网联汽车信息安全现状分析

1 车联网安全威胁

2 车联网安全评估

3 车联网安全技术研究

4 车联网安全思考

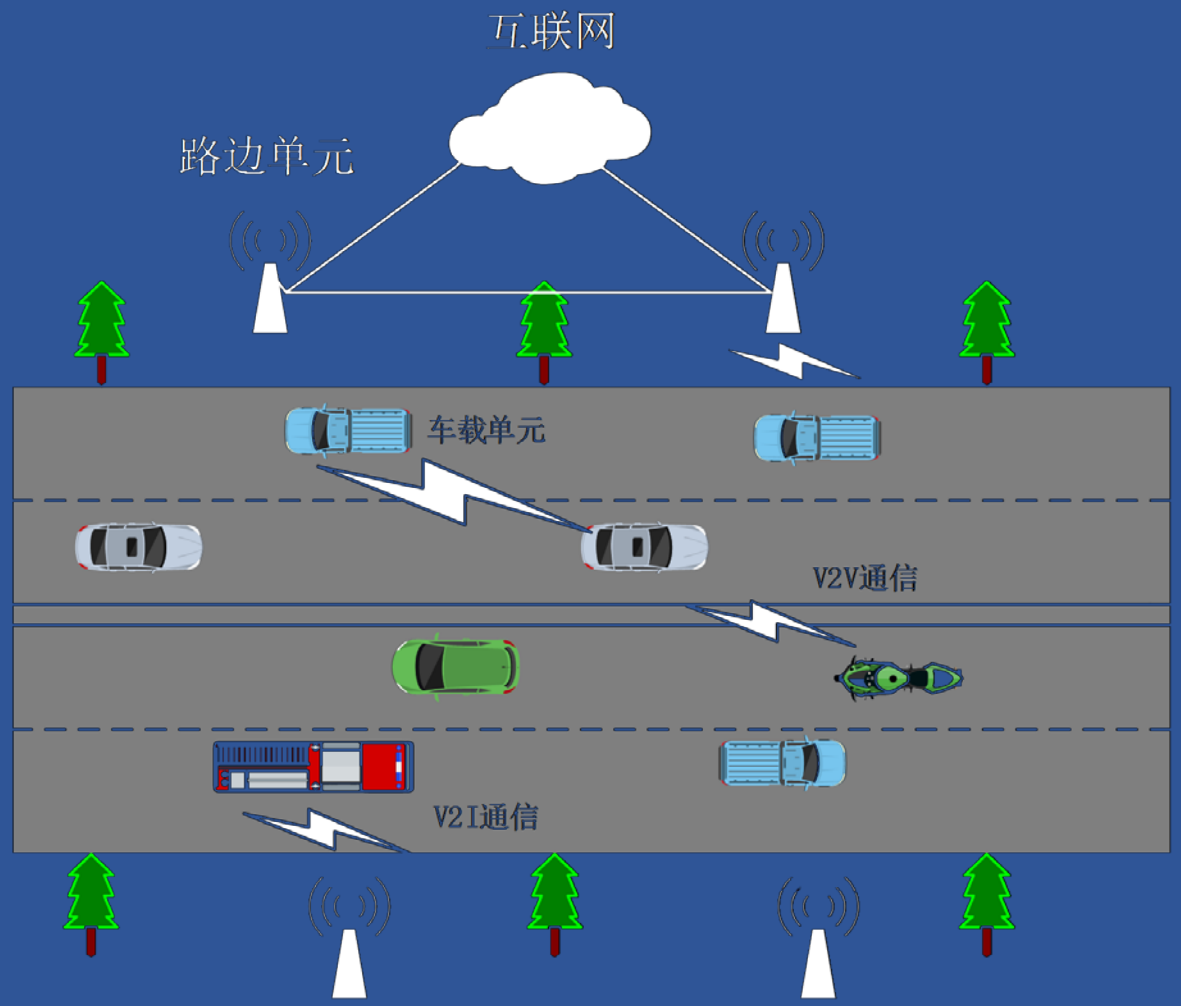
1 车联网安全威胁

- 车联网安全威胁——攻击链
- 车联网安全威胁——攻击点

车联网安全威胁

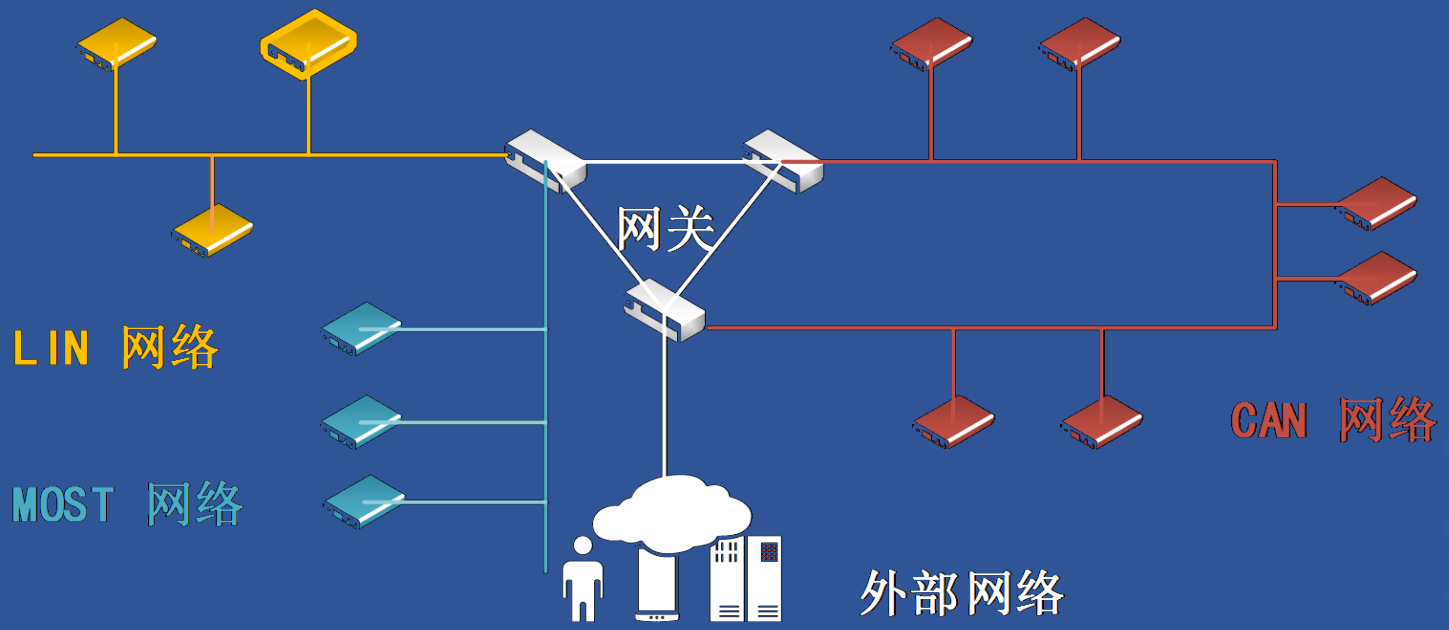
车联网体系结构

- 云端
- 管道
- 终端



车联网安全威胁

- 车内网结构
  - 多总线
  - 网关



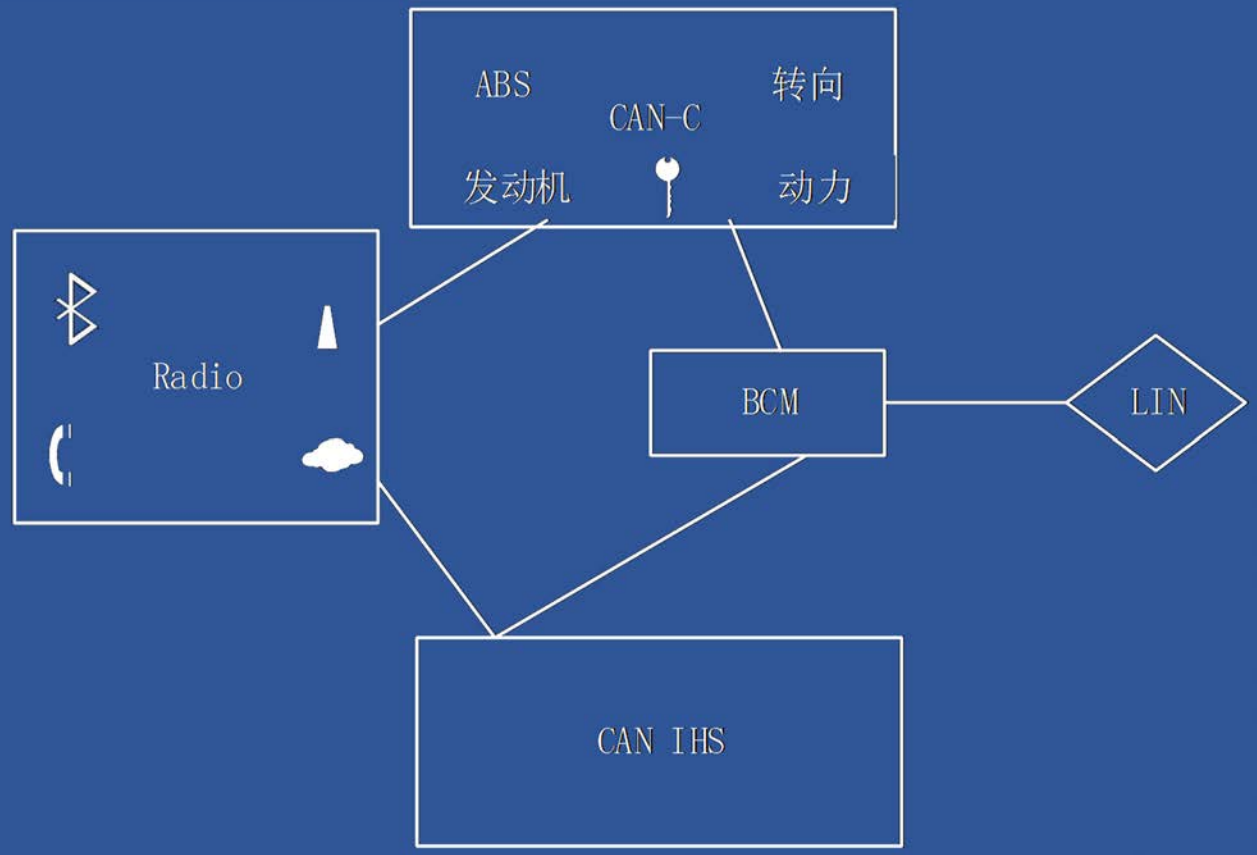
车联网安全威胁

- 安全事件回顾——攻击链

  - Charlie Miller 成功实现远程汽车控制
  - 目标：2014 Jeep Cherokee
  - Remote Exploitation of an Unaltered Passenger Vehicle

