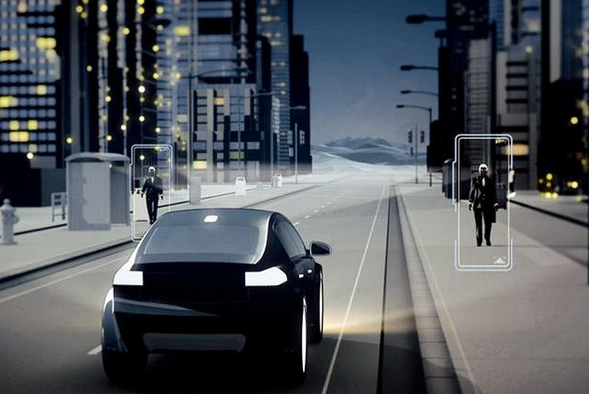
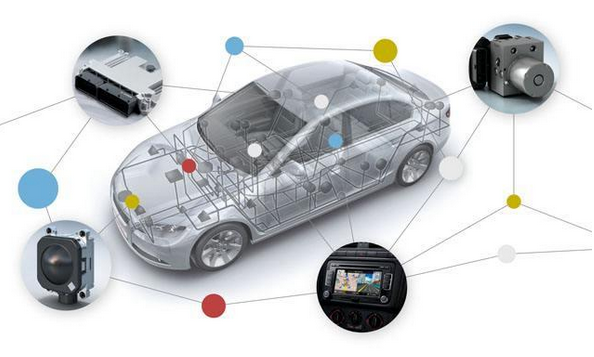
现在的汽车变得越来越聪明了，启用泊车系统则汽车可以自主寻找停车位，启用自适应巡航系统则汽车可自动调速跟车行驶，然而我们在享受汽车智能化带给我们便捷和舒适的同时，也面临智能汽车所带来的安全问题，那么智能汽车安全如何分类？黑客如何攻击智能汽车？车联网安全技术如何布局？  
  
1、智能汽车安全如何分类？  
智能汽车终极发展阶段是无人驾驶，车联网则是无人驾驶实现的基础，然而车联网技术应用过程中却会带来信息安全问题，具体可分为以下三种：  
其一，用户隐私  
汽车智能化是建立在车辆动态数据收集及应用上的，如车辆行驶、车体、动力、安全及环境数据等层面， 尤其是车辆行驶数据一直都被视为变现的大数据金矿，无论是车联网前装的车商，还是车联网后装的互联网科技公司，都在用户不知情的情况下收集车主驾驶历史数据，除了自用外，甚至还会商业变卖给第三方使用，由此造成用户隐私泄露危险（本文属于原创，猫视汽车首发，转载请注明）。  
其二，网络通信  
汽车智能化强度依赖于数字交通信号的传输，可能会面临接触设备故障、无网络覆盖及网络中断三大通信风险，接触设备故障指的是恶劣天气打坏车顶的传感器，或者是传感器无法识别积雪道路等；无网络覆盖指的是汽车进入山区或者遇到暴雨天气，通信网络覆盖及传输不到；网络中断指的是车载终端与远程云端通信时，因局部电源、信号导线等故障引发的临时性网络中断；  
其三，黑客攻击  
黑客攻击是媒体爆料最多的智能汽车安全风险，具体可分为接触式攻击、非接触性攻击和后装产品攻击三大类，常见的接触式攻击为OBD车辆诊断攻击；非接触式攻击则有云端服务攻击、TPMS攻击和无钥匙启动系统三种；后装产品攻击则是通过车辆下载互联网应用产品攻击，如WIFI网络、蓝牙、移动APP等软件应用  
2、黑客如何攻击智能汽车？  
黑客攻击智能汽车的危害最大，因为你无法想象在高速路行驶时，汽车转向系统及刹车系统突然失灵;你更无法想象车辆在没钥匙开门启动时，竟然被黑客开走;下面就和大家分享下黑客攻击智能汽车的技术（本文属于原创，猫视汽车首发，转载请注明）：  
其一，CANBus总线是攻击焦点  
CANBus全称为控制器局域网总线技术，有高速和低速之分，高速CANBus总线主要连接发动机控制单元、ABS控制单元、安全气囊控制单元、组合仪表等这些与汽车行驶直接相关的系统；而低速CANBus则主要连接像中控锁、电动门窗、后视镜、车内照明灯等对数据传输速率要求不高的车身舒适系统上；因为CANBus总线设计之初没有考虑到通讯安全因素，通常不需要身份验证也可以访问，因此一旦黑客攻破外围系统，实现与CANBus总线连接，就能实现对汽车的控制。  
其二，通过OBD入侵CANBus；  
黑客物理接触攻击都要通过OBD车载诊断系统，一般位于方向盘下方的前内饰板内，OBD作为汽车的对外接口，可以访问CANBus，因此通过专门的控制设备接入OBD端口，就可实现对车辆控制，甚至能修改一些行车电脑配置。  
其三，通过WIFI及蓝牙入侵CANBus；  
大部分厂商设置WIFI及蓝牙功能，是为了更好的连接移动设备来控制车载软件系统，如影音娱乐系统和无钥匙控制系统等，同时这些车载软件系统又能与CANBus总线交换数据，因此黑客可以通过破解WIFI及蓝牙密码，顺利入侵车内软件系统，进而入侵CANBus，从而实现对车辆控制；  
其四，通过云端、手机及APP入侵CANBus；  
当前很多车辆为了实现网络通讯，通常会设置云端服务、内置SIM卡及APP应用等软件系统，用以连接或与CANBus交换数据，因此黑客们一旦破解这些软件系统的登录名及登录密码，就可以访问CANBus，实现对车辆的远程控制。  
  
3、车联网安全技术如何布局？  
智能汽车最大安全隐患来自于黑客攻击，而黑客攻击重点是入侵CANBus总线，因此车联网安全技术核心就是围绕保护CANBus总线来展开，具体措施如下（本文属于原创，猫视汽车首发，转载请注明）：  
其一，车载终端设备安全  
车载终端设备分为车商前装设备和互联网智能后装设备，车商前装设备需要嵌入安全芯片，用以管理密钥和加密运算，进入整车厂的前装序列；互联网智能后装设备则需要隔离汽车底层，加硬件防火墙的方式，来保障车辆安全；  
其二，车联网运营端安全  
车联网运营平台分为云服务器端和移动APP端，车联网运营安全需要做到两点，首先是在云服务端配置安全产品和策略，加载了自主研发的密钥应用SDK，负责与车载端和移动终端加密往来数据；其次是在移动终端APP，对关键代码进行了动态加密和篡改识别，同时将移动终端设备、用户账号和信息、手机号码，通过数字证书技术进行绑定，确保移动终端的合法可靠性；  
其三，车联网通信安全  
车联网通信包括车辆内部网络通信和车辆外部网络通信两种，内部网络通信安全可采用防火墙与智能检测技术，实现车内娱乐、导航等系统与车机内网的安全隔离、访问控制及异常检测；外部网络通信安全则通过加强车与外界（V2X）的认证技术，减少来自外部的各种网络攻击。  
总结  
智能汽车给我们带来舒适和便利的同时，也面临着用户隐私泄露、网络通信及黑客攻击三大安全风险问题，其中黑客攻击智能汽车的技术核心，是通过OBD、车载系统、云服务平台及移动APP四种方式，入侵CANBus总线系统，来实现对汽车的控制;因此车联网安全技术应从车载终端、车联网运营端及车辆通信三个层面进行安全布局。