智能外设入侵汽车网络解密

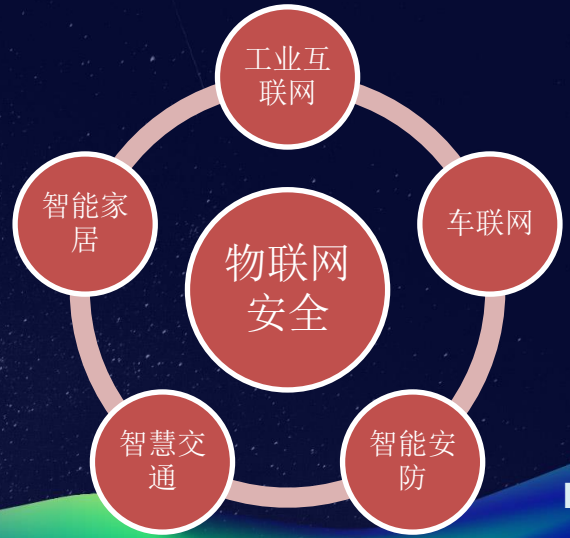
安恒安全研究院 海特实验室

About Me

安恒研究院海特实验室

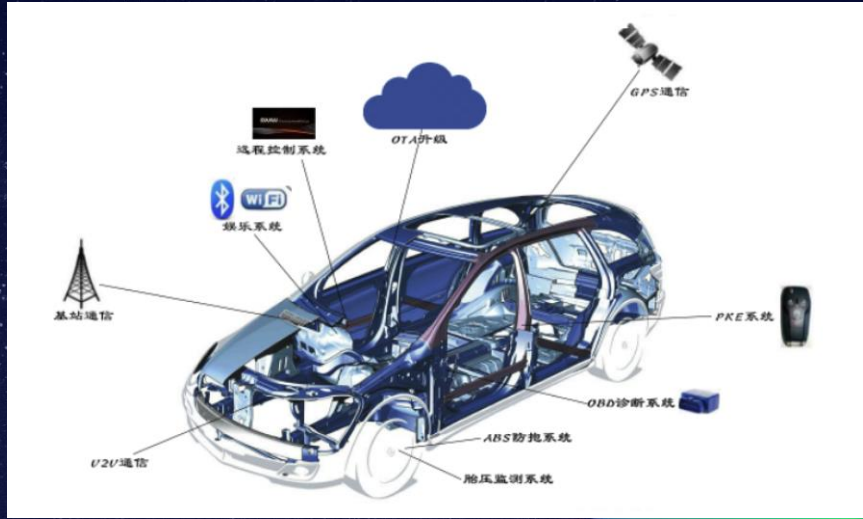
HATLAB

Hack AnyThing

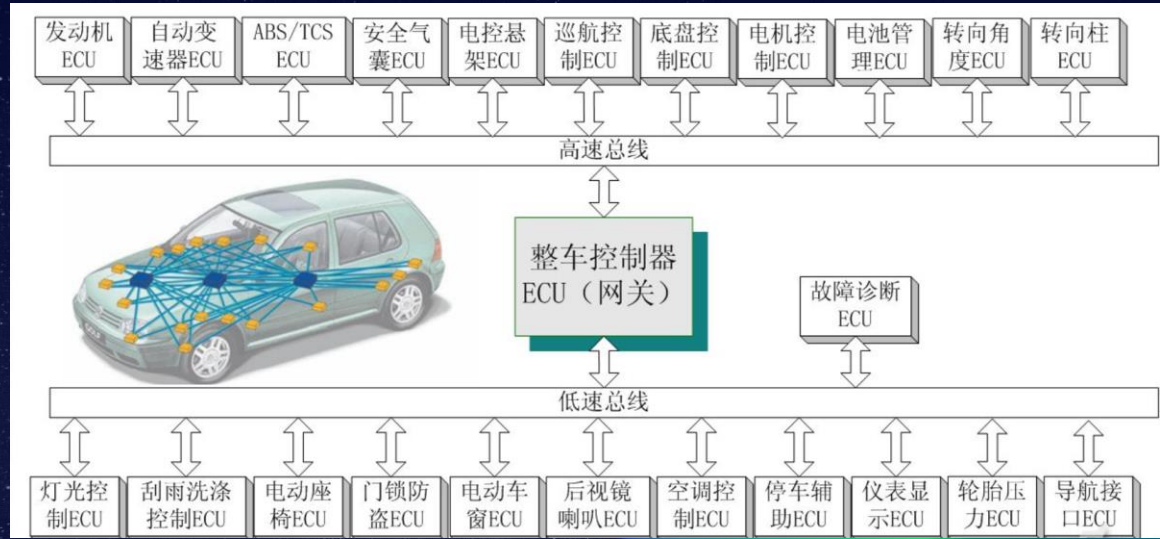


HACK DEMO

汽车的攻击面



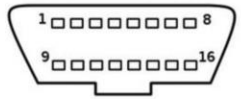
HACK DEMO


发动机ECU
自动变速器ECU
ABS/TCS ECU
安全气囊ECU
电控悬架ECU
巡航控制ECU
底盘控制ECU
电机控制ECU
电池管理ECU
转向角度ECU
转向柱ECU
高速总线
整车控制器ECU（网关）
故障诊断ECU
低速总线
灯光控制ECU
刮雨洗涤控制ECU
电动座椅ECU
门锁防盗ECU
电动车窗ECU
后视镜喇叭ECU
空调控制ECU
停车辅助ECU
仪表显示ECU
轮胎压力ECU
导航接口ECU

OBD接口

汽车 OBD-II 接口引脚定义

汽车上的 OBD-II 接口（母）：



ELM327 用到的引脚：

2: SAE-J1850 PWM 和 SAE-1850 VPW 总线(+)