车联网安全威胁

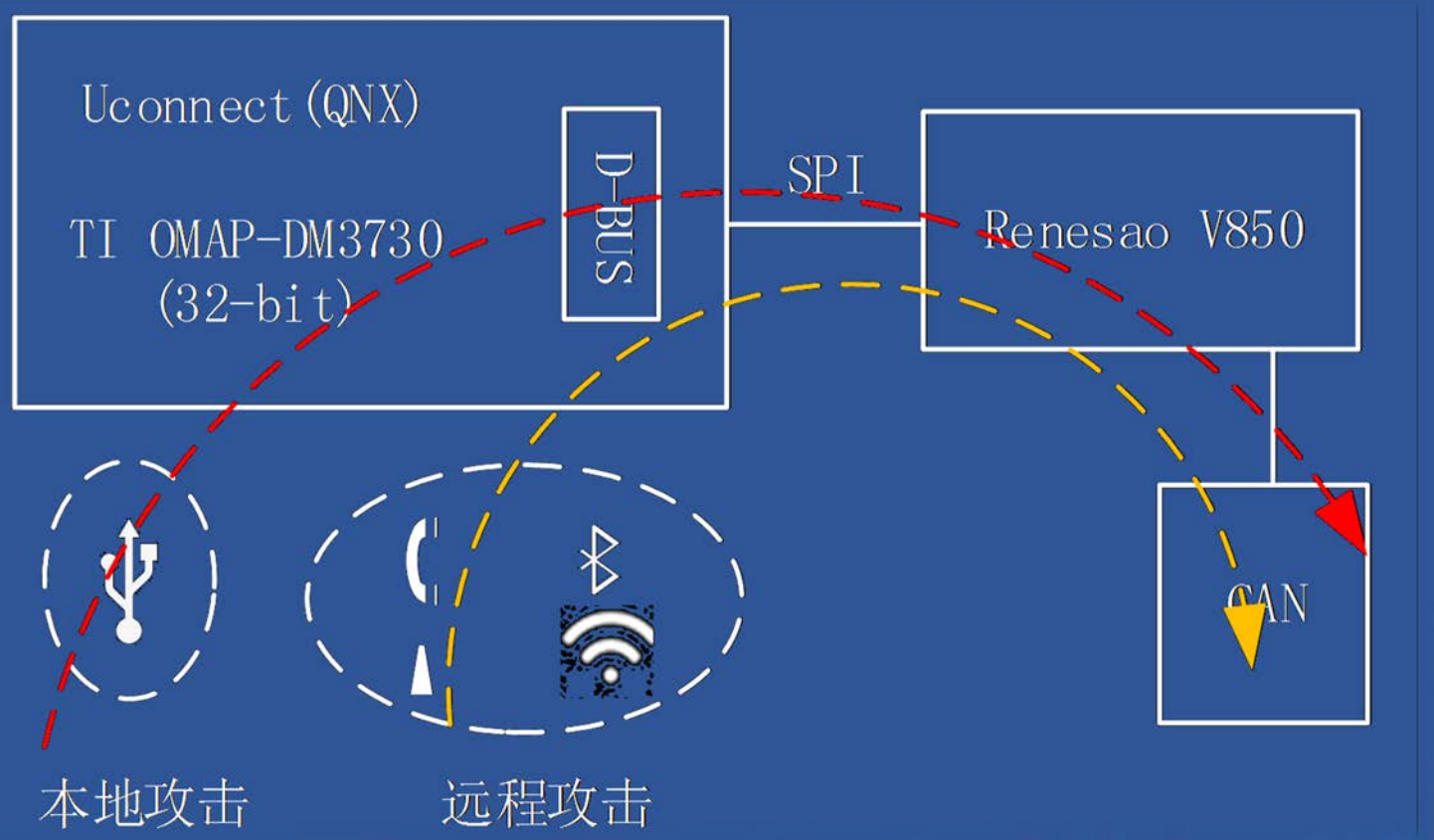
- Jeep Cherokee 内部网络架构



车联网安全威胁

- 攻击链路

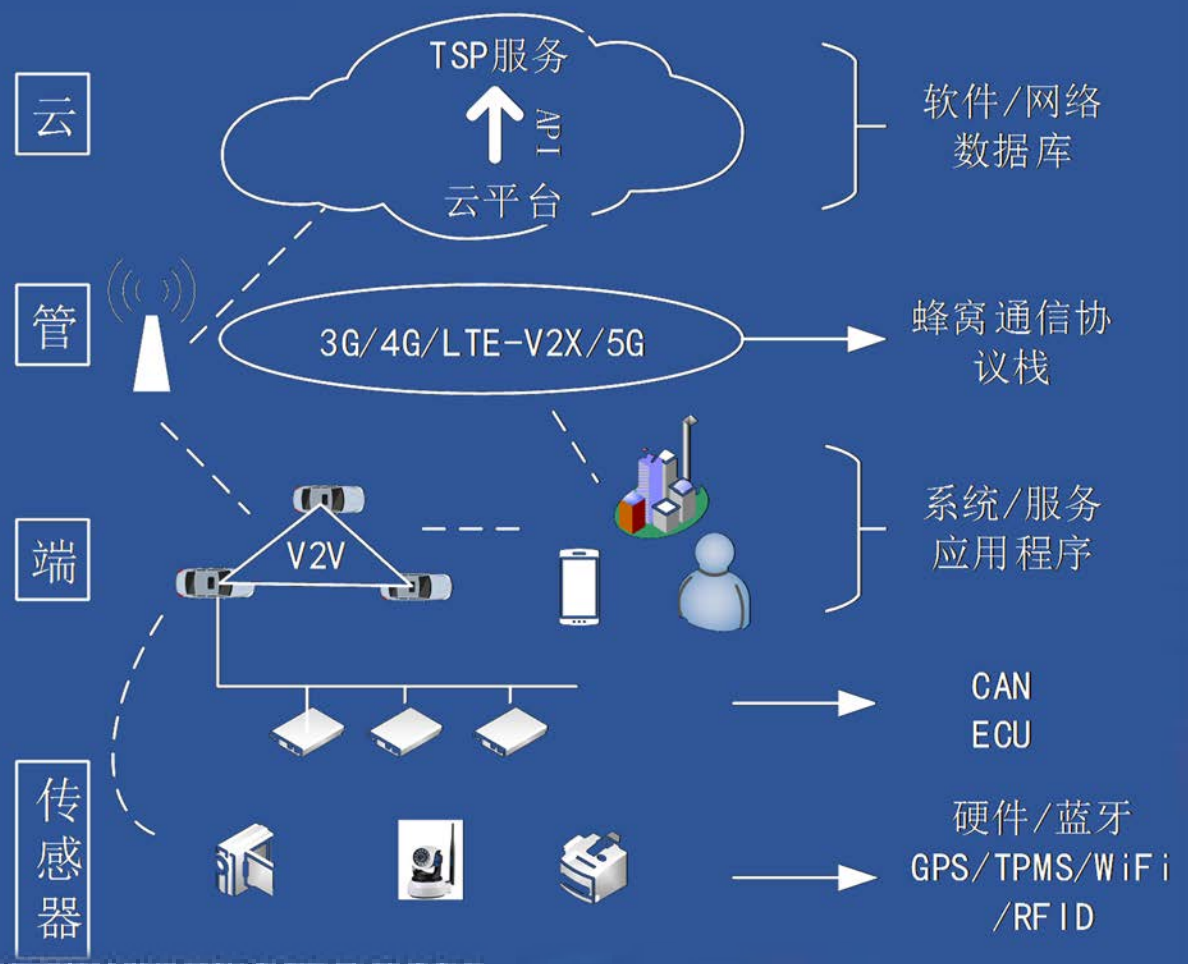
  - 本地攻击链路
  - 远程攻击链路



车联网安全威胁

- 安全威胁分析——攻击点

  - 智能网联汽车
  - 移动智能终端
  - 云端服务平台
  - 车联网通信
  - 数据安全与隐私保护



2 车联网安全评估

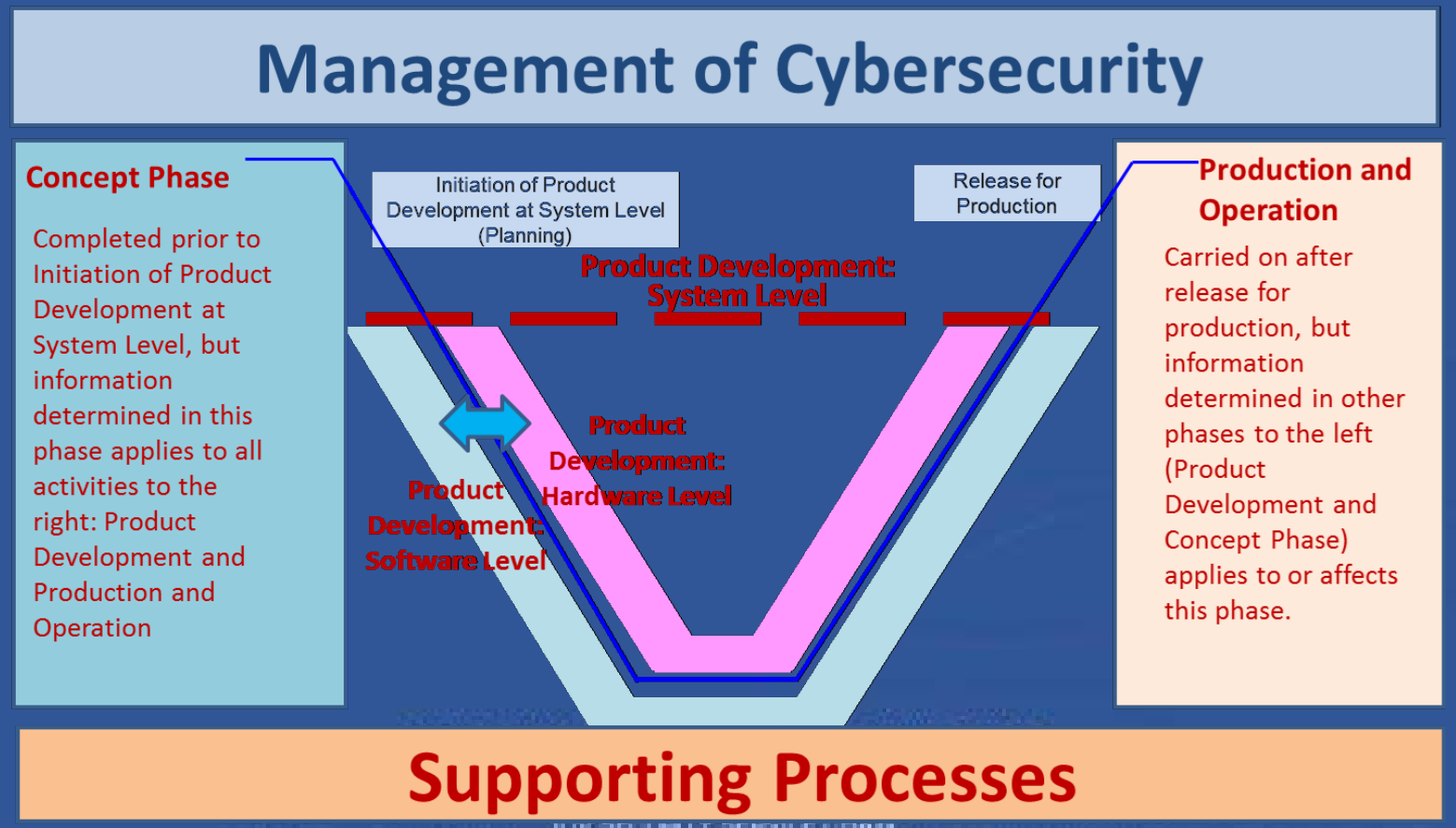
- SAE J3061汽车网络安全标准
- 车联网安全评估体系

车联网安全评估

- SAE J3061汽车网络安全标准
  - 目的：保证车联网产品的信息安全
  - 原则：将信息安全融入产品设计
  - 措施：定义了安全流程框架

车联网安全评估

- SAE J3061信息安全流程框架



车联网安全评估

- SAE J3061信息安全流程框架
  - 信息安全管理
  - 信息安全流程核心活动
    - ·概念阶段
    - ·开发阶段
    - ·生产运行阶段
  - 信息安全支持

车联网安全评估

威胁分析与风险评估

- EVITA（ E-Safety Vehicle Intrusion Protected Applications ）
- TVRA（ Threat, Vulnerabilities, and implementation Risks Analysis）
- OCTAVE（ the Operationally Critical Threat, Asset, and Vulnerability Evaluation ）
- HEAVENS（ HEAling Vulnerabilities to ENhance Software Security and Safety ）
- Attack Tree

车联网安全评估

- EVITA（https://www.evita-project.org/）

EVITA项目于2008年开始，欧盟委员会资助。成员包括MIRA、宝马集团、博世、欧洲大陆、ESCRYPT、富士通、英飞凌在内的众多机构。该项目的目标是设计、验证原型车载网络架构，保证网络安全相关组件受到保护，敏感数据不受威胁。为了达到目的，项目根据ISO / IEC 15408（7）的关键方法确定信息安全功能要求，并采用ISO / DIS 26262流程和系统工程实践

车联网安全评估

EVITA（https://www.evita-project.org/）

- 四个信息安全目标

·功能 - 以保持所有车辆和ITS功能正常运行
·安全 - 确保车辆乘客和其他道路使用者的安全
·隐私 - 保护车辆驾驶员的隐私和汽车制造商供应商的知识产权
·财产 - 防止欺诈性商业交易和车辆盗窃

- 对于每一个安全目标，EVITA项目考虑：

·威胁确认：使用攻击树分析法来识别通用威胁，从而确信息安全要求
·威胁分类：根据攻击结果的严重程度和成功攻击的可能性制定威胁风险分类建议

- 风险分析

根据威胁分类结果对采取安全机制提供参考

车联网安全评估

- 车联网安全评估体系
  - 科学的评估准则
  - 标准的测试流程
  - 丰富的测试用例

车联网安全评估

❖科学的评估准则

- VVSS（Vehicle Vulnerability Scoring System）

·本方案基于SAE J3061汽车安全指南、EVITA威胁严重性分类模型、HEAVENS模型、CVSS通用漏洞评级系统创建。它是一种对汽车漏洞进行打分、评级的系统，帮助我们对汽车漏洞事件的反应更加及时高效，确定对不同漏洞修复的优先等级。

车联网安全评估

科学的评估准则

攻击途径（AV）	远距离无线网络	1.0
	短距离无线网络	0.9
	物理接触	0.85
攻击难易性（ACo）	易	1.0
	中	0.9
	难	0.85
攻击者能力（ACa）	业余者	1.0
	修理厂/维修员	0.9
	黑客/汽车安全专家	0.85
	多领域安全专家组	0.7
攻击设备（AE）	公开的硬件设备和软件	1.0
	公开的专用硬件设备和软件	0.9
	定制或专有的硬件设备和软件	0.85
	定制或专有的硬件设备和软件	0.7
攻击范围（AS）	对单一设备	0.85
	对多个设备	0.9
	对所有设备	1.0
攻击方式（AM）	单一攻击	0.9
	复合攻击	0.95
权限获取或绕过（Pr）	需要	0.8
	不需要	1.0
机密性（CI）	不受影响	0
	部分	0.7
	完全	1.0
完整性（II）	不受影响	0
	部分	0.7
	完全	1.0
可用性（AI）	不受影响	0
	部分	0.7
	完全	1.0
权值倾向（IB）	平均	各项0.333
	机密性权值	依次0.5/0.25/0.25
	完整性权值	依次0.25/0.5/0.25

漏洞信息（VI）	无	1.0
	只可定位漏洞位置	0.95
	可获取详细的漏洞资料和技术支持	0.87
技术支持（TSu）	无	1.0
	概念证明	0.95
	成熟的技术支持	0.9
	证实有效的技术支持	0.87
修复措施（RM）	无	1.0
	非官方修复措施	0.95
	官方临时修复措施	0.9
	官方正式修复措施	0.87
响应速度（RS）	慢	1.0
	中	0.95
	快	0.9
车辆状态（VS）	高速行车	1.0
	低速行车	0.95
	驻车	0.9
攻击目标（AT）	对单车辆攻击	0.95
	对多种多辆车同时攻击	1.0

