CSTC中国评测 见证质量 技术白皮书

智能网联汽车安全渗透白皮书（2020 年）

中国软件评测中心·智能网联汽车测评工程技术中心

2020 年 12 月

序　言

随着汽车智能化、网联化和电动化程度的不断提高，智能网联汽车信息安全问题日益严峻，产业链的各个环节对信息安全的重视程度还远没有达到要求，甚至存在多个环节并没有考虑信息安全需求的情况。因此全面推进智能网联汽车信息安全发展，定期进行安全渗透测试，积极探索信息安全关键技术和产品创新，进一步建立健全智能网联汽车信息安全防护体系至关重要。

为此，我们组织撰写了《智能网联汽车安全渗透白皮书（2020年）》，从产业发展、安全态势、攻击场景、渗透指标、渗透实践等切入点对智能网联汽车安全总体形势进行分析，提出安全渗透测试指标并基于此进行渗透实践，针对性剖析安全漏洞，提出安全保障建议。

本白皮书由智能网联汽车测评工程技术中心（赛迪汽车）团队撰写，参与人员包括邹博松、朱科屹、王卉捷、郭盈、王荣，在此特别感谢中国电子信息产业发展研究院副院长黄子河、副总工程师安晖、中国软件评测中心总工程师陈渌萍对本白皮书的撰写指导，中心品牌宣传推广部刘喜喜、闫晓丽的编辑及排版支持。

本白皮书的主要观点和内容仅代表编写组的研判和思考，部分内容难免存在纰漏，欢迎业界同仁提出宝贵意见，批评指正。

中国软件评测中心　宋娟

2020 年 12 月

版权声明

指导组：黄子河　　安　晖　　陈渌萍　　宋　娟

编写组：邹博松　　朱科屹　　王卉捷

　　郭　盈　　王　荣

目 录

前　言

近年来，智能网联汽车作为关联众多重点领域协同创新、构建新型交通运输体系的重要载体，已经上升到国家战略高度。发改委、工信部、交通运输部、科技部、公安部等部委加快出台一系列政策法规推动我国智能网联汽车产业发展，加强顶层设计和战略谋划。

本白皮书聚焦智能网联汽车信息安全问题，首先从安全产业的总体趋势、技术研究及政策法规等方面阐述智能网联汽车信息安全的发展现状；其次，对当前智能网联汽车信息安全总体态势进行分析；然后，从攻击场景入手，基于安全渗透指标进行渗透测试实践，进行重点问题分析；最后，提出智能网联汽车信息安全能力提升的相关建议。

中国软件评测中心（工业和信息化部软件与集成电路促进中心），是工业和信息化部的直属单位。长期服务和支撑国家部委、地方政府以及电信和互联网、汽车、教育、卫生、广电、交通、能源、银行、证券、保险、航空等各大行业，业务范围覆盖全国 31 个省、自治区、直辖市，业务网络覆盖全国 500 多个城市，构建了基于第三方服务的科技产业链。

智能网联汽车测评工程技术中心（赛迪汽车）是中国软件评测中心核心业务板块，依托于智能网联驾驶测试与评价工业和信息化部重点实验室及智能网联汽车软件检测中心，开展整车信息安全、V2X 安全、车载终端信息安全、电动汽车通信协议及数据格式一致性及安全、源代码安全等测评服务，以及标准政策解

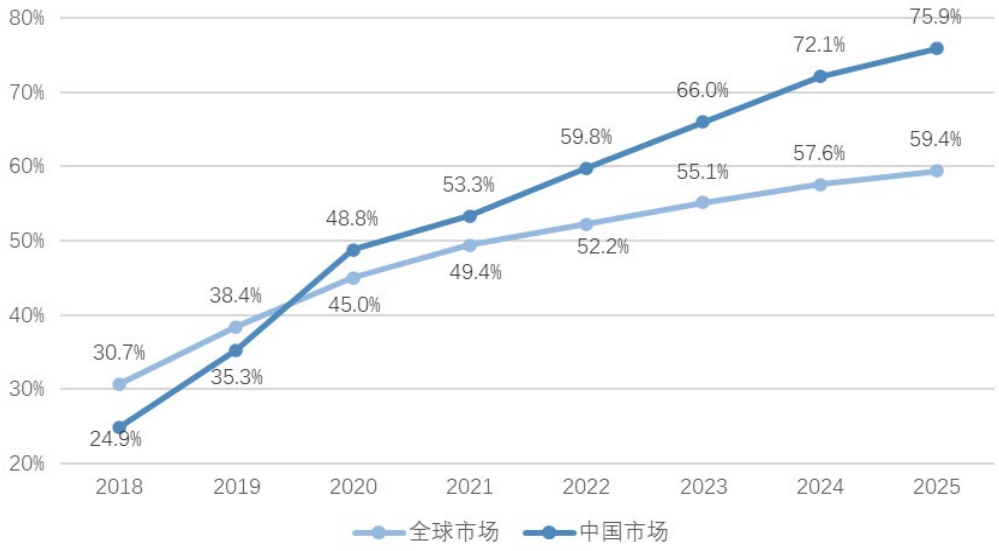
读、共性技术研究、产业发展规划等专业咨询服务。具备整车及零部件的功能、性能、可靠性、信息安全的综合测试与评价能力，致力于为政府部门、企业、科研院所等提供专业、安全、可靠的第三方咨询、测试、评估服务。

一、智能网联汽车安全产业概述

(一) 产业生态总体趋势

智能网联汽车市场规模预计将持续增长。在互联网多模式发展和工业智能化趋势的背景下，智能网联汽车作为创新发展的新方向，将汽车产业带入到多领域、大系统融合的高速发展时期，产业链各主体都在积极开展相关产业布局，汽车产业正在发生革命性变化。工业和信息化部部长肖亚庆在 2020 世界智能网联汽车大会上表示，随着汽车信息通讯、人工智能、互联网等行业深度融合，智能网联汽车已经进入技术快速演进、产业加速布局的新阶段。据 IHS Markit 数据显示，目前全球市场搭载车联网功能的新车渗透率约为 45%，预计至 2025 年可达到接近 60%的市场规模。长期预测中国的智能网联汽车市场将不断增长，至 2025 年接近 2000 万辆，市场渗透率超过 75%以上。