4. 车身地
5. 信号地
6. CAN high (ISO 15765-4 和 SAE-J2284)
7. ISO 9141-2 和 ISO 14230-4 总线的 K 线
10. SAE-J1850 PWM 协议总线(-)(not SAE-1850 VPW)
Europe, etc. Chrysler CCD Bus(+)
14. CAN low (ISO 15765-4 和 SAE-J2284)
15. ISO 9141-2 和 ISO 14230-4 总线的 L 线
16. 蓄电池电压

OBD智能盒子

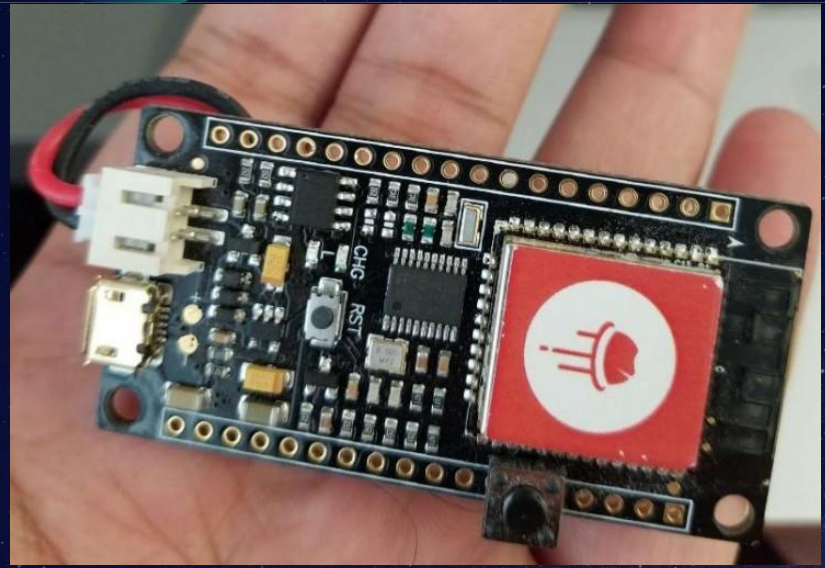
Q1 OBD智能盒子和OBD诊断接头分别是什么鬼？

实际上车厂给汽车装上这个OBD接口有两个原始目的，一是为了检测汽车，通过专用的检测设备来读取汽车电脑的数据，分析一个汽车的状态和故障；二是可以用于汽车排放标准的检测接口，因为OBD诊断接头可以输出一系列的发动机传感器数据，这些数据中的氧传感器，也可以分析发动机的燃烧效果。这个接口一般是修车店使用来检测车辆故障情况的。

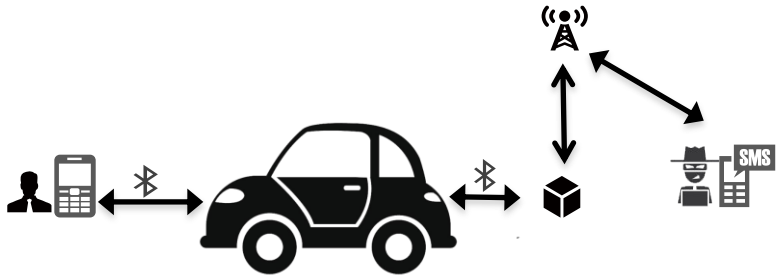
车上OBD接口位置

原始OBD诊断接头

OBD智能盒子攻击



攻击流程



Hack Demo!