车联网安全评估

科学的评估准则

车辆被控人员伤害（PD）	无	0
	轻度伤害	0.85
	严重受伤	0.9
	生命威胁	1.0
经济损失（EL）	无	0
	单人单车经济损失	0.85
	多人多车经济损失	0.9
	车厂召回甚至导致国家层面经济损失	1.0
数据CIA (DC)	无	0
	部分	0.8
	全部	1.0
公共安全（SSe）	低	0.7
	中	0.85
	高	1.0

评分	漏洞等级
0.0-3.9	低
4.0-6.9	中
7.0-8.9	高
9.0-10.0	严重

车联网安全评估

- 可用的测试方法
  - 可实际操作
  - 可重复使用
  - 自动化测试
  - 详细测试报告

车联网安全评估

❖丰富的测试用例

分类	测试名称
TSP云端	常规的web漏洞
手机端	常规的app漏洞
手表/环	蓝牙测试
	NFC测试
	固件逆向
	APP漏洞
其他	
T-BOX	T-BOX硬件
	T-BOX操作系统及应用
	T-BOX系统源码审计
	T-BOX通信接口及外部接口
IVI	FM/AM/XM
	显示屏
	APP漏洞
	IVI系统源码审计

IVI	FM/AM/XM
	显示屏
	APP漏洞
	IVI系统源码审计
	IVI硬件
	IVI系统更新攻击
	IVI业务功能安全
wifi	WEP,WPA密钥破解
	Dos攻击
	RF干扰攻击
	欺诈AP
	广播监听
	通过已经入侵的设备侵入网络
	MAC欺诈
蜂窝通信	2G
	GSM伪基站
	3G

USB接口安全测试	USB数据监听
	autorun.inf自动播放
	伪装攻击
	漏洞攻击
V2X、V2V通讯设备	蓝牙
	WiFi
	NFC
	设备硬件
DSRC	
RFID	
NFC	
车载网关	网关硬件
	网关软件
OBD测试	USB-OBD
	蓝牙OBD
	wifi-OBD
	固件安全存储
	固件逆向
	ECU安全访问权限
	ECU数据篡改
	ECU欺骗

3 车联网安全技术研究

- 无线通信安全研究
- ECU安全研究
- CAN网络安全研究
- OTA安全研究
- 车联网隐私安全研究

车联网安全技术研究

- 无线通信安全研究
  - WiFi
  - 蓝牙
  - GPS
  - TPMS
  - PKE/RKE
  - 蜂窝通信
  - 广播
  - RFID

车联网安全技术研究

- WiFi安全研究
  - WEP
  - WPA
  - 客户端攻击
  - DOS攻击

车联网安全技术研究

WiFi测试结果

```
CH  2 ][ Elapsed: 1 min ][ 2018-12-11 22:45 ][ WPA handshake: 28:6C:07:65:9D:24

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

28:6C:07:65:9D:24  -56   3      480     8907  359   2  54e  WPA2 CCMP   PSK  DianyuanDianji#3

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

```
                          Aircrack-ng 1.2 rc4

      [00:09:30] 664224/858186 keys tested (1109.03 k/s)

      Time left: 2 minutes, 54 seconds                          77.40%

                        KEY FOUND! [ qqwweerrttyy ]


      Master Key     : 45 58 A9 29 3F DF D8 EB 22 76 67 28 CE DF F9 BC
                       93 6A 3E 6A B8 85 2B 50 11 FD DB 2E B7 78 1B 1F

      Transient Key  : 7D 07 8D 51 DC F0 03 07 43 66 89 E8 F8 A8 95 35
                       1B 7C EE 59 81 E9 7A 41 17 43 46 D0 5E B4 3B 53
                       22 E1 8B 21 03 E8 8B E3 17 8E FF 03 15 C5 A9 24
                       2B A7 A6 1C 04 20 97 81 35 80 21 F0 5A 9D 4D 15