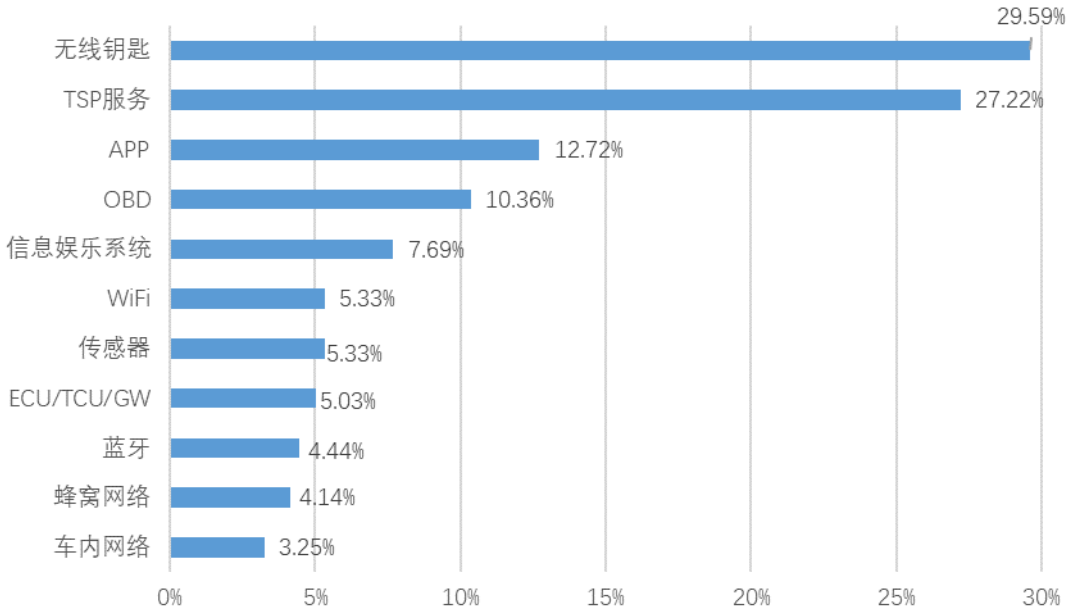
图 1：2018-2025 年智能网联汽车渗透率趋势



图片来源：IHS Markit 车联市场分析，2020 年

智能网联汽车信息安全问题日益严峻。一方面，2019 年上市的传统燃油车联网率超过 40%，预计 2020 年后将超过 70%，网络技术的普及和不断提升推动了智能网联汽车发展，汽车的联网率增加使得其逐步成为网络攻击重点目标，安全问题风险突出，安全防护基础薄弱。另一方面，根据工信部车联网动态监测情况显示，2020 年以来发现整车企业车联网信息服务提供商等相关企业和平台的恶意攻击达到 280 余万次，平台的漏洞、通信的劫持、隐私泄露等风险十分严重，危害更加严峻。威胁由车外进入车内、影响程度加大、网络安全与功能安全要求矛盾等问题层出不穷。

图 2：智能网联汽车信息安全事件统计



图片来源：Upstream Security，2020 年

(二) 安全技术研究现状

面对日益严峻的智能网联汽车信息安全问题，关键在于产业

链条上的各主体。智能网联汽车产业链长、防护界面众多，安全问题复杂，各主体探索建立车联网产业链信息安全分级分类管理模式，明确各自安全的要求也迫在眉睫。

整车企业、互联网企业和安全解决方案提供商纷纷布局汽车安全领域，推出特有的解决方案。整车企业携手网络安全公司，共建智能网联汽车安全实验室，合力推进汽车网络安全检测技术和防护技术的研发。互联网依托在传统 IT 领域的技术沉淀和积累，推出了安全芯片、安全操作系统、安全网关等产品。安全解决方案提供商则在汽车信息安全领域中投入大量测试类产品，通过对车辆自身特性以及网络传输协议的分析，实现对车辆信息安全测试的标准化、工具化、流程化，保障车辆不受外界攻击，提高车辆的安全防护能力。

2020 年信息安全十大风险分析了包括不安全的云端接口、未经授权的访问、系统存在的后门、不安全的车载通讯等在内的最常见、最危险的汽车信息安全漏洞。近期爆出的安全事件也显示，攻击者一旦利用安全漏洞，便可实现非法访问、敏感数据窃取、远程控制等操作，严重影响驾驶员的行车安全，甚至生命财产安全。为了避免更大的损失，各主体都开始强化在汽车信息安全方面的能力，例如针对现有车型可以开展渗透测试、漏洞挖掘等，依据分析结果和影响危害，设计防护方案以及创新安全技术。

(三) 标准政策法规动态

2017 年 9 月，国务院批准设立国家制造强国建设领导小组车联网产业发展专项委员会，将健全车联网安全管理制度和标准

体系、加强检测评估和安全保障等纳入车联网产业发展专项委员会重点工作任务。

2017 年起，工业和信息化部联合公安部、交通运输部、国家标准化管理委员会等部门制定《国家车联网产业标准体系建设指南》系列文件，指导通信、汽车等相关标准化技术委员会研究编制车联网网络安全标准体系框架。

2018 年 12 月，工业和信息化部制定实施《车联网(智能网联汽车)产业发展行动计划》，明确“强化管理、保障安全”的基本原则，围绕健全安全管理体系、提升安全防护能力、落实企业主体责任等方面，就车联网网络安全作出系统部署。

2020 年 2 月 24 日，发改委、工信部等 11 部委联合印发《智能汽车创新发展战略》文件指出“要严格落实国家网络安全法律法规和等级保护，完善智能汽车网络安全管理制度，建立覆盖汽车制造企业、电子零部件供应商、网络运营商、服务提供商等产业链关键环节的安全责任体系”。

2020 年 4 月 16 日，工信部发布《2020 年智能网联汽车标准化工作要点》提出，2020 年智能网联汽车标准化工作将以推动标准体系与产业需求对接协同、与技术发展相互支撑，建立国标、行标、团标协同配套新型标准体系为重点。目前，指导推进车联网信息服务平台防护、无线通信技术安全、数据安全、用户个人信息保护等多项国内标准报批发布，推动汽车网关安全、车载信息交互系统安全等国内标准研制，支持通信数据安全、异常行为检测、路侧单元安全、威胁信息共享框架等国际标准立项。

二、智能网联汽车信息安全态势

(一) 网络安全技术领域扩展，智能网联汽车成为新目标

随着云计算、大数据、车联网等创新技术的逐步应用，新形式网络安全威胁和风险正不断滋生、扩散和叠加。其中，汽车行业的产品、产业的智能化升级是典型代表。智能网联汽车作为搭载先进传感器等装置，融合云、网、路、端、人各要素，涉及信息通信、电子汽车交通等多行业、多领域、多主体，运用人工智能、自动驾驶等新技术的新一代产品，其网络安全问题呈现融合性、整体性特点。

