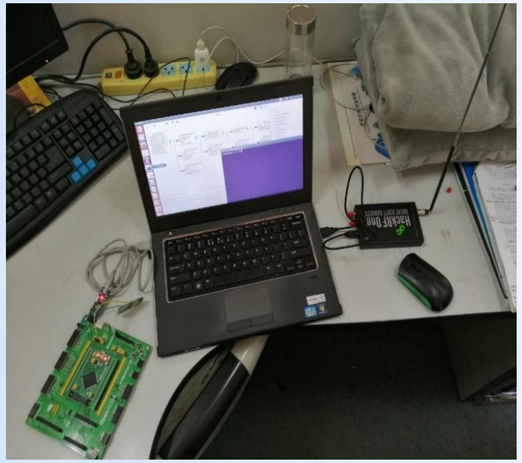


GSM伪基站：
测试环境：两台USRP B210、主机、Ubuntu16.04、openBTS



IMSI Catcher
测试环境：两台USRP B210、主机、Ubuntu16.04、OAI

无线电安全



攻击环境与设备

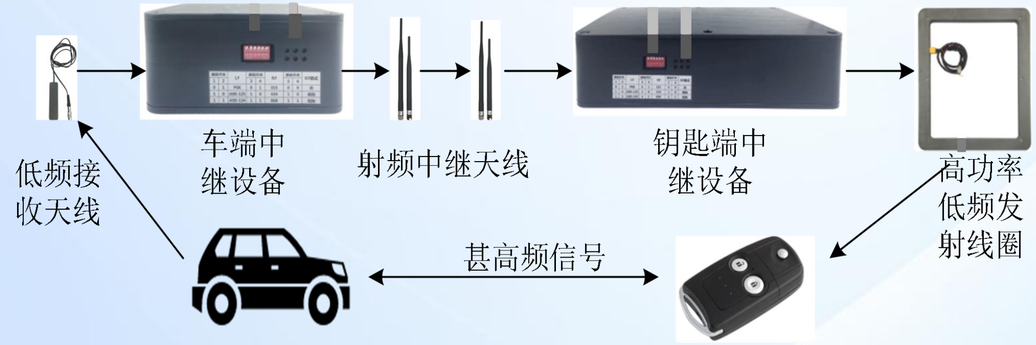
Hitag2应用于包括宝马、传祺、雪佛兰科鲁兹、奇瑞瑞虎、长城炫丽、吉利远景、大众途锐、华泰B11车、现代圣达菲、雪铁龙、标致等知名品牌。