      EAPOL HMAC     : 51 09 BB 36 47 BC 66 43 E1 BA 4B 86 FF BB 56 01
```

车联网安全技术研究

- 蓝牙安全研究
  - 蓝牙嗅探： ubertooth、 kismet
  - 蓝牙扫描： Blue scanner、 hcitool、 BTScanner
  - 服务枚举： sdptool
  - 蓝牙窃听： gr-bluetooth、 frontline、 FTS48T
  - PIN攻击、身份伪造

车联网安全技术研究

❖蓝牙安全研究

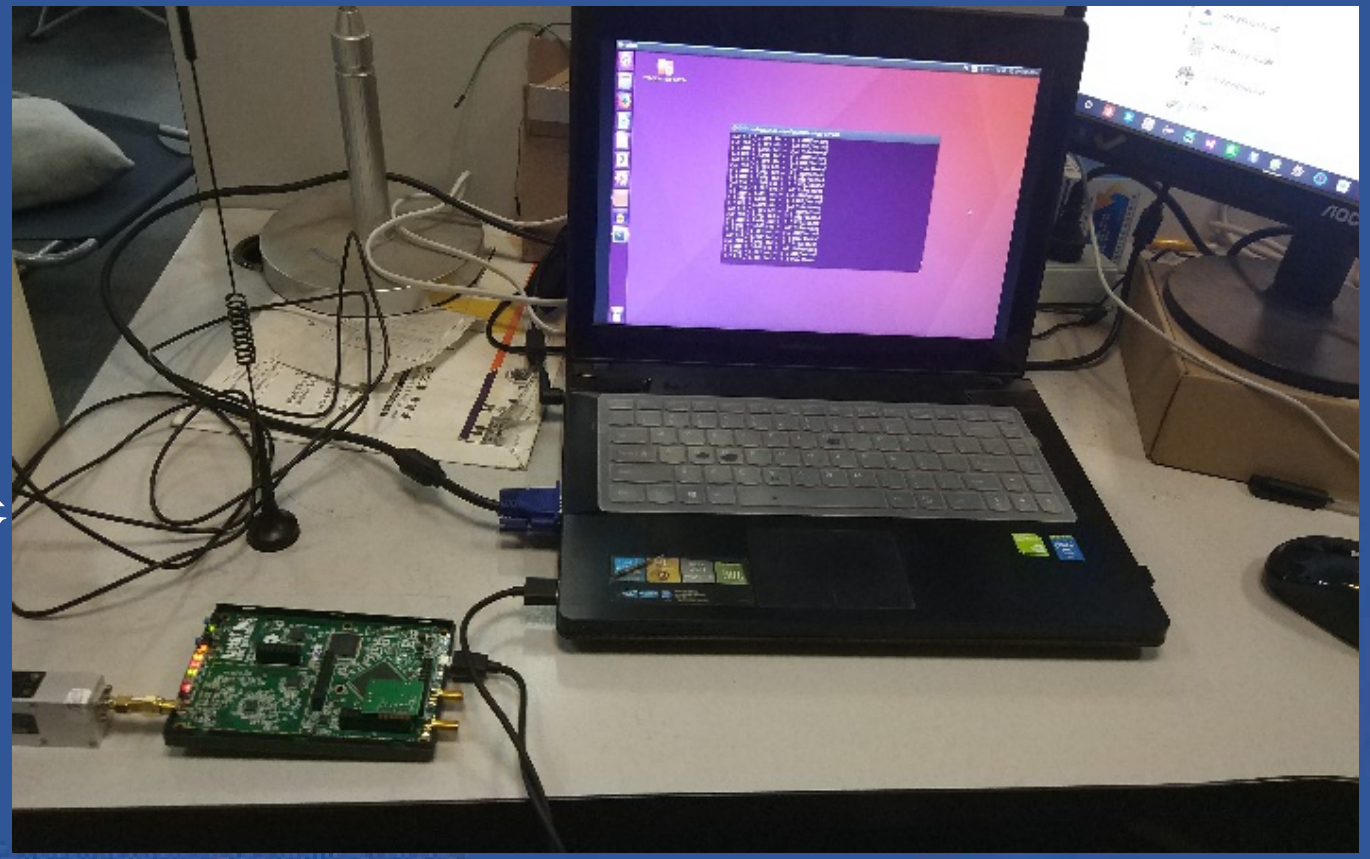
蓝牙v4.0之前版本	进行身份认证的尝试是可重复的：蓝牙设备需要包含一种机制来阻止无限次的认证请求。蓝牙规范要求连续认证尝试之间的等待时间间隔呈指数增加。然而，它对于认证过程的质询请求并未要求这样的等待时间间隔，因此攻击者可以收集大量的质询响应（这是用机密的链接密钥加密的），那就可能会泄露关于机密的链路密钥的信息。	共同版本漏洞	没有用户认证存在：规范只提供了设备认证。应用级安全性，包括用户认证，可以由应用程序开发人员通过在规范之上叠加一层来实现。
	用于广播加密的主设备密钥是在所有的微微网设备间共享的：在超过两方之间共享密钥会方便发起伪装攻击。		没有执行端到端的安全性：只有单独的链接进行了加密和认证。在中间的一些节点，数据被解密。在蓝牙协议栈之上的端到端的去安全性需要使用其他安全控制来提供。
	蓝牙BR/EDR加密所用的E0流密码算法是相对较弱的：通过在蓝牙BR/EDR加密之上叠加应用层的FIPS认证加密来实现FIPS认证加密。需要注意的是低功耗蓝牙使用AES-CCM。		可发现和/或可连接的设备都容易受到攻击：任何设备必须进入可发现或可连接模式进行配对或连接，它们应该用最少的时间来这样做。一个设备不应该一直在可发现或可连接模式下。
	如果蓝牙设备地址（BD_ADDR）被捕获并与特定用户关联，隐私可能会受到损害：一旦BD_ADDR与特定用户相关联，该用户的活动和位置可能被跟踪。	蓝牙漏洞攻击(Bluesnarfing)	Bluesnarfing让攻击者能够利用旧设备的固件漏洞来访问开启蓝牙功能的设备。这种攻击强制建立了一个到蓝牙设备的连接，并允许访问储存在设备上的数据，包括设备的国际移动设备身份码（IMEI）。IMEI是每个设备的唯一身份标识，攻击者有可能使用它来把所有来电从用户设备路由到攻击者的设备。