智能化、网联化发展使得汽车面临的网络安全风险不断增大，相较传统互联网，因其应用环境更加特殊、组网更加复杂、管理更加困难，智能网联汽车面临的安全威胁也更加突出。**第一，车端威胁复杂。**智能网联汽车车端威胁主要涉及车载信息交互系统、车载诊断（OBD）接口、车载网关、车内网络等。车内多个存在攻击风险的脆弱点，引入了众多威胁场景。**第二，软件大规模应用。**软件重新定义汽车的趋势导致智能网联汽车车内代码量和复杂度激增，漏洞数量也随之增加，给了攻击者更多的可乘之机。**第三，与外部连通性增强。**车车通信、车路通信、车云通信和短距通信等车内外通信场景为攻击者提供了更多的攻击面，通信安全防护水平参差不齐也极大降低了攻击成本与难度。智能网联汽车功能的大幅增加，导致信息安全接入点和风险点不断暴露，逐渐成为攻击者目标。

(二) 产业价值体系正在构建，外部环境安全隐患突出

智能网联汽车产业已进入技术快速演进、产业加速布局的新阶段。近日，世界智能网联汽车大会发布了《智能网联汽车技术路线图 2.0》，目标到 2035 年智能网联汽车技术和产业体系全面建成，产业生态健全完善，整车智能化水平显著提升，网联式高度自动驾驶汽车大规模应用。新产品、新业态、新模式不断涌现，以智能网联汽车为载体的产业多样化服务伴随着大量信息资产的产生。

随着汽车与外部的互联互通程度不断增强，一旦攻击者利用高危漏洞，除了对本车及车主造成安全威胁，甚至还有可能蔓延至其他车辆，从中获取大量利益，甚至可能威胁公共安全乃至国家安全。近年来智能网联汽车信息安全事件频发，外部环境安全隐患日益突出。根据工信部数据统计，在 2019 年的专项调研、检测中发现，85%的关键部件存在着安全的漏洞，80%以上的车联网平台和 App 存在缺乏身份鉴别、数据明文存储等隐患，近六成企业缺乏自动化的网络安全监测响应能力。Upstream Security 的《2020 年汽车网络安全汇报》指出，汽车制造行业的互联网攻击快速提升，全行业遭遇的威胁愈来愈广泛。数据显示自 2016 年到 2020 年 1 月，汽车网络安全事件的年安全事故总数提升了 605％，仅在 2019 年就提升了一倍左右。按照目前的发展趋势，随着汽车联网率不断提升，安全问题会更加突出。

(三) 数据信息泄露风险加剧，个人信息保护不断加强

智能网联汽车的信息安全危机不仅能够造成个人隐私泄露、

企业经济损失、车毁人亡等严重后果，甚至上升成为国家公共安全问题。据统计，有56%的消费者表示信息安全和隐私保护将成为他们未来购买车辆时主要考虑的因素。由此可见，智能网联汽车信息安全已经成为汽车产业甚至社会关注的焦点。当前，正处于智能网联汽车发展关键时期，强化智能网联汽车的数据及个人信息安全保障已成为当务之急。

针对车联网数据安全和个人隐私保护，国家采取了一系列措施。**（一）法律法规方面，**加快构建数据安全法律体系，先后出台《网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》等法律法规，明确数据安全、数据跨境流动管理的基本原则和制度要求。2020年10月全国人大就《中华人民共和国个人信息保护法（草案）》征求意见。**（二）管理实践方面，**2019年，工信部印发的《关于做好2020年电信和互联网行业网络数据安全管理工作的通知》中明确提出，“将加强车联网等新领域网络数据安全管理列为年度重点工作之一，从贯标试点、项目遴选、评估检测等方面明确具体工作举措”。在关于政协十三届全国委员会第三次会议第1506号提案答复的函中表示“将面向5大类70余款车联网App开展安全评测，分析车联网用户个人信息在采集、存储、传输等环节存在的安全隐患”。**（三）标准制定方面，**围绕车联网数据分类分级、数据保护能力评估、数据脱敏等方面推进车联网数据安全标准化工作，2020年4月工信部发布《车联网信息服务 数据安全技术要求》《车联网信息服务 用户个人信息保护要求》标准草案，明确车联网数据安全管理和个人信息保护基线要求。

(四) 安全建设能力仍需完善，渗透测试服务不可或缺

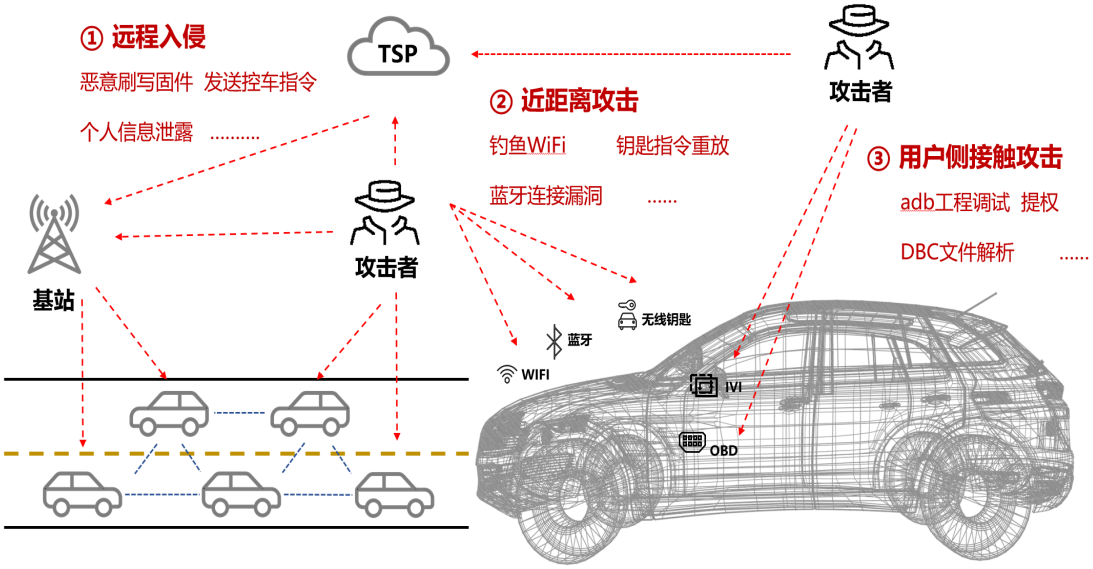
整车企业对信息安全的意识逐步提升，近年来已着手开始加强自身信息安全能力的建设。国内合资整车企业已经普遍建设完成自有的安全能力，自主品牌整车企业中的广汽集团、上汽集团、比亚迪、吉利集团、一汽集团等也都已经相继投入建设。而限于传统汽车行业与信息安全行业的理念与技术差异性，当前并没有一个完整的行业级智能网联汽车信息安全解决方案。智能网联汽车安全体系建设中涉及到的信息资产多，分布分散，管理难度大，当前离散化的建设机制难以及时响应威胁攻击。工业和信息化部网络安全管理局局长赵志国在 2020 中国汽车产业发展国际论坛上表示，从车联网企业网络安全实际看，产业链相关企业，特别是传统车企，网络安全意识不强，防护能力不足，安全投入不够等问题也比较突出。