实际车辆演示

无线电安全

新能源车型

燃油车车型



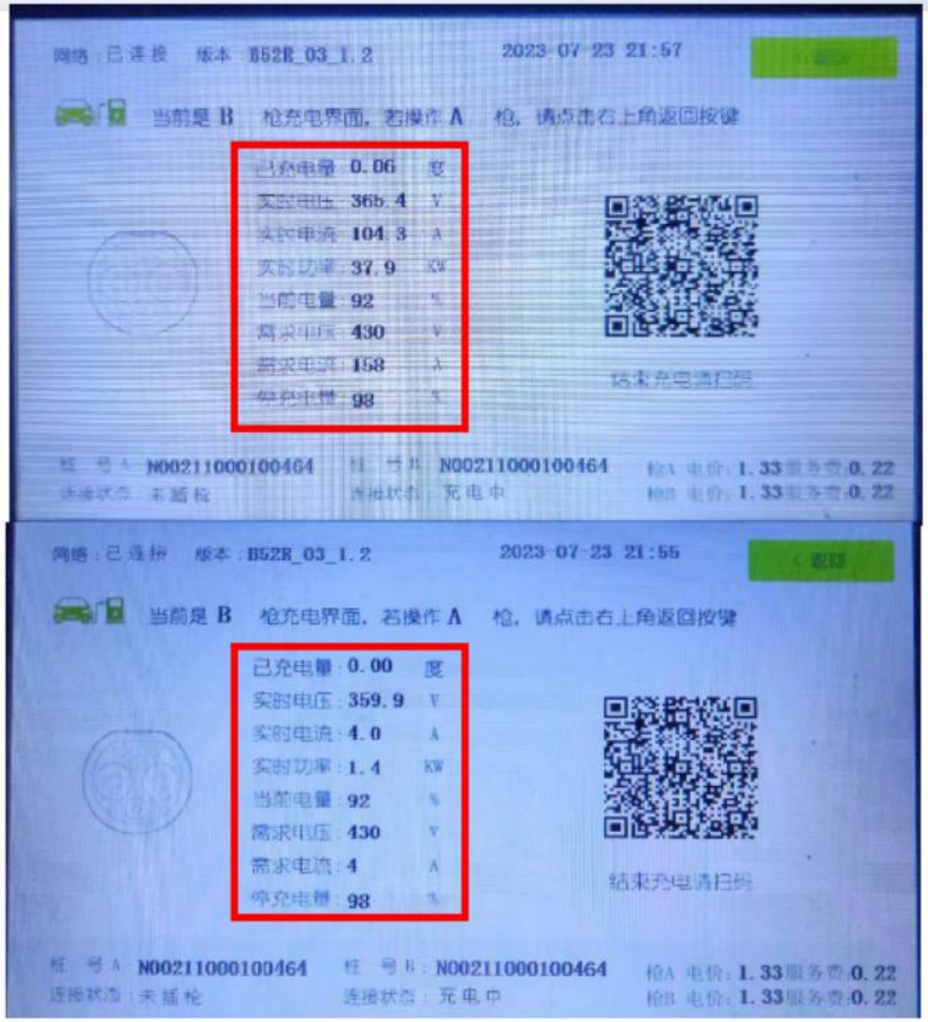
适用于当前大多数车辆

充电场景安全

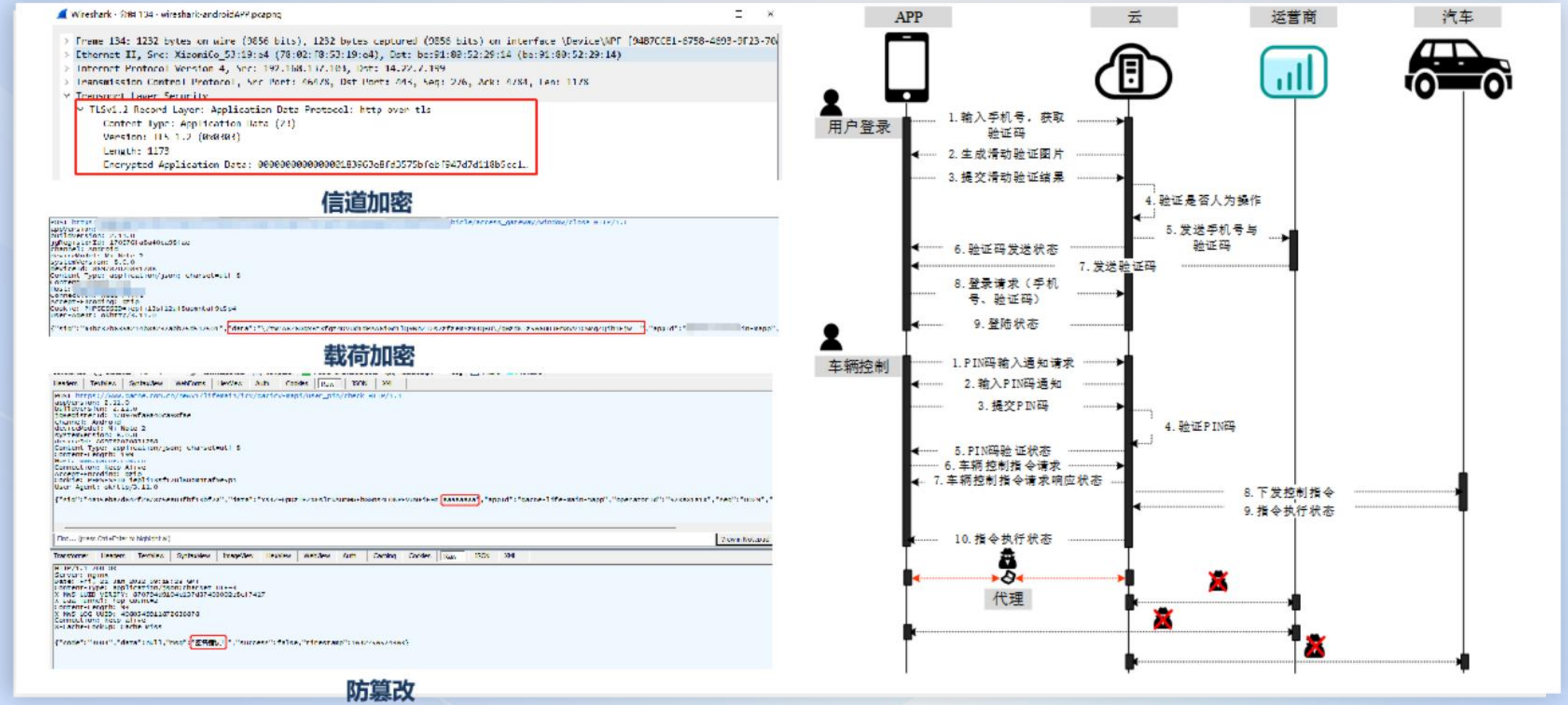
充电场景安全

修改前：191A

修改后：4A



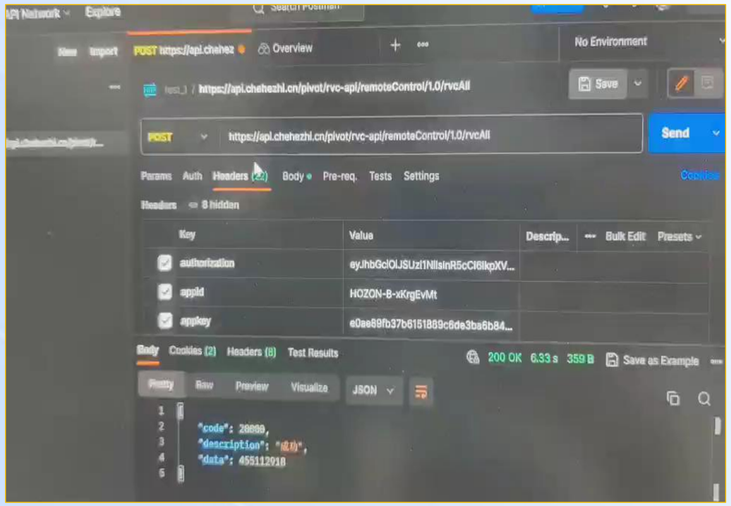
网络安全


Wireshark · 分组 134 · wireshark-androidAPP.pcapng
Frame 134: 1232 bytes on wire (9856 bits), 1232 bytes captured (9856 bits) on interface \Device\NPF_{94B7CCE1-6758-4693-8F23-70
Ethernet II, Src: XiaomiCo_53:19:e4 (78:02:78:53:19:e4), Dst: be:91:80:52:29:14 (be:91:80:52:29:14)
Internet Protocol Version 4, Src: 192.168.137.103, Dst: 14.22.7.199
Transmission Control Protocol, Src Port: 46078, Dst Port: 443, Seq: 226, Ack: 6784, Len: 1178
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: http over tls
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 1173
Encrypted Application Data: 000000000000001B38GJeBfdD575bfeb7947d7d118b5cc1...
信道加密
载荷加密
防篡改
APP
云
运营商
汽车
用户登录
1. 输入手机号，获取验证码
2. 生成滑动验证图片
3. 提交滑动验证结果
4. 验证是否人为操作
5. 发送手机号与验证码
6. 验证码发送状态
7. 发送验证码
8. 登录请求（手机号、验证码）
9. 登陆状态
车辆控制
1. PIN码输入通知请求
2. 输入PIN码通知
3. 提交PIN码
4. 验证PIN码
5. PIN码验证状态
6. 车辆控制指令请求
7. 车辆控制指令请求响应状态
8. 下发控制指令
9. 指令执行状态
10. 指令执行状态
代理