	设备认证是简单的共享密钥的质询/响应过程：单向质询/响应认证会受到MITM攻击。蓝牙提供了相互认证，这应被用来提供设备合法性的验证。	蓝牙劫持（Bluejacking）	Bluejacking是一种在开启蓝牙功能的设备上实施的攻击，例如对手机的攻击。攻击者通过发送未经请求的消息给开启蓝牙功能的设备用户来发起Bluejacking。实际的消息不会对用户的设备造成损害，但是它们可以诱使用户以某种方式做出响应或添加新联系人到设备的地址薄。这种消息发送攻击类似于对电子邮件用户进行垃圾邮件和网络钓鱼攻击。当用户对包含有害目的之bluejacking消息发起了一个响应，则Bluejacking能够造成危害。
蓝牙v4.0	LE配对没有提供窃听保护。此外，立即工作配对方法没有提供MITM保护：窃听者可以捕获在配对期间分配的机密的密钥（即LTTL、CSRK、IRK）。此外，MITM攻击者可以捕获和操纵受信设备之间传输的数据。LE设备应该在安全的环境中配对以最小化窃听和MITM攻击的风险。立即工作配对不应被使用。	蓝牙窃听(Bluebugging)	Bluebugging利用一个在一些较老设备固件上存在的漏洞来获取设备和其命令的访问权限。这种攻击无需通知用户就使用设备的命名，从而让攻击者可以访问数据、拨打电话、窃听通话、发送信息和利用设备提供的其他服务与功能。
	LE安全模式1的等级1不要求任何安全机制（即没有认证或加密）：与BR/EDR安全模式1类似，这本质上是不安全的。LE安全模式1的等级3（认证配对和加密）是被强烈推荐来替代它。	拒绝服务(Denial of Service)	让设备的蓝牙接口无法使用和耗尽设备电池。
		配对窃听(Pairing Eavesdropping)	PIN码/传统配对（蓝牙2.0及更早版本）和LE配对（蓝牙4.0）都易受到窃听攻击。如果给予足够的时间，成功的窃听者会收集所有的配对帧，然后他/她能够确定这个（些）机密的密钥——它允许受信设备模拟和主动

车联网安全技术研究

- GPS安全研究
  - GPS干扰攻击

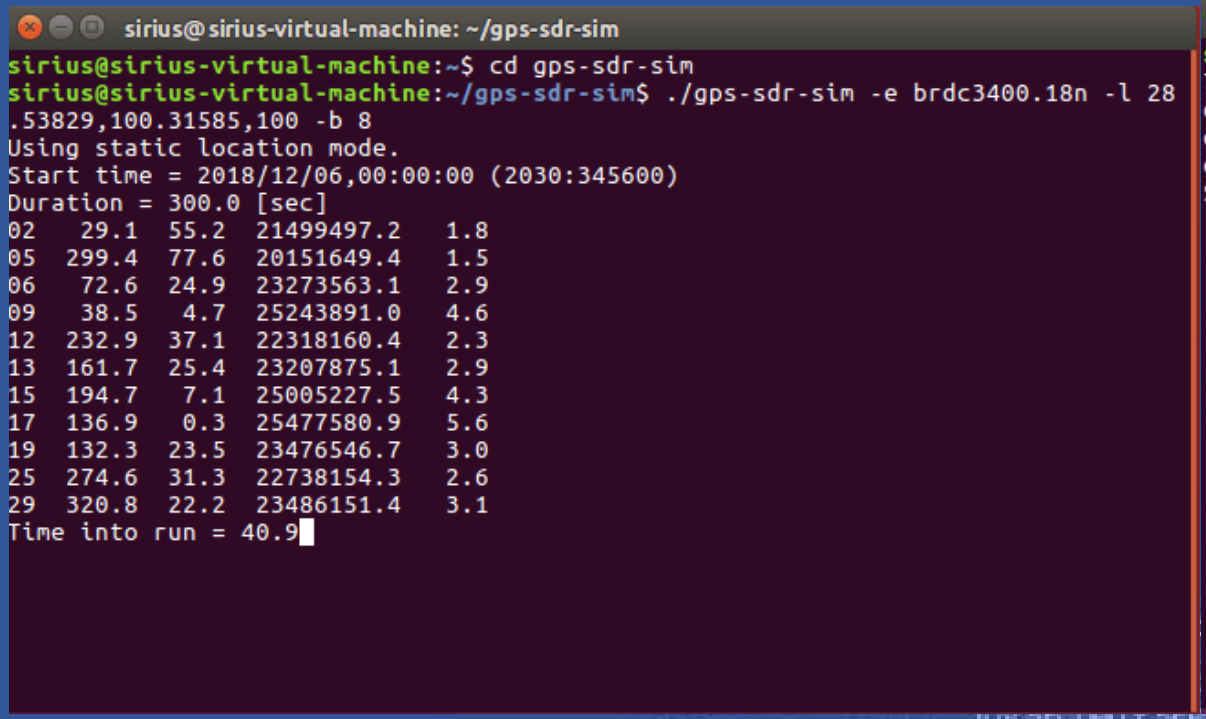
·Hackrf,天线 ,TCXO时钟模块（10MHz,2.5ppm），低噪放大器

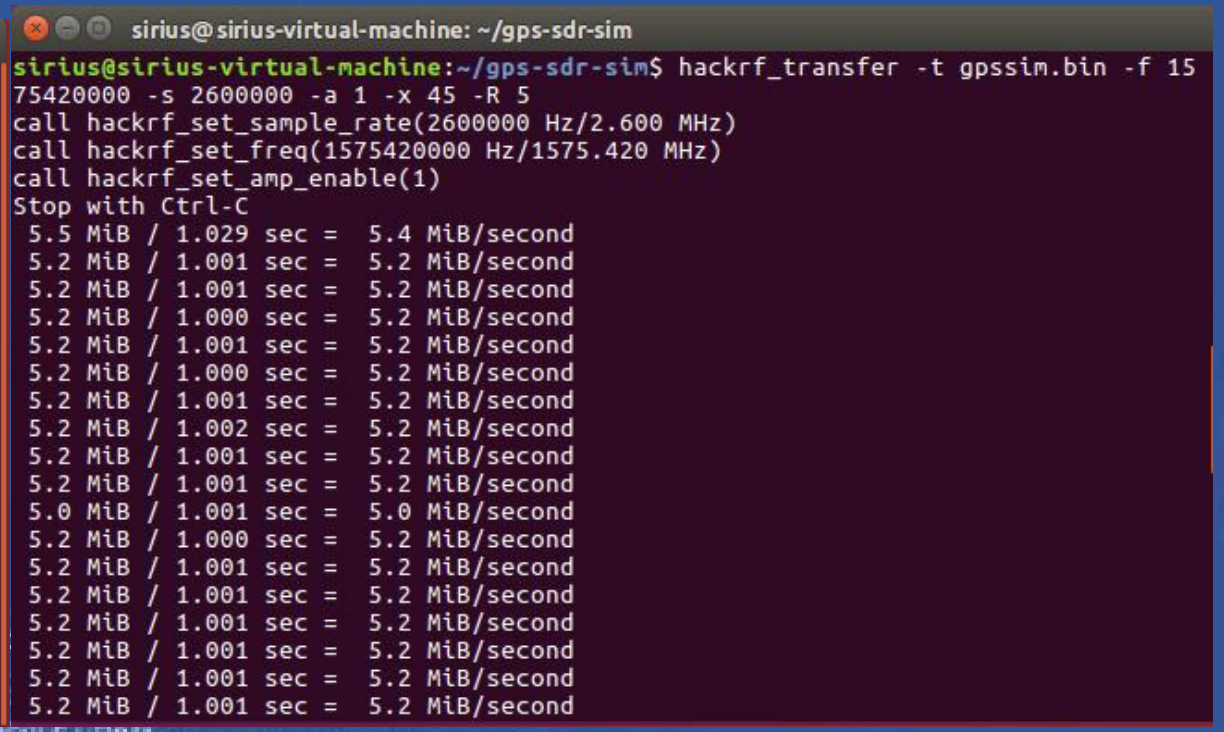
·ubuntu系统，gps-sdr-sim工具



车联网安全技术研究

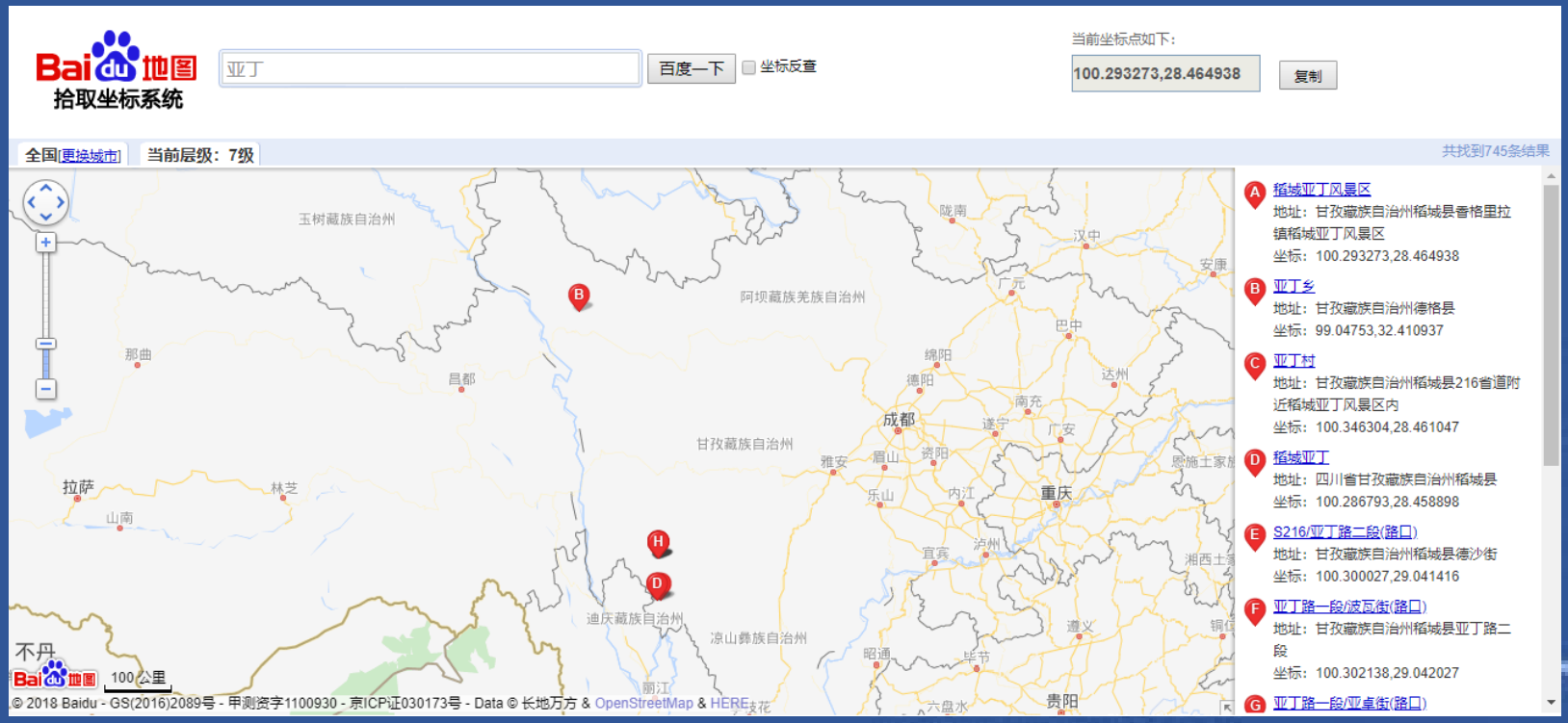
- GPS安全研究
  - 测试过程





车联网安全技术研究

- GPS安全研究
  - 测试结果



车联网安全技术研究

- TPMS安全研究
  - TPMS干扰
    - 解码工具包gr-tpms
    - 测试环境：

SDR+低噪放大器

车联网安全技术研究

- TPMS安全研究