受限于成本、技术成熟度等因素，整车企业网络安全测试评价基础薄弱，在车内部件、整车等方面测试验证能力不足，整车渗透还主要依赖于人工实施，渗透深度和水平缺乏可量化评估标准。2019 年 360 正式发布的《智能网联汽车信息安全年度报告》指出，整车企业应该遵循相关汽车网络安全系列标准，执行严格的供应链管理机制，定期进行渗透测试，持续监控网络安全风险。通过渗透测试整车企业可以从攻击角度了解车辆是否存在隐性漏洞和安全风险，有助于进一步健全安全建设体系。

三、智能网联汽车攻击场景分析

智能网联汽车安全典型攻击场景可大体分为远程入侵，短距离攻击，接触式攻击三大类。远程入侵场景中，攻击者可通过直连车辆或经过云端转发等方式恶意刷写车辆关键固件、发送控车指令、窃取个人敏感信息；近距离攻击场景中，攻击者可通过 WiFi、蓝牙、NFC 等通信方式，通过控车指令重放方式威胁用户车辆财产安全、使用未授权设备与车辆建立连接影响车内用户正常使用通信设备；接触式攻击场景中，攻击者通过攻入 IVI 工程模式，窃取车辆数据、分析车辆电子电气拓扑结构、捕获控车报文、解析车辆 DBC 文件等。

图 3：智能网联汽车典型攻击场景



(一) 工程模式入侵

IVI 是集成汽车中控台的智能多媒体设备，包括收音机、GPS 导航、娱乐、语音助手、蓝牙、WiFi 等功能。因为其附属功能多且集成度高，因而成为攻击者的重要目标。

攻击者通过 IVI 尝试打开系统工程模式，使用 adb 或 USB 等方式连接 IVI 系统；连接成功后，使用暴力破解等手段获取系统登录名及密码；登录成功后，尝试提权。

如上述操作顺利实现，则攻击者可访问 IVI 系统中任意文件，窃取个人隐私数据或密钥信息，篡改系统配置，启停车辆正常服务，注入恶意脚本。对车辆功能安全及信息安全造成严重威胁。

(二) 无线通信安全威胁

智能网联汽车无线通信方式包括蜂窝网络（4G/5G）、WiFi、蓝牙以及基于蜂窝移动通信环境下的 LTE-V2X 通信等。

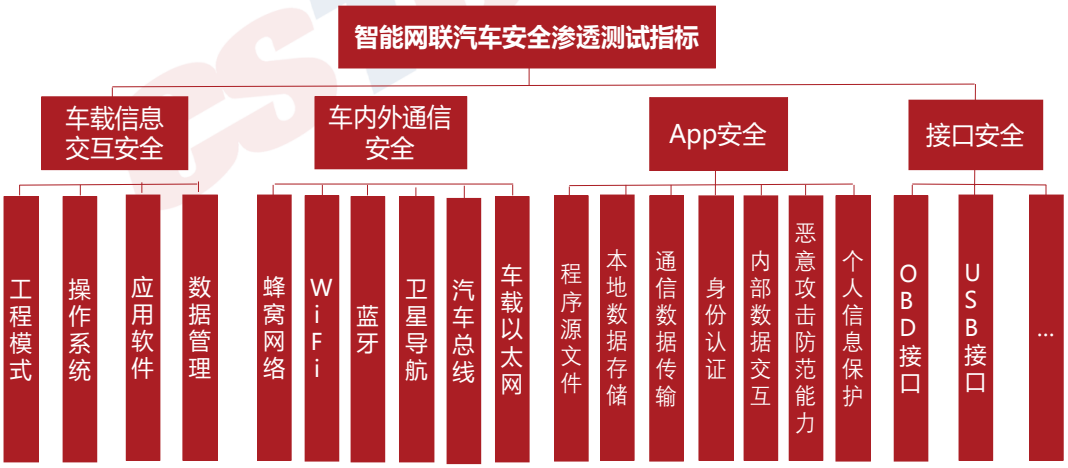
（1）蜂窝通信。攻击者可通过建立伪基站，利用 DNS 劫持等常规方式对 T-Box 会话及通信数据进行劫持、监听，实现对通信过程中敏感数据（如：用户信息、车辆状态信息）的窃取。**（2）WiFi 通信。**攻击者可通过对 WiFi 认证口令的破解，连接车内网络，对车辆敏感数据及隐私数据实现非授权获取。另外，还可通过结合操作系统已知漏洞的方式，对车辆进行组合式渗透攻击。**（3）蓝牙通信。**攻击者可利用劫持方式，拦截蓝牙钥匙与车辆之间的通信流量，篡改、重放恶意流量，造成车辆失窃，威胁车辆功能安全。

四、智能网联汽车安全渗透指标

中国软件评测中心参考 ISO/SAE-21434《道路车辆 信息安全工程》、20191065-T-339《汽车信息安全通用技术要求》、

20191069-T-339《车载信息交互系统信息安全技术要求》、GB/T 34975-2017《信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法应用》等国内外标准，结合攻击场景进行威胁分析，基于现有的渗透技术和汽车信息安全测试工具，寻找攻击路径。智能网联汽车的信息安全问题主要来源于汽车可以连接网络、与外界通信，成为网络中的节点。所以目前重点关注的攻击路径均围绕与汽车网联化相关的点展开。在不损坏车辆、不拆解车辆、黑盒测试的前提下，给出用户侧渗透测试指标，主要包括车载信息交互安全、车内外通信安全、接口安全、App 安全等方面。

图 4：渗透测试指标



(一) 车载信息交互系统安全

车载信息交互系统具备数据输入输出、计算处理、存储、通信等功能，可以采集车内相关的 ECU 数据并发送控制 ECU 的指令，集成定位、导航、娱乐等多种功能，是汽车网联化、接入移动互联网和车际网的重要子系统。侧重于车内信息娱乐的 IVI、

侧重于远程通信服务的 T-Box，都是典型的车载信息交互系统，二者还有融合的趋势。本文不严格限定车载信息交互系统的边界，而将其视为连接车内网与车外网，实现信息交互的抽象节点。

车载信息交互系统存在的远程攻击面，比车上其它任何组件都要丰富。作为内外交通的咽喉要道，安全攻防的必争之地，车载信息交互系统安全无论对整车企业还是用户都具有直接的现实意义。车载信息交互系统主要从工程模式、操作系统、应用软件、数据存储等方面进行测试：工程模式包括工程模式入口、安全认证机制、口令强弱检测，调试模式安全认证等指标；操作系统包括权限管理、系统参数设置等指标；应用软件安全包括语音助手身份校验、应用软件劫持篡改、软件升级安全等指标；数据管理包括日志管理、密钥信息管理、用户信息管理等指标。