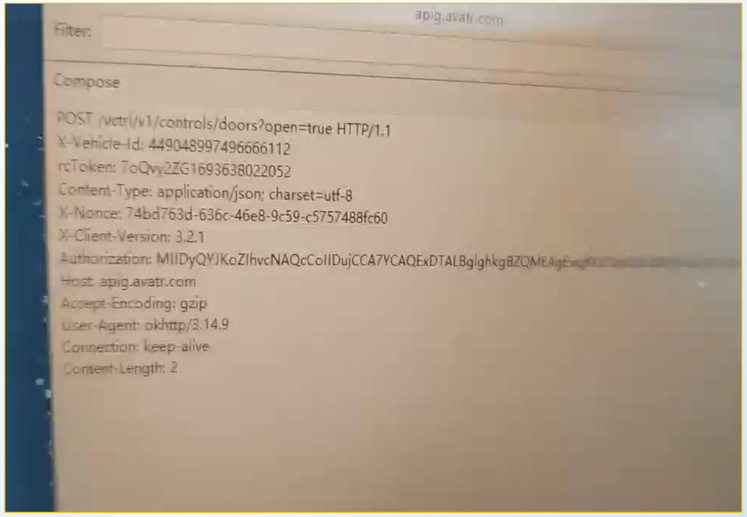
APP安全

车窗控制

车门解锁

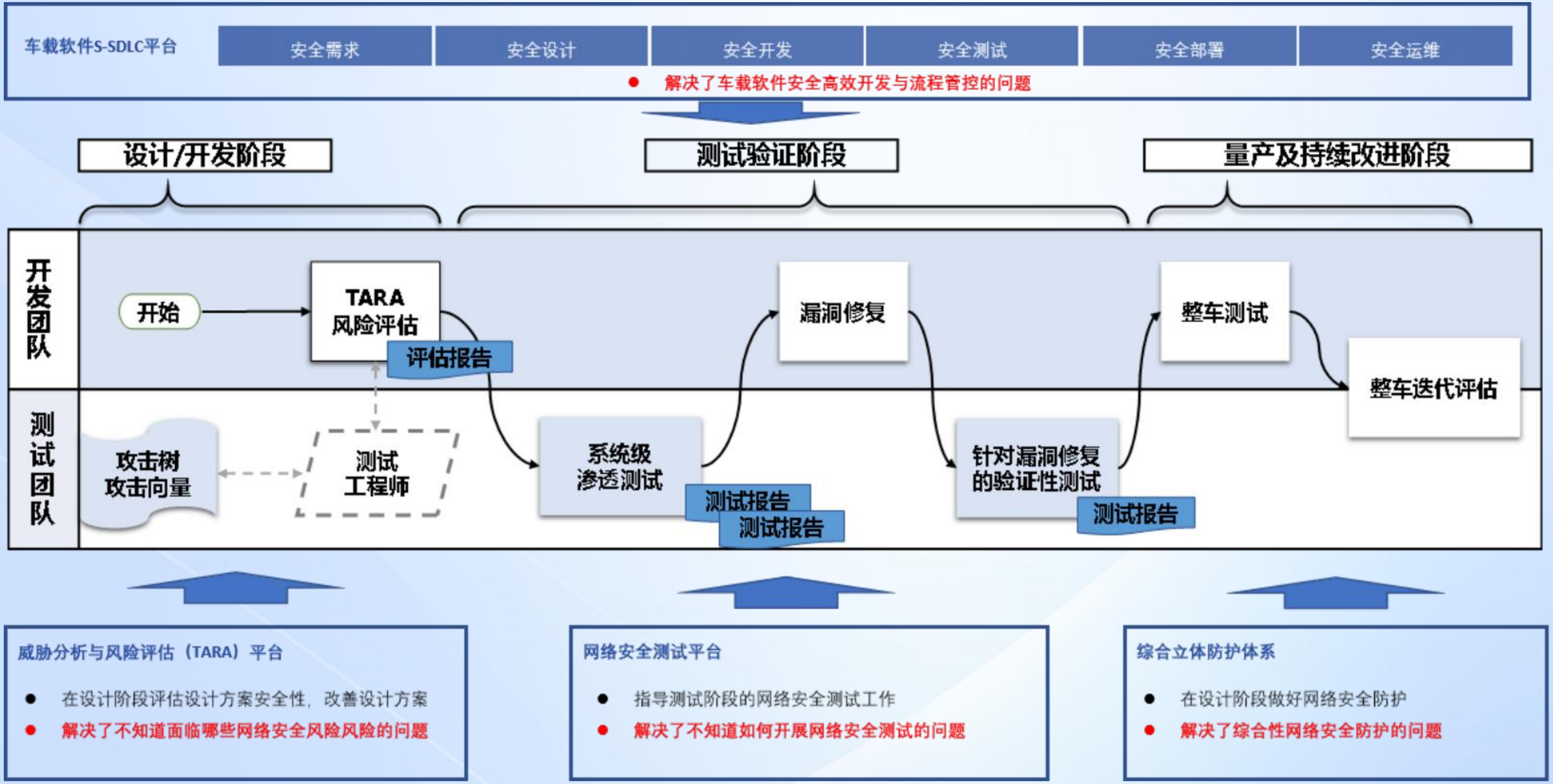


打开后备箱



车辆控制

全生命周期解决方案


车载软件S-SDLC平台
安全需求
安全设计
安全开发
安全测试
安全部署
安全运维
解决了车载软件安全高效开发与流程管控的问题
设计/开发阶段
测试验证阶段
量产及持续改进阶段
开发团队
测试团队
开始
TARA
风险评估
评估报告
漏洞修复
整车测试
整车迭代评估
攻击树
攻击向量
测试
工程师
系统级
渗透测试
测试报告
测试报告
针对漏洞修复
的验证性测试
测试报告
威胁分析与风险评估（TARA）平台
在设计阶段评估设计方案安全性，改善设计方案
解决了不知道面临哪些网络安全风险风险的问题
网络安全测试平台
指导测试阶段的网络安全测试工作
解决了不知道如何开展网络安全测试的问题
综合立体防护体系
在设计阶段做好网络安全防护
解决了综合性网络安全防护的问题

OWASP 中国 Open Worldwide Application Security Project

OWASP 中国 | 北京分会 Open Worldwide Application Security Project

网安加社区

探真科技 TensorSecurity

开源网安 SECZONE GROUP

BrainAu 脑动极光 BRAINAU

THANKS

感谢您的观看

2024 OWASP中国安全技术论坛

全球视野下的网络安全趋势