  - TPMS攻击危害
    - 车辆追踪
    - 事件触发
    - 数据欺诈

车联网安全技术研究

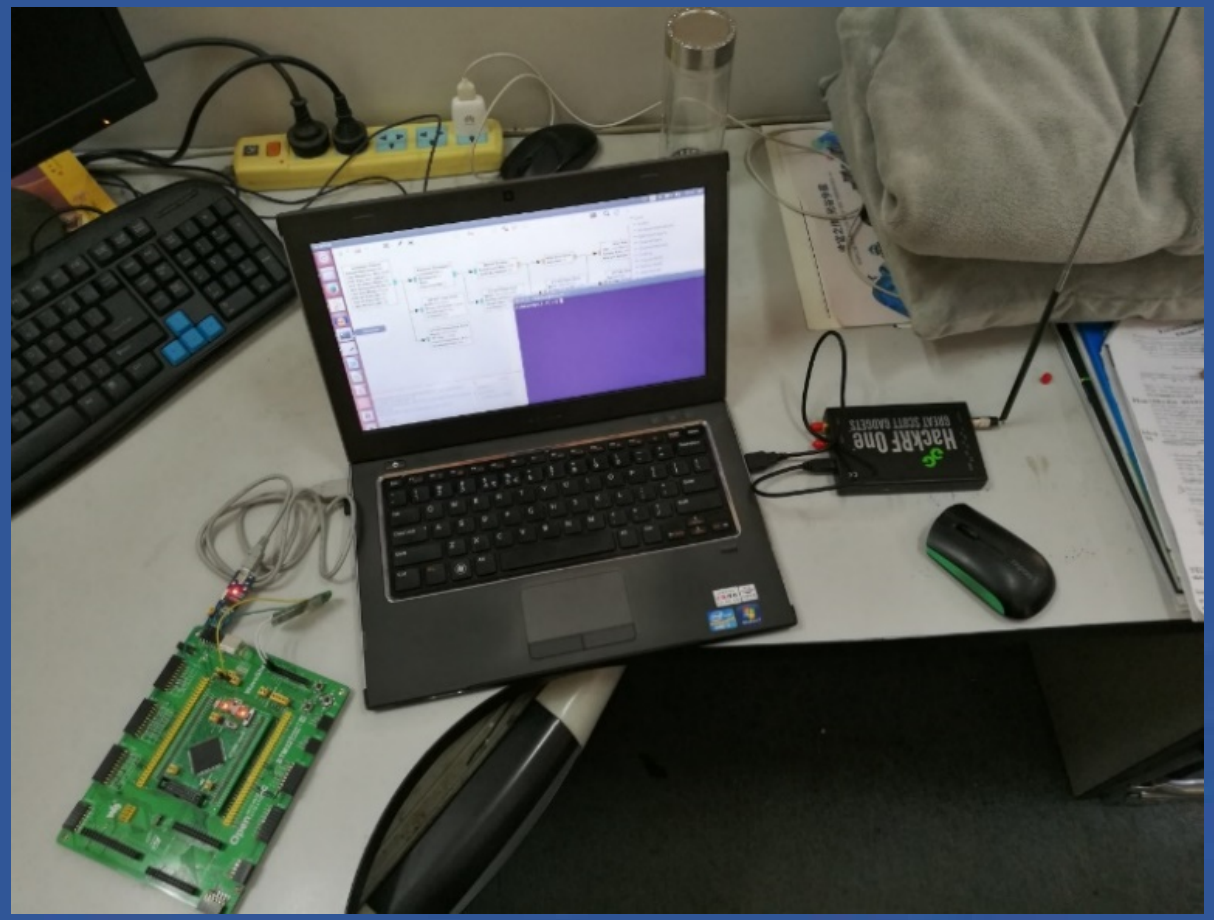
- PKE安全研究

  - Hitag2算法攻击

    测试环境：

    STM32F407开发板， hackrf

    Ubuntu16.04, gnuradio3.7.12



车联网安全技术研究

- PKE安全研究

  - Hitag2算法攻击

    测试结果：

车联网安全技术研究

- 蜂窝安全研究
  - GSM伪基站
  - 3G安全研究
  - LTE安全研究

车联网安全技术研究

- 蜂窝安全研究
  - GSM伪基站

·测试环境：

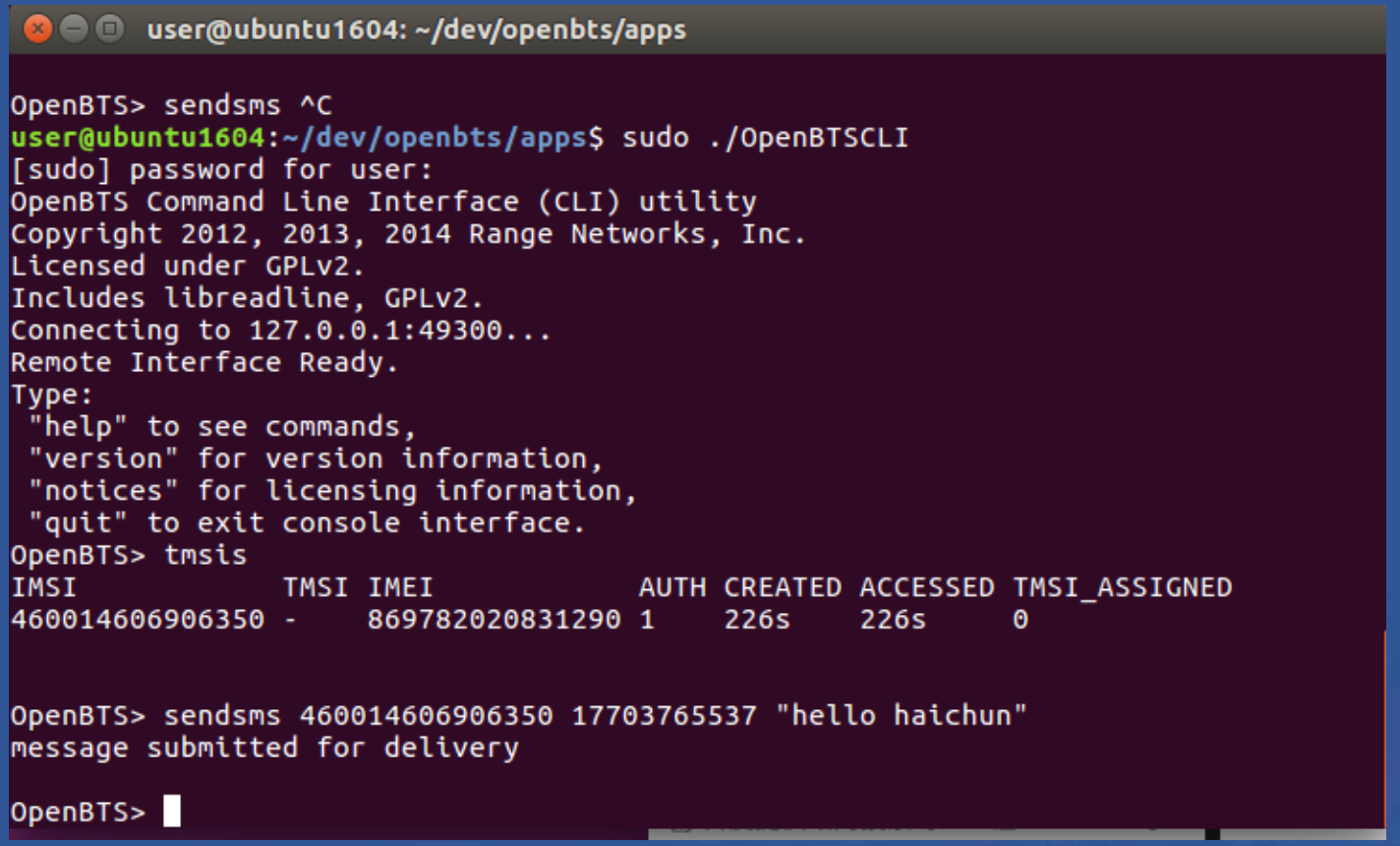
USRP B210,天线

Ubuntu16.04,OpenBTS

车联网安全技术研究

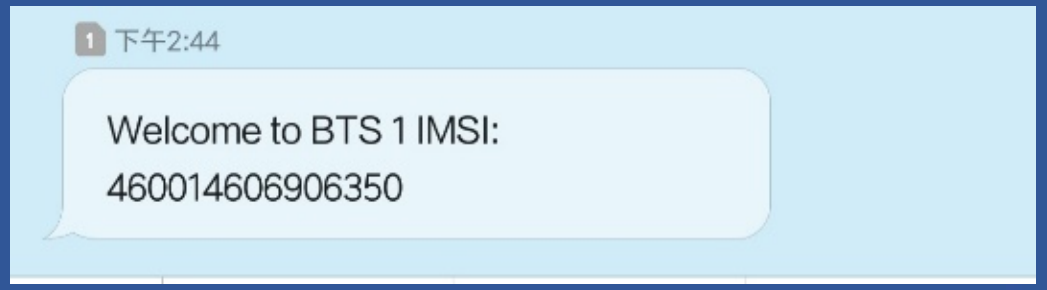
- 蜂窝安全研究
  - GSM伪基站

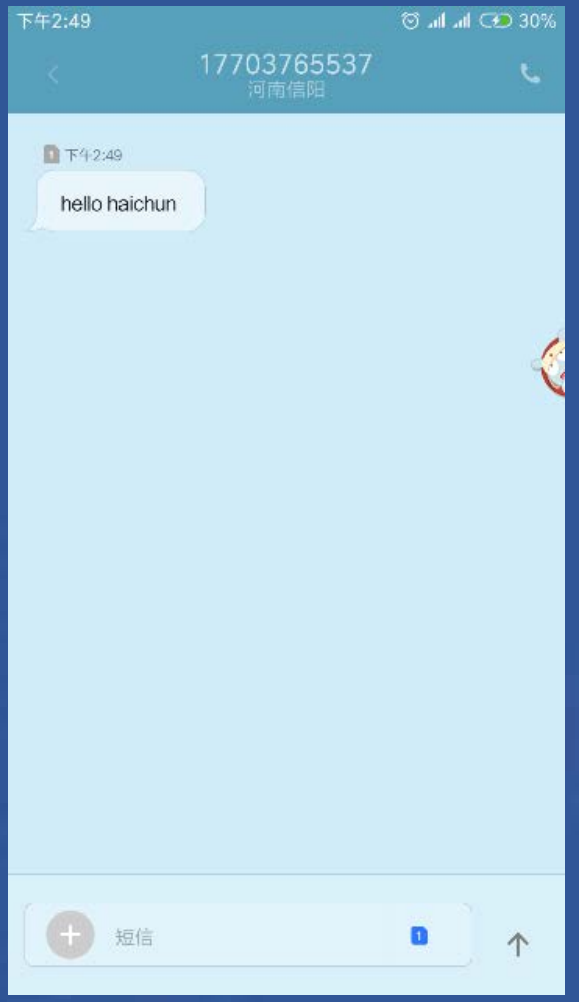
·测试过程：



车联网安全技术研究

- 蜂窝安全研究
  - GSM伪基站
  - ·测试结果：

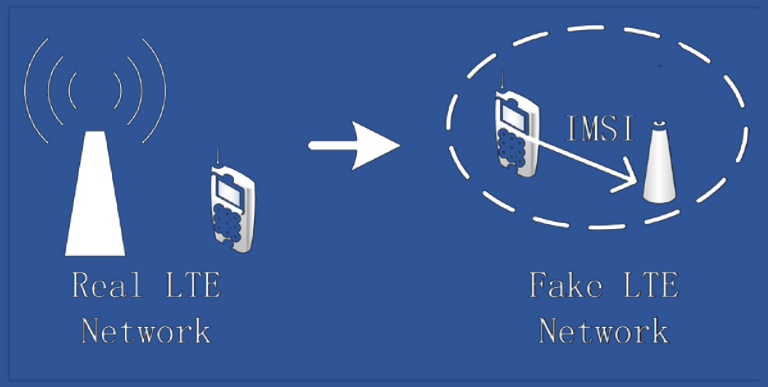




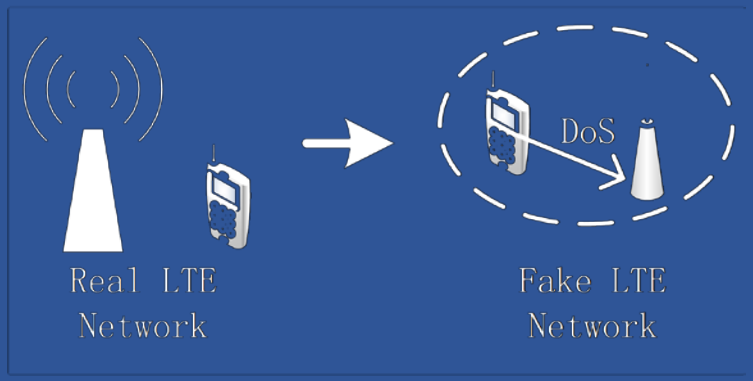
车联网安全技术研究

蜂窝安全研究

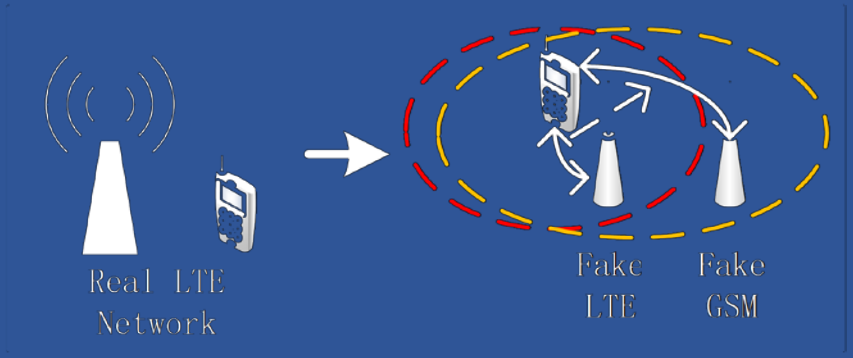
- IMSI Catcher
- Dos Attack
- Redirection Attack
- Soft Downgrade



IMSI Catcher



Dos Attack



Redirection Attack

车联网安全技术研究

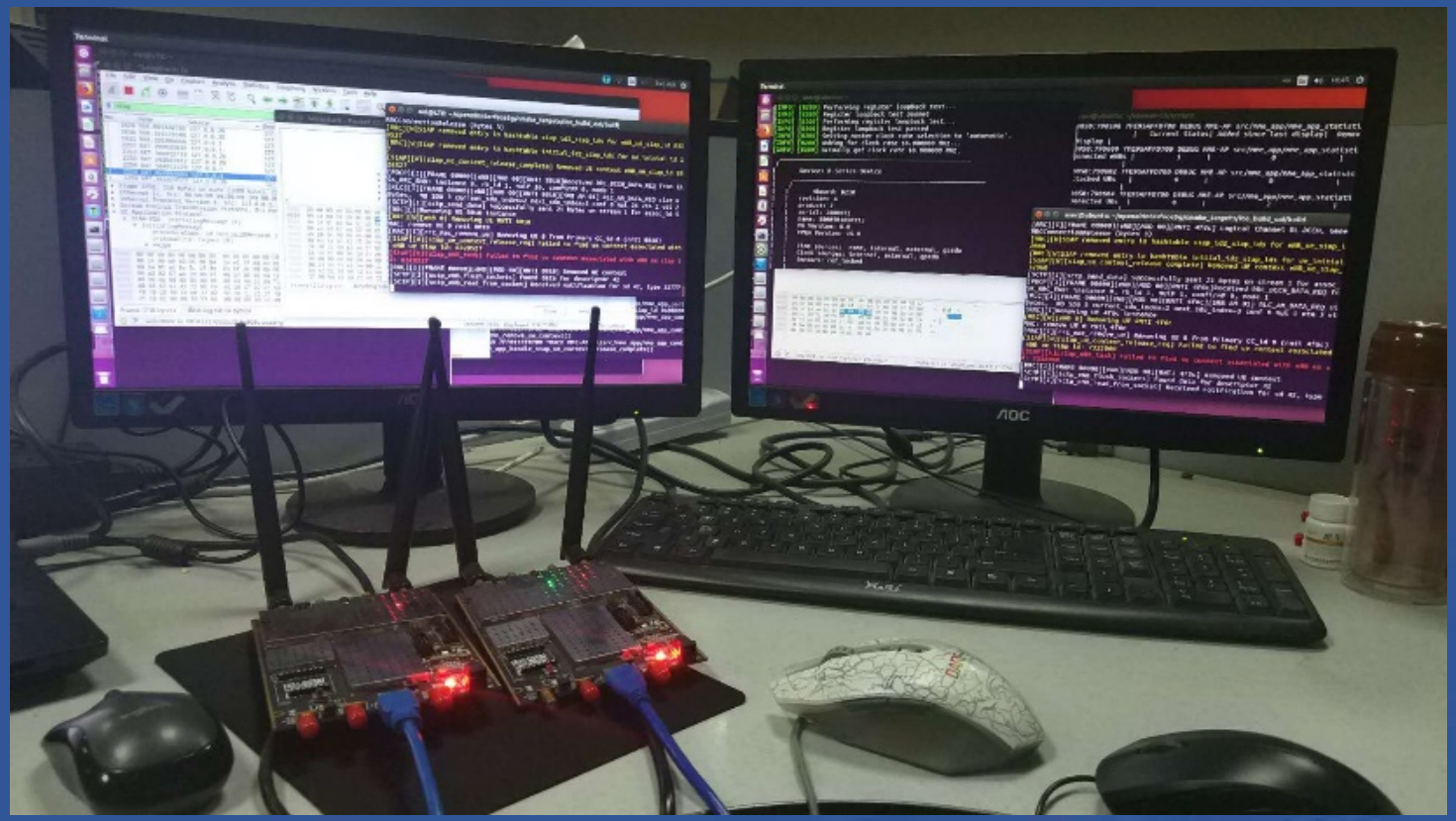
❖LTE安全研究

➢IMSI Catcher

·测试环境：

两台USRP B210，主机

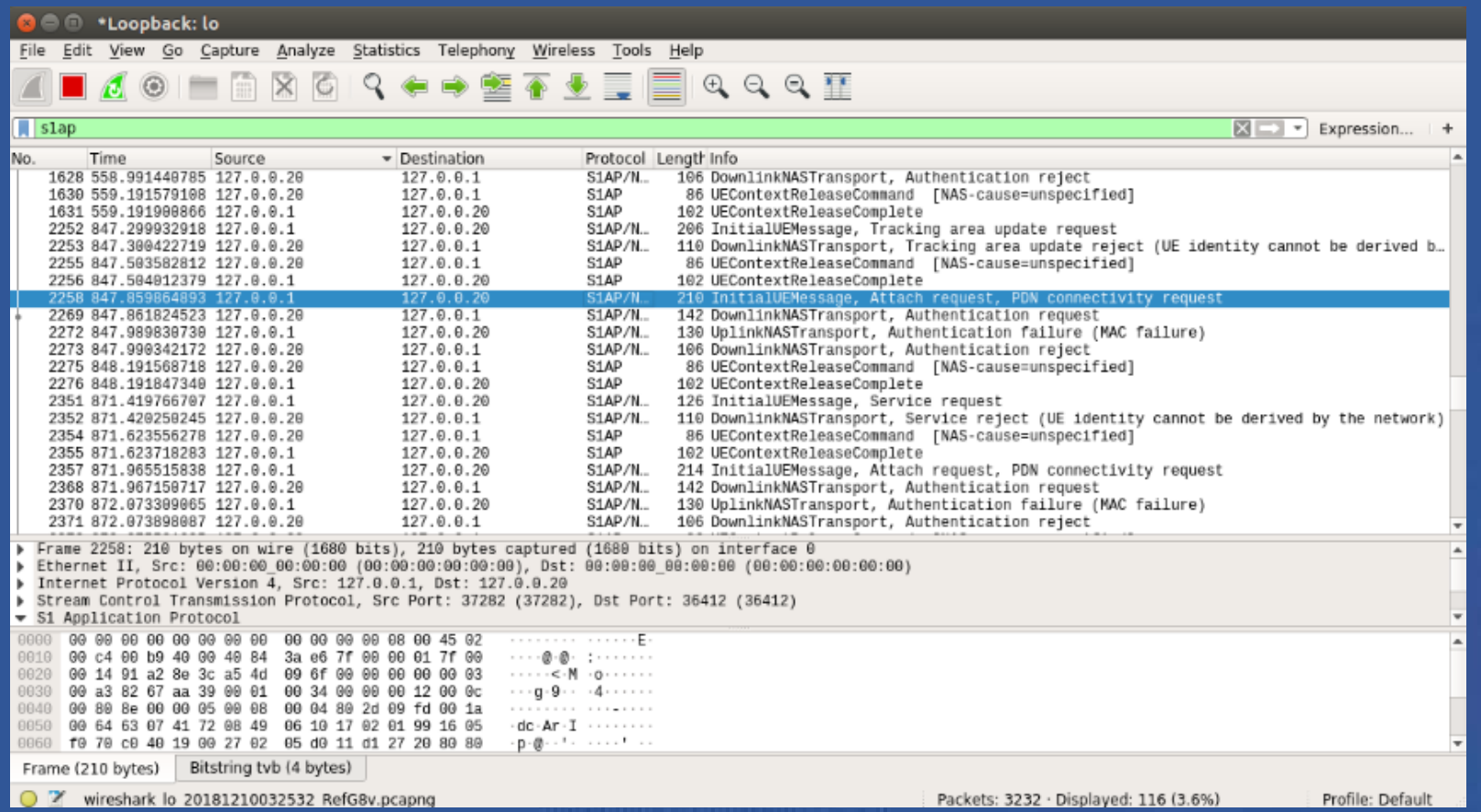
Ubuntu16.04 ， OAI



车联网安全技术研究

❖LTE安全研究

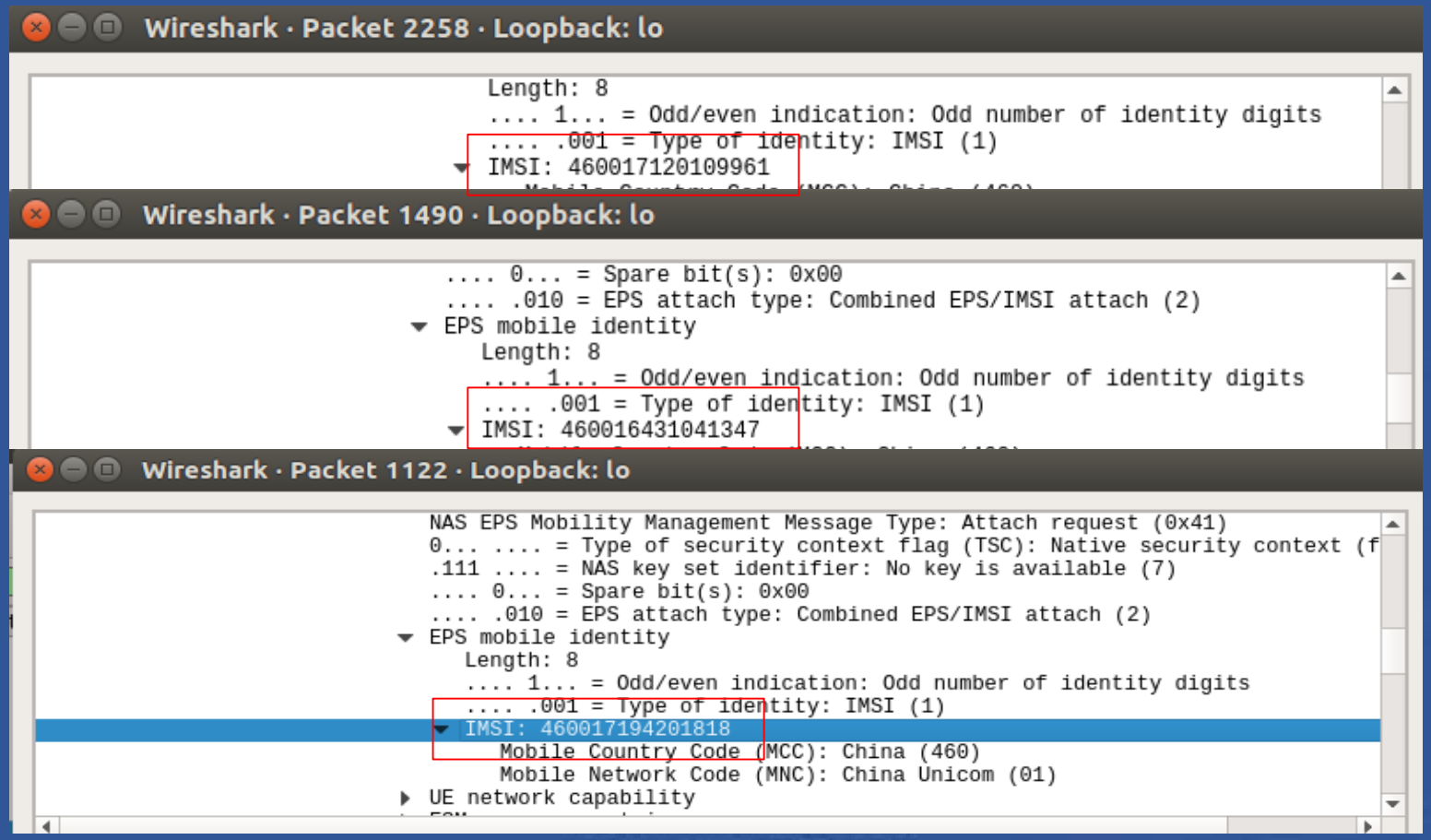
➢ IMSI Catcher测试结果



车联网安全技术研究

❖LTE安全研究

➢ IMSI Catcher测试结果



车联网安全技术研究