(二) 车内外通信安全

车内外通信主要指智能网联汽车具备对外通过蜂窝网络（4G/5G）、WiFi、蓝牙、卫星导航等方式与互联网中其他节点建立连接进行数据交换的功能。车内电子电气通过 CAN、LIN、MOST、Flex Ray 等汽车总线协议、车载以太网协议进行信息采集、数据传递与指令下发。车内外通信安全要求通过采用安全协议、完整性校验、身份认证、访问控制等措施，抵御报文破解、中间人攻击、重放攻击、拒绝服务攻击、报文篡改等威胁，实现车辆与其他节点的安全通信。

车外通信主要测试指标包括基于蜂窝网络通信的伪基站识别、通信内容加密传输，基于 WiFi 的通信内容监听、流量劫持、

信息重放、数据包篡改、钓鱼 WiFi 识别等，基于蓝牙通信的身份鉴别、协议安全，基于卫星导航的信号干扰等。车内通信主要测试指标包括车内通信数据监听、DBC 文件解析等。

(三) 接口安全

接口安全主要是指智能网联汽车接触式通信接口，如 OBD 接口、USB 接口等的安全。攻击者可通过植入恶意软件、监听车内数据、非法访问文件等手段分析车辆信息及运行逻辑，进一步入侵车内系统，窃取车辆数据或修改车辆关键控制系统参数等。

接触式攻击是最直接有效的接口攻击方式。OBD 接口安全测试指标主要包括数据监听、UDS 安全认证机制：数据监听指查看和验证 OBD 接口输出的数据是否包含重要指令、是否可以获取动力 CAN 数据；若可监听到数据，便进一步验证 UDS 诊断是否有安全认证机制。USB 接口安全测试指标主要包括设备认证、权限控制等：设备认证主要是指 USB 接口是否可识别 U 盘、鼠标、键盘等输入设备；若可识别，便继续验证是否可以安装 U 盘中的恶意软件或复制文件到 U 盘。

(四) App 安全

智能网联汽车相关的移动终端 App 按照用途可大致分为车控类、查询类、服务类，本文重点关注车控类 App 安全。车控类 App 需与车辆绑定，为用户提供控车功能，主要包括远程开关锁、车辆启动、空调启动、座椅调节、车窗开关、车灯开闭、

后备箱开关、除霜、鸣笛、泊车，同时还支持用户获取行车数据、车辆油量（电量）等信息。

车控类 App 往往直接与车辆直接绑定，对其分析可获得高价值线索。目前，智能网联汽车 App 还处于“附属品”的阶段，防护强度不高，呈现包含高价值信息、攻击难度较小等特点，易于自动化执行，容易成为注重性价比的攻击者的首选目标。App 安全主要基于移动应用安全检测平台，从程序源文件、本地数据存储、通信数据传输、身份认证、内部数据交互、恶意攻击防范能力、个人信息保护等方面进行检测；同时结合人工进行逆向分析，检查代码逻辑、数据内容、通信内容等。

五、智能网联汽车渗透实践聚焦

为了贯彻落实《中华人民共和国网络安全法》，推动智能网联汽车信息安全发展，赛迪汽车在全国范围内启动了智能网联汽车渗透测试工作。随机选取 10 辆目前在售车型进行渗透测试。被测车辆覆盖传统车企和造车新势力产品，其中新能源车 6 辆，燃油车 4 辆。具体信息如下:

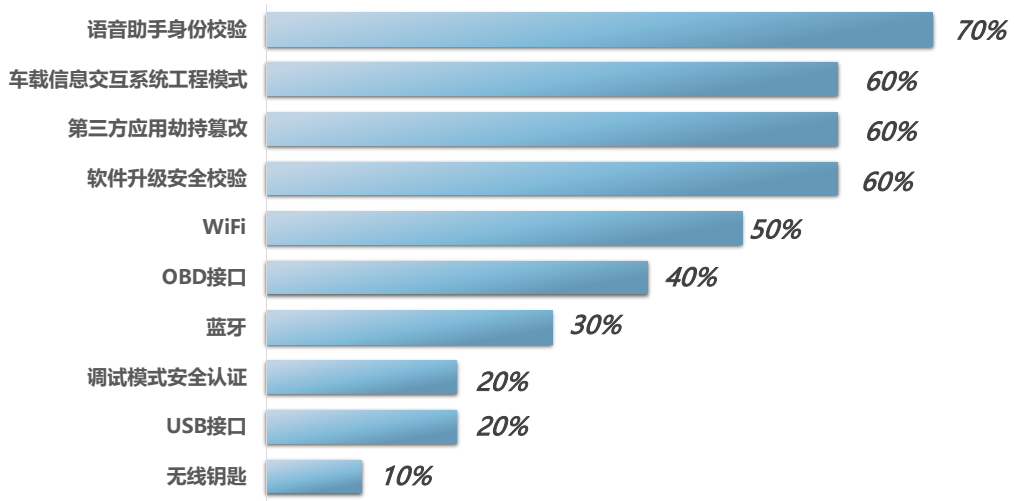
表 1：被测车辆信息

车企	车型
奇瑞汽车股份有限公司	小蚂蚁 EQ1
威马智慧出行科技(上海)股份有限公司	EX5
长城股份有限公司	VV6
广州汽车集团股份有限公司	传祺 GS8
浙江合众新能源汽车有限公司	哪吒 U
北京现代汽车有限公司	索纳塔 10

车企	车型
北京新能源汽车股份有限公司	ARCFOX 极狐
零跑汽车有限公司	S01
华晨汽车集团控股有限公司	中华 V7
重庆长安汽车股份有限公司	逸动

测试过程中，发现的典型问题包括语音助手未进行身份校验，车载信息交互系统工程模式易进入、可以获取调试权限，第三方应用与服务器通信内容易被劫持篡改，软件升级未进行校验，无线网络通信内容可被监听，OBD 接口可以获取报文，蓝牙连接未进行认证，USB 接口可以进行调试，无线钥匙可以重放等，以上问题检出率情况如下图所示：

图 5：典型问题检出率



结合渗透实践结果，聚焦目前智能网联汽车信息安全中检出率高、影响严重的问题进行重点分析。

(一) 系统调试模式开启

测试内容：尝试是否可以在 IVI 交互界面进入工程模式，进

入工程模式后通过 adb 或 USB 等方式成功连接 IVI 查看是否有安全验证机制；若有，使用暴力破解等手段获取系统登录名及密码；登录成功后，尝试取得系统 root 权限。

测试结果：在本次渗透测试过程中，发现有 60%的被测车辆可以触发进入工程模式，其中 66.6%的车辆进入 IVI 工程模式没有安全认证，可以直接提权（root），获取调试权限（见图 6）；33.4%进入工程模式时需要口令，但是口令易破解，同样可以获得调试权限。