ECU安全研究

- 硬件安全
- 侵入式攻击
- 非侵入式攻击
- 半侵入式攻击
- 认证攻击

车联网安全技术研究

ECU安全研究

- 硬件安全

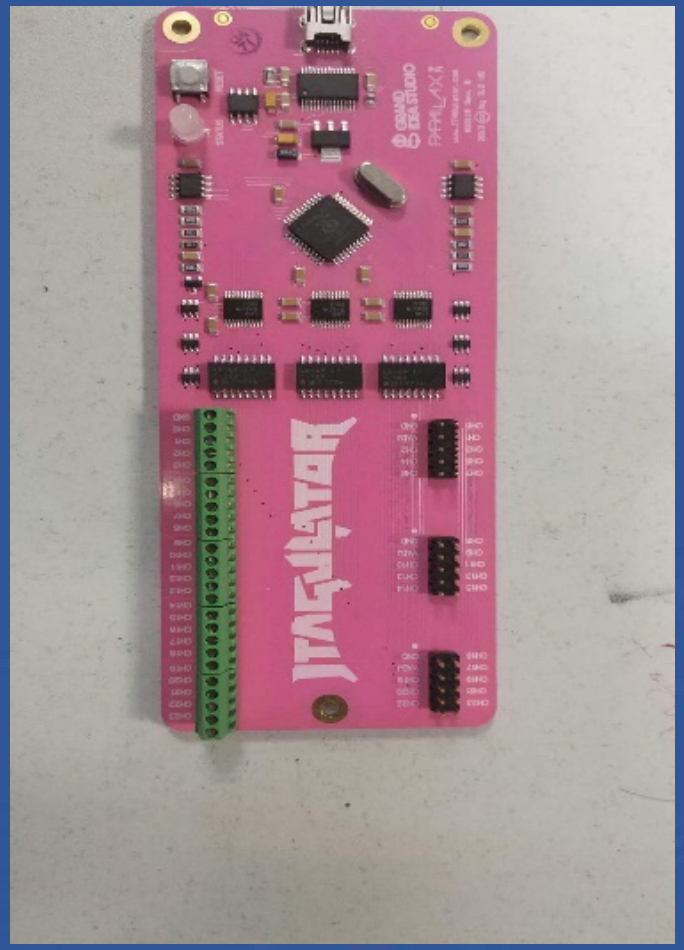
·调试接口逆向

万用表、示波器、逻辑分析仪

Jtagulator

·芯片识别

·USB接口



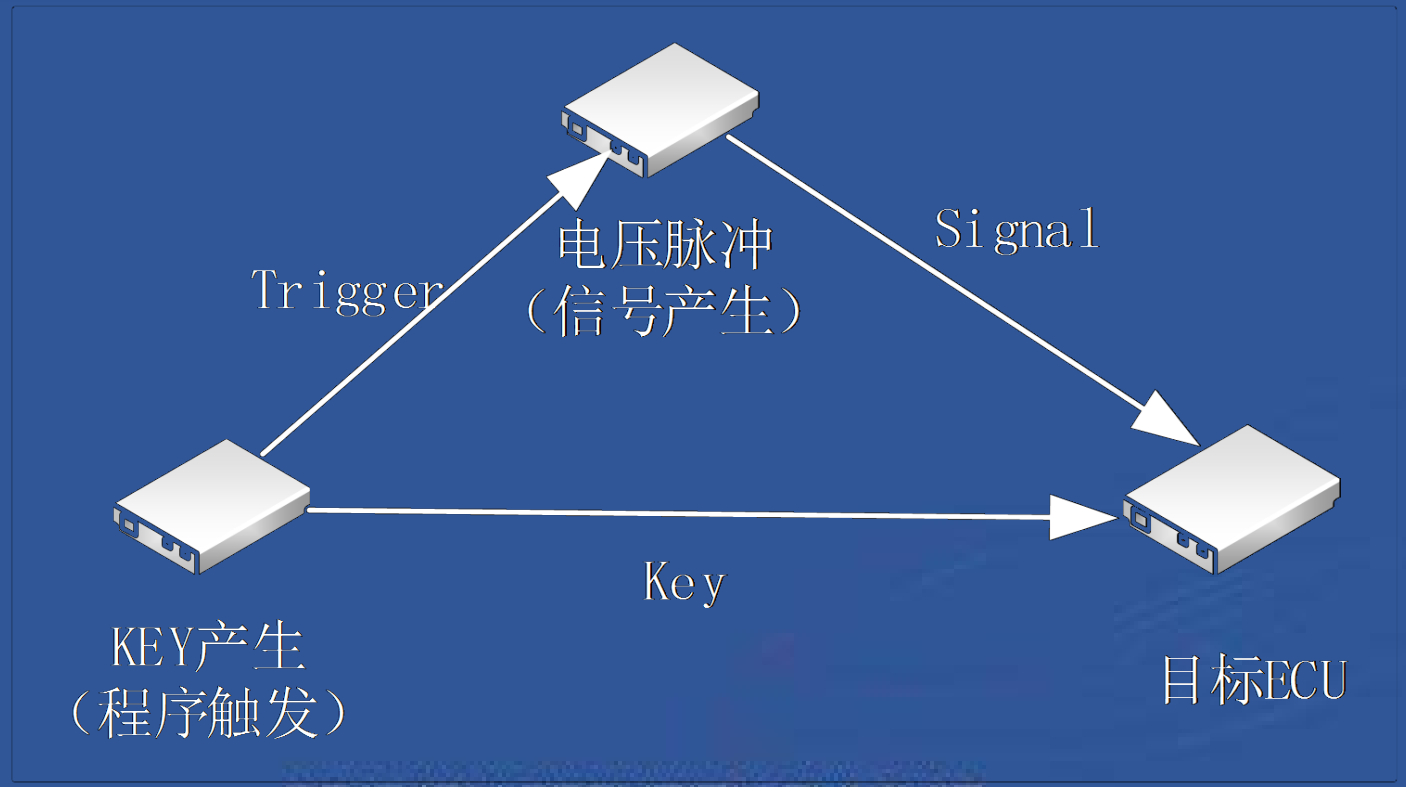
车联网安全技术研究

ECU安全研究

- 侵入式攻击
  - ·微探测
  - ·反向工程
- 半侵入式攻击
  - ·电压
  - ·时钟
  - ·数据剩磁

车联网安全技术研究

- 故障注入攻击——ECU认证



车联网安全技术研究

ECU安全研究

- 非侵入式攻击

·被动：

功耗分析，时序攻击

·主动

暴力攻击，脉冲注入

车联网安全技术研究

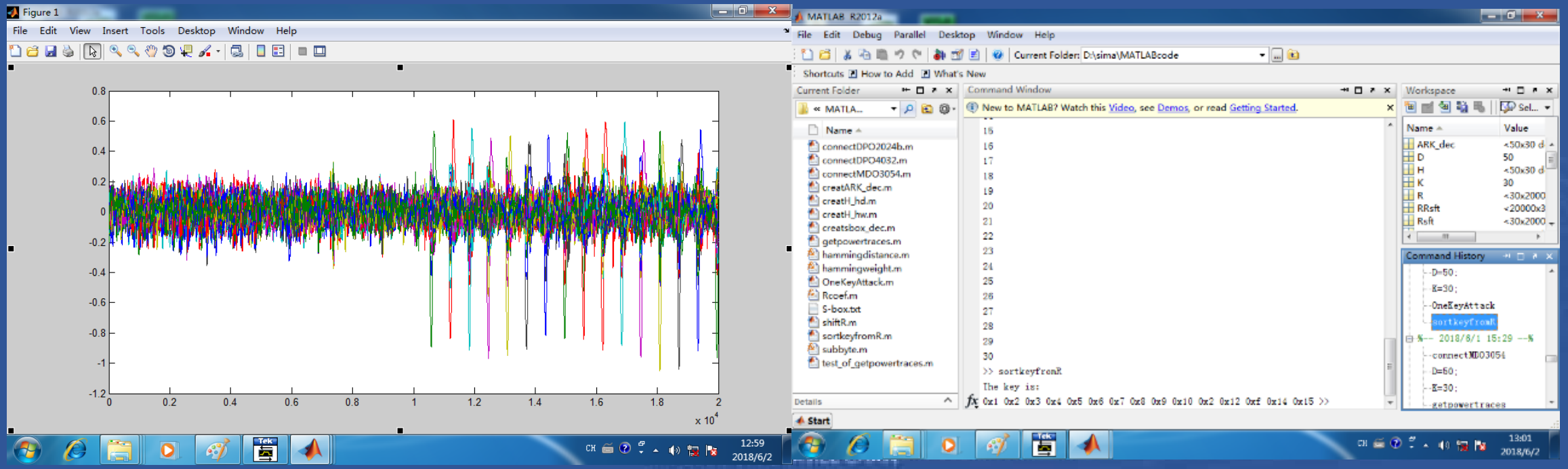
ECU安全研究

- 功耗分析平台

车联网安全技术研究

ECU安全研究

- 功耗分析平台



车联网安全技术研究

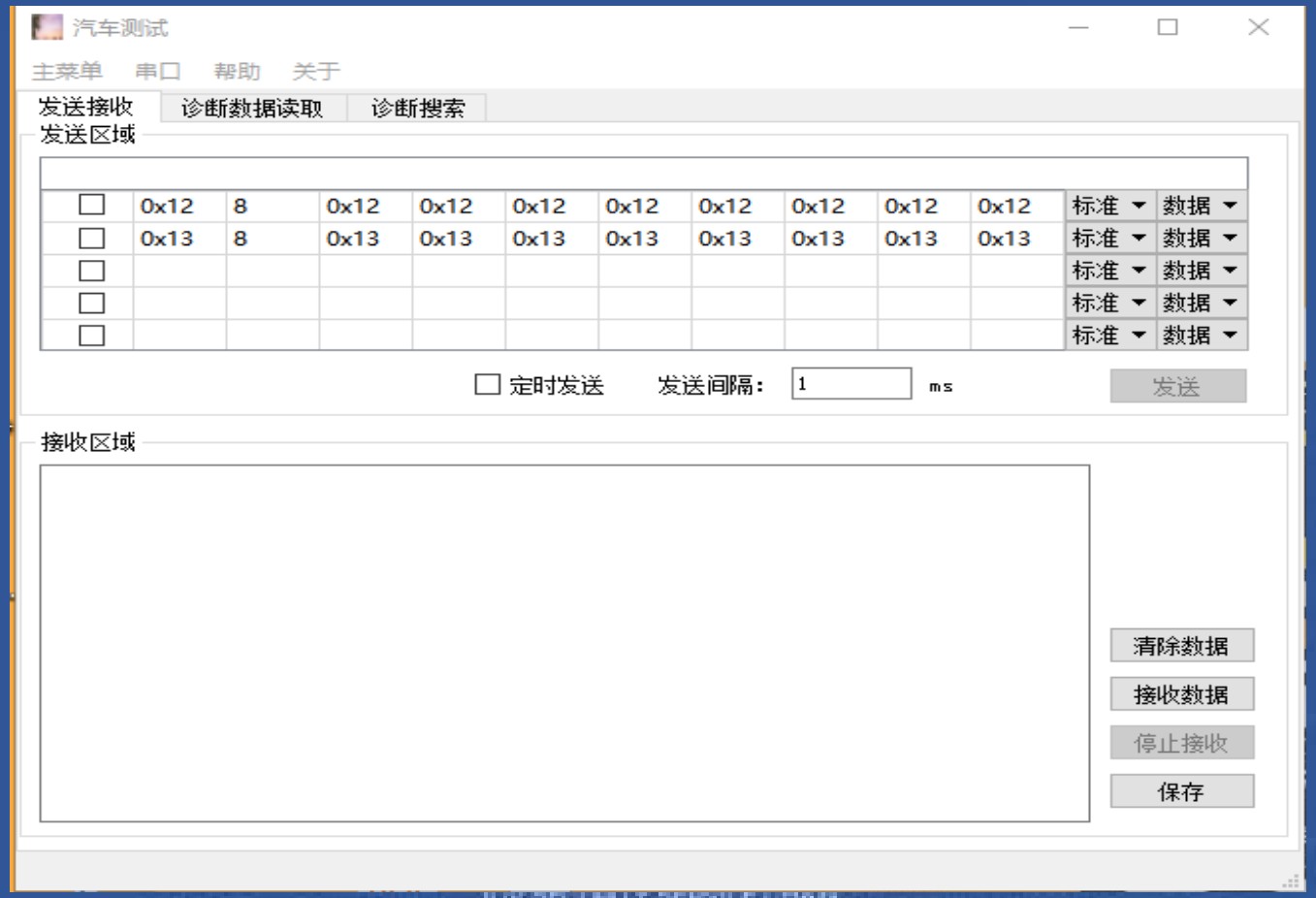
- CAN网络安全研究
  - 指令破解（正常数据包）
  - 诊断破解（诊断数据包）
  - 安全通信
  - 渗透测试
  - 模糊测试

车联网安全技术研究

- CAN网络安全特性
  - 无数据完整性检查
  - 数据未加密
  - 广播通信
  - 优先级仲裁机制

车联网安全技术研究

- CAN网络安全研究



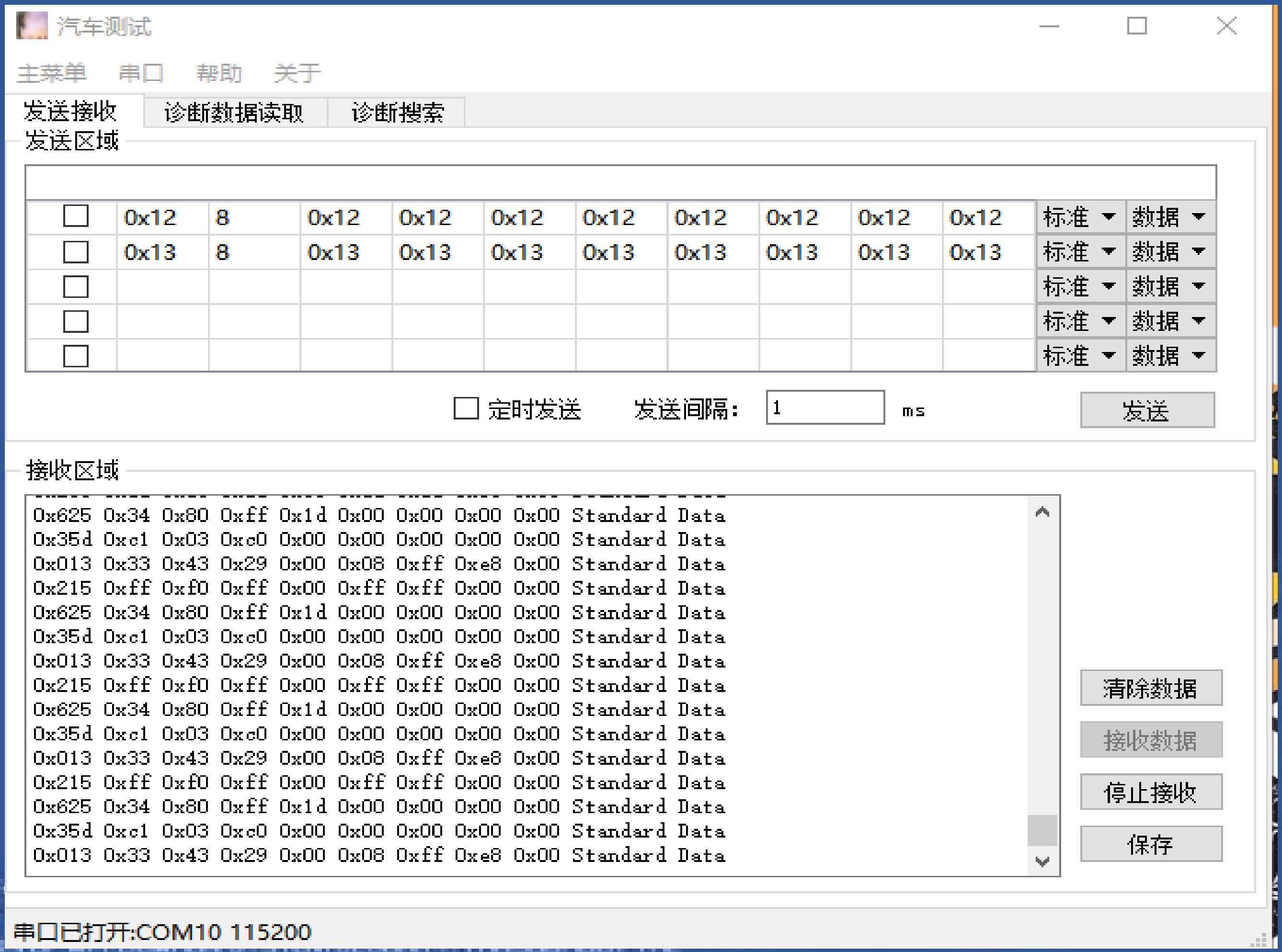
车联网安全技术研究

- CAN网络安全研究
  - 指令破解（正常数据包）
  - ·实现常见汽车指令的CAN数据逆向
  - ·配合DBC等文件实现一定程度的汽车控制

车联网安全技术研究

❖CAN网络安全研究

➢指令破解

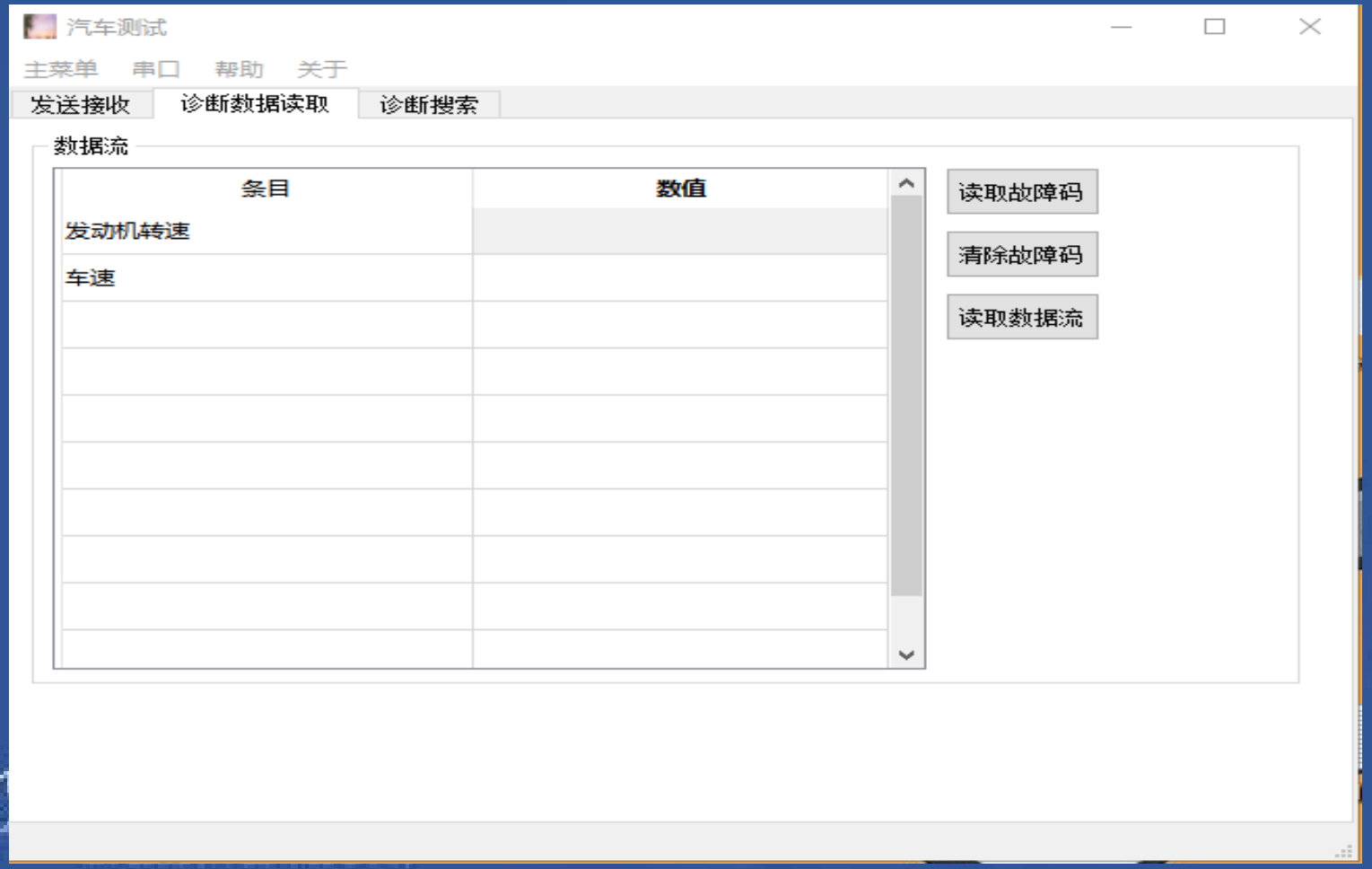


车联网安全技术研究

- CAN网络安全研究
  - ➢诊断数据破解（诊断数据包）
  - ·ECU扫描
  - ·诊断服务扫描
  - ·读取重放诊断数据

车联网安全技术研究

- CAN网络安全研究
  - 获取诊断数据



车联网安全技术研究

- CAN网络安全研究
  - 安全通信
  - ·算法破解
  - ·固件逆向
  - ·认证绕过

车联网安全技术研究

CAN网络安全研究

➢ 渗透测试

·黑盒/灰盒/白盒

·确定测试范围

·收集分析信息

·漏洞探测