图 6：获取调试权限

问题分析：获取调试权限后，可以查看 IVI 系统运行信息、系统文件、日志文件、用户信息等；可以注入恶意程序，恶意刷写固件，影响车辆功能；可以篡改系统配置，启停系统服务，导致系统功能失效；可以获取密钥，解密 IVI 与 TSP 平台通信内容，分析业务逻辑，进一步获取车辆控制权。

防护建议：上市前对 IVI 系统进行安全扫描、关闭调试模式，隐藏工程模式入口，部署多种独立安全机制形成多层次防护体系。

(二) 敏感数据明文存储

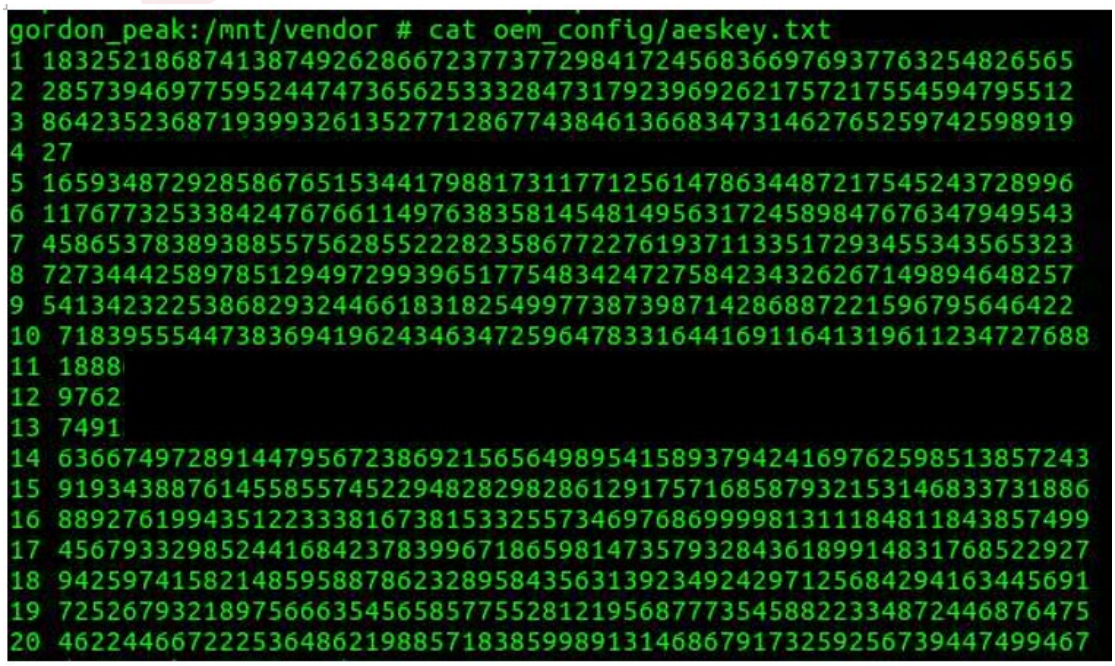
测试内容：通过进入车载信息交互系统工程模式，搜索、查看系统运行信息、系统配置文件、日志文件、用户信息等敏感数

据；尝试读写关键系统文件、导出关键信息。

测试结果：在本次渗透测试过程中，发现部分被测车辆明文存储用户及车辆敏感数据，且存储路径存在暴露风险。如：私钥、语音助手对话日志、用户通讯录信息等。进一步提权后，可对敏感数据进行读写、复制、导出、删除等操作。

问题分析：当前技术背景下，智能网联汽车的软件升级，绝大多数依赖于车载信息交互系统作为车辆的边界节点，即云端将软件升级包通过该节点转发至车内其他部件，因此妥善管理密钥成为安全设计的必要环节。一般情况下密钥会妥善存储于安全芯片或系统内部。本次测试过程中，发现存储在 IVI 系统中的密钥明文存储（见图 7）。攻击者利用密钥可打包任意内容的伪造升级包；通过云端批量刷入控车脚本至用户车辆，导致“僵尸车”的出现。

图 7：整车企业密钥明文存储



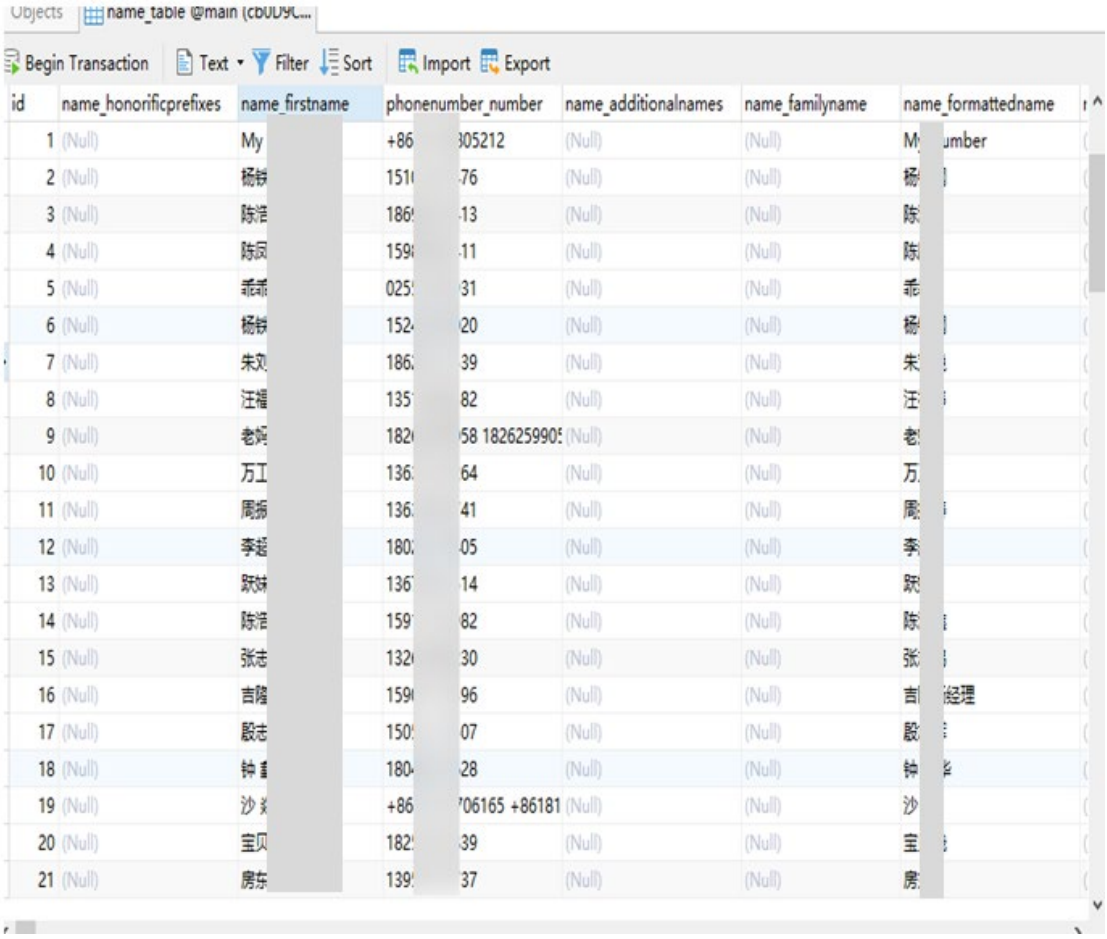
根据语音助手日志判断，车辆的语音助手被激活后，在非授

权条件下录制车内所有连续的语音内容，并将录制的语音内容上传到服务器，经服务器解析转换为文本后，下发至车载信息交互系统并明文存储（见图 8）。通过语音助手记录车内对话信息易造成个人重要信息被监听、上传及泄露等风险。在数据安全被高度重视的时代，汽车数据安全不仅关乎个人信息安全，更会危害社会公共安全，乃至上升到国家安全层面。

图 8：明文存储语音助手对话内容

另外，在测试过程中还发现部分车辆在 IVI 中明文存储用户的通讯录信息，包括姓名、联系电话等。并未对其使用人员进行最小权限的限制，被他人获取后可以刻画用户画像，进一步对用户造成严重影响。

图 9：明文存储用户通讯录



防护建议：密钥等关键数据存储于安全芯片或系统内部加密存储区域；个人信息在采集、传输、存储、删除时需得到用户授权；关键信息加密存储；车辆量产前关闭非必要日志功能。

(三) 应用软件通信内容劫持

测试内容：通过流量监听工具捕获车载信息交互系统与服务器通信的流量，查看通信内容是否可以被劫持；若可劫持，分析其业务逻辑，篡改通信内容并重发，实现中间人攻击。

测试结果：在本次渗透测试过程中，可以劫持 60%被测车辆

与服务器间的通信流量，分析通信内容（见图 10）并找到服务器地址，编写脚本伪造服务器，将篡改后内容重发至车载信息交互系统（见图 11）。

图 10：劫持通信内容

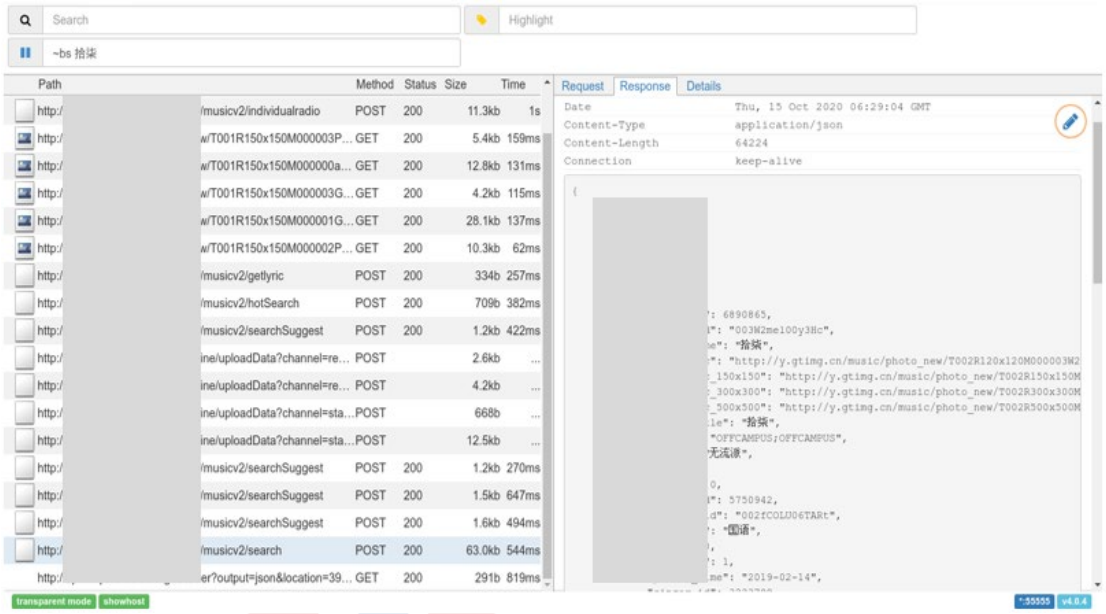


图 11：篡改通信内容

问题分析：目前车载信息交互系统中应用软件不仅包括系统自带的应用软件，还包括大量的第三方应用，应用环境复杂且难以管理，由此也带来了各种各样的攻击入口。一旦关键核心业务，如 TSP 平台给车辆下发的控车指令被监听，实现中间人攻击后便可伪造服务器端给车辆发送指令，远程控制车辆，造成极大安全隐患。

防护建议：加密关键应用软件通信内容，传输采用安全的通信协议等。

(四) 车内外通信未加密

测试内容：利用流量监听工具，捕获车载信息交互系统与外部服务器及内部设备的通信流量，查看通信内容是否可以分析。

测试结果：在本次渗透测试过程中，有 60%的被测车辆可以监听车载信息交互系统与外部服务器以及内部设备的通信流量；其中存在超过半数的车辆未对传输内容加密，采用明文进行传输。

问题分析：测试过程中发现，部分车辆的车载信息交互系统与外部服务器明文通信，传输 VIN、密码等敏感信息（见图 12）；部分车辆的车载信息交互系统与内部设备之间明文传输 CAN 报文相关的敏感信息（见图 13）；更有甚者，与 CAN 直接相连并明文通信（见图 14），尝试给该 CAN 接口发送数据可导致其无法再使用。