·攻击测试

·分析报告及系统恢复

·访问受限文件

·改变受限文件

·读取传输数据

·控制网络及系统

·击破用户账号

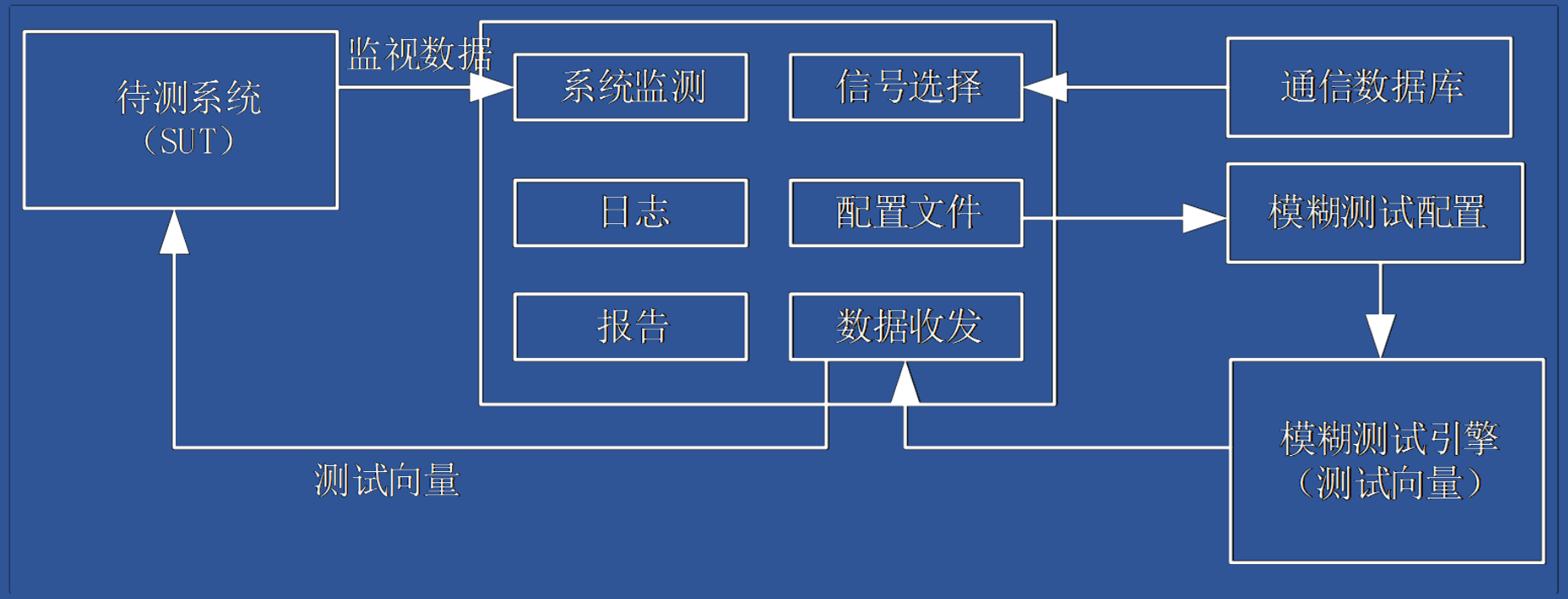
·超级权限

车联网安全技术研究

- CAN网络安全研究
  - 模糊测试
    - ·根据不同厂商动态化产生模糊测试用例
    - ·详尽监测汽车潜在的响应
    - ·高层协议支持

车联网安全技术研究

- CAN网络安全研究
  - 模糊测试框架



车联网安全技术研究

OTA安全研究

- 厂家发布固件到升级服务器
  - ·服务安全
  - ·对服务器的认证
- 汽车下载固件
  - ·通信安全加密
  - ·断点续传
  - ·防止固件知识产权泄露
- 汽车验证并升级固件
  - ·固件签名防止篡改
  - ·固件版本验证
  - ·固件加密
  - ·升级失败处理
  - ·ECU更换认证

车联网安全技术研究

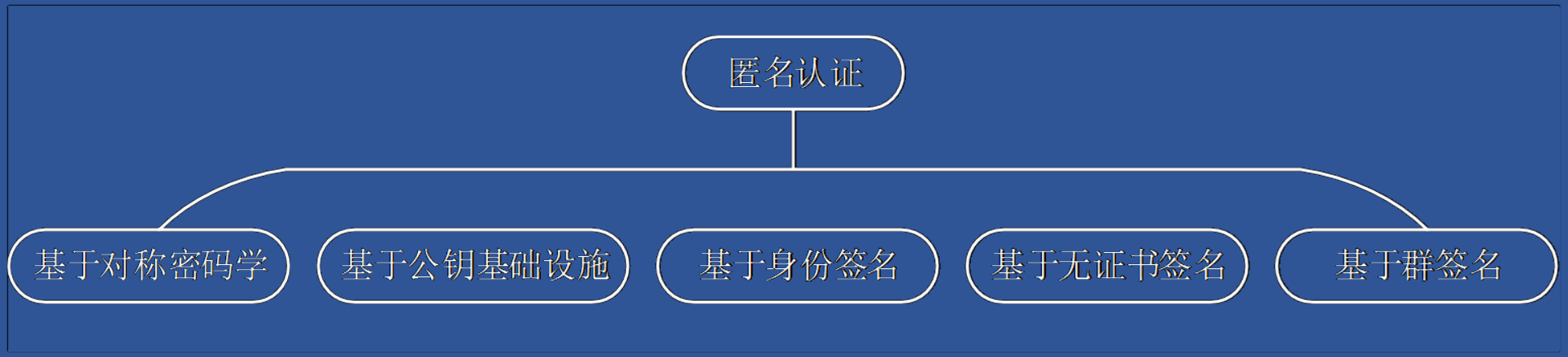
- 车联网隐私安全研究
  - 身份隐私保护
  - 位置隐私保护

车联网安全技术研究

- 车联网隐私问题产生原因
  - 广播的消息中含有大量隐私
  - 车辆运动轨迹可预测性

车联网安全技术研究

❖身份隐私保护方案



- ➢可信权威机构行为不透明
- ➢撤销列表开销大
- ➢认证效率低下

车联网安全技术研究

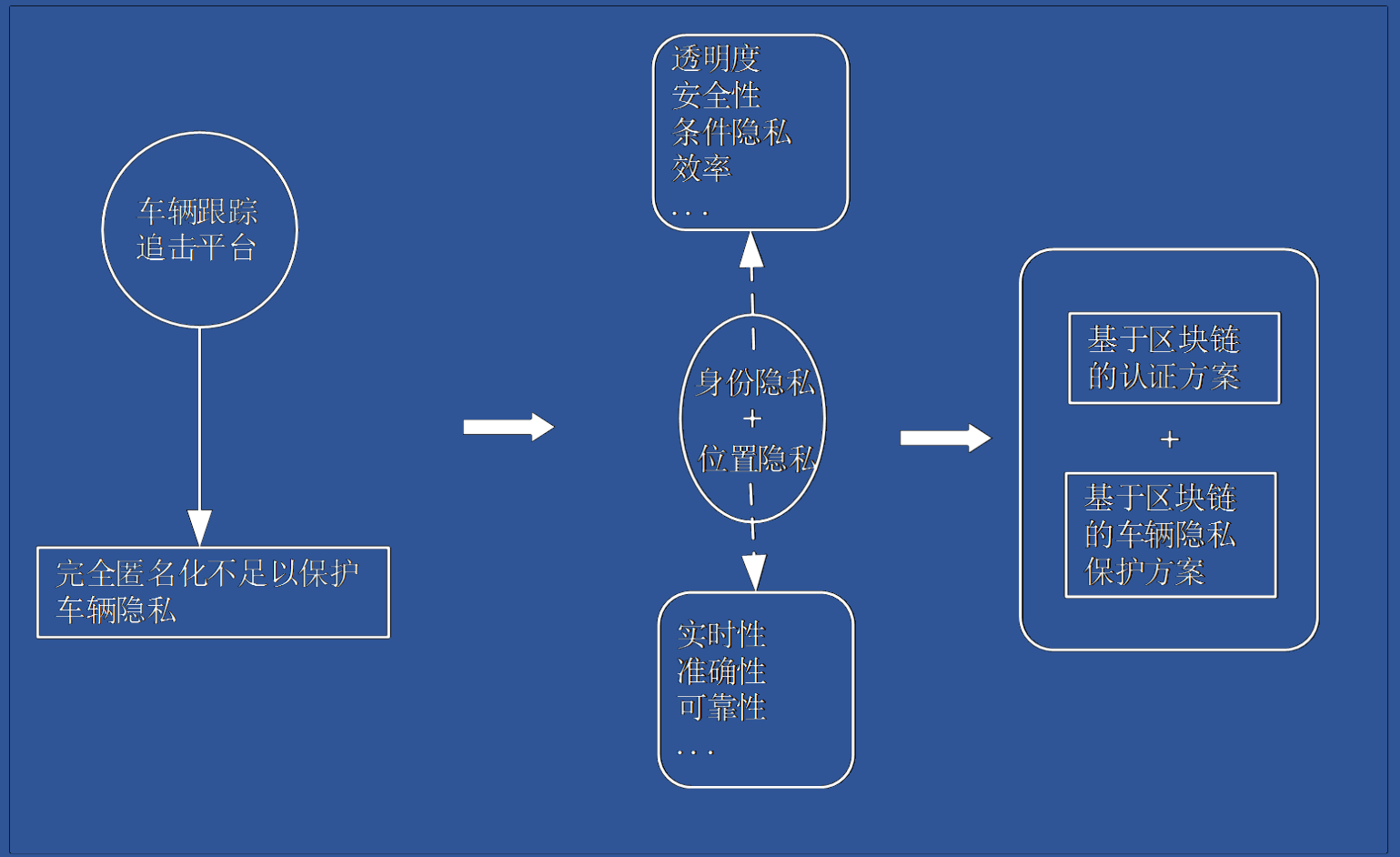
- 位置隐私保护方案
  - K-匿名方案
  - 混合区域方案
  - 基于模糊的方案

车联网安全技术研究

- 车联网隐私保护方案目标
  - 保护车辆身份隐私和位置隐私
  - 不能影响服务质量
  - 车辆隐私保护是有条件的

车联网安全技术研究

研究思路



4 车联网安全思考

- 测试与评估标准
- ECU与CAN总线
- 安全OTA
- 隐私保护

车联网安全思考

- 测试与评估标准
  - 科学的评估准则
  - 标准的测试流程
  - 丰富的测试用例

车联网安全思考

- ECU与CAN总线
  - 加密
  - 认证
  - 完整性检查

车联网安全思考

安全OTA

- 厂家发布固件到升级服务器

·服务安全

·对服务器的认证

- 汽车下载固件

·通信安全加密

·断点续传

·防止固件知识产权泄露

- 汽车验证并升级固件

·固件签名防止篡改

·固件版本验证

·固件加密

·升级失败处理

·ECU更换认证

车联网安全思考

- 隐私保护
  - 身份隐私保护
  - 位置隐私保护

谢 谢！