图 12：与外部服务器明文通信

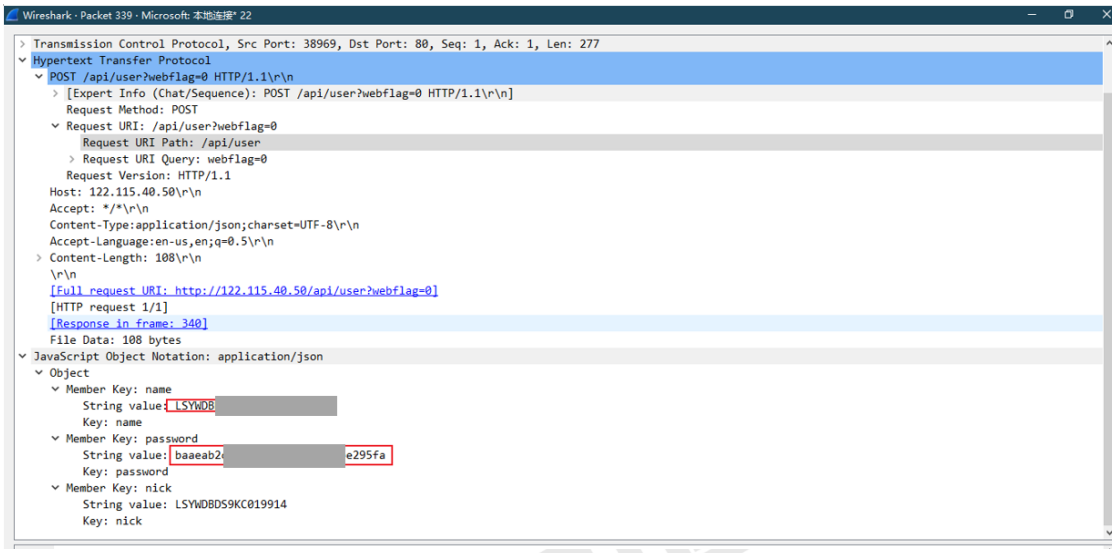
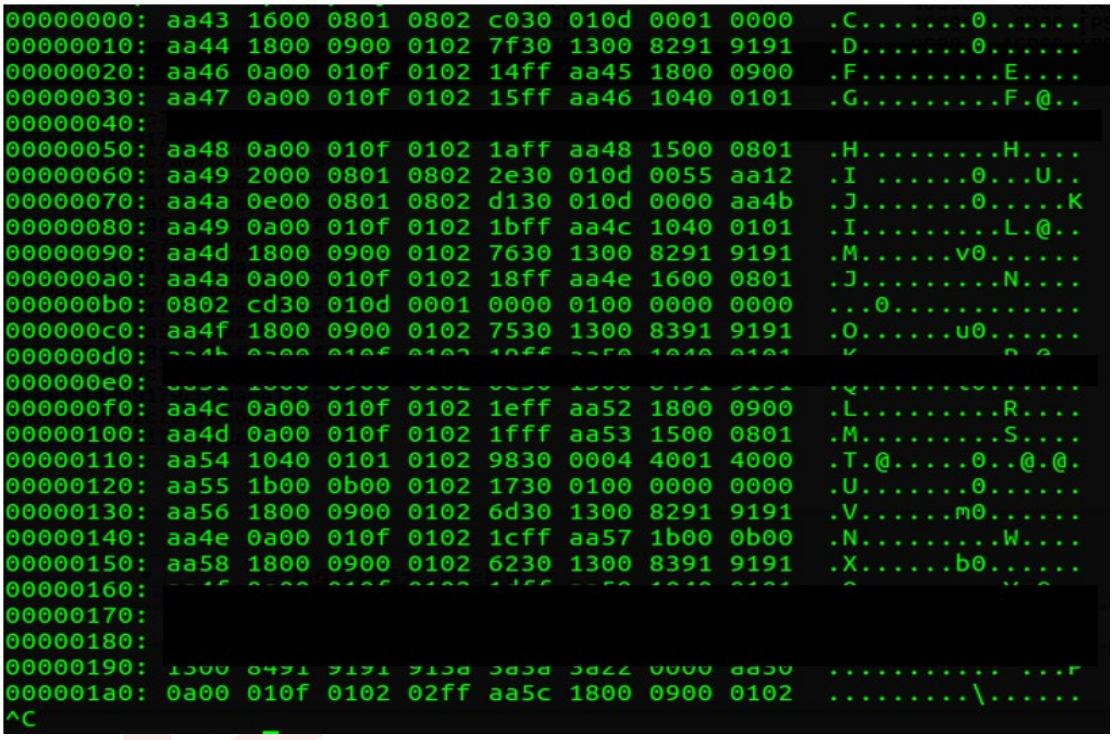


图 13：与内部设备明文通信

图 14：与 CAN 直接通信



防护建议：根据场景，采用安全的通信协议、身份认证、完整性校验、访问控制等措施，抵御重放攻击、拒绝服务攻击、报文篡改等威胁，实现车内外通信数据保密性、完整性及可用性。

(五) 蓝牙连接认证机制薄弱

测试内容：查看蓝牙功能的设置页面，默认连接认证功能是否开启，并尝试连接车辆蓝牙，验证蓝牙连接方式是否安全；通过测试工具监听、捕获蓝牙流量。

测试结果：在本次渗透测试过程中，有 30%的被测车辆在外界移动设备连接车辆蓝牙时无需进行认证便可直接连接，实现影响车内正常使用蓝牙功能：例如断开合法用户正常连接，向车内

发送垃圾语音信息等。

问题分析：在本次测试过程中，部分车型蓝牙配对未设置口令或使用弱口令进行安全认证；未实现用户级认证，即应用级安全性，可由开发人员通过在标准蓝牙规范之上叠加一层实现。

防护建议：将蓝牙设备的功率水平设置为最低程度，使信号传输保持在安全边界内；PIN 码应具备随机性和隐私性，避免静态和弱 PIN 码，如全零；敏感数据，可考虑在蓝牙协议栈之上使用应用级的认证及加密。

(六) OBD 数据监听

测试内容：通过工具监听 OBD 接口输出的数据，验证监听数据是否包含重要指令、是否可以获取动力 CAN 数据。

测试结果：在本次渗透测试过程中，40%的被测车辆 OBD 口可以监听到数据，其中 50%可以通过开关灯、启动停止车辆等操作判断 CAN 报文内容。

问题分析：经测试发现，部分车辆诊断网关对 CAN 总线的防护能力较弱。在 OBD 接口上能够监听到车门解锁、熄火、开关灯等操作的 CAN 报文。通过分析找到了几组指令能实现对车辆的操控。如车辆上锁后，从 OBD 发送 ID 为 112，数据为 XX AE XX XX 39 E4 的 CAN 报文能够解锁车辆车门。从 OBD 发送 ID 为 11F，数据为 XX F8 F9 XX F1 XX 30 FF 或 XX 8B XX F9 FF XX 77 XX FF 的 CAN 报文能够关闭发动机机引擎。

防护建议：静默 OBD 接口数据，关键总线数据进行隔离。

(七) USB 外接设备及调试模式

测试内容：验证 USB 接口插入 U 盘、鼠标、键盘等外接设备，是否可识别；如果可识别，继续验证外接设备是否可以操作车载信息交互系统；是否可以在非授权条件下安装 U 盘中的恶意软件或将系统中文件复制到 U 盘。

测试结果：在本次渗透测试过程中，20%的被测车辆未限制 UBS 接口连接外接设备，部分车型接入 UBS 外接设备后，可以通过键盘执行截屏、声音加减、黑屏等操作。可以把存放恶意软件的 U 盘接入目标系统，并且运行恶意软件。

问题分析：部分车型的车载信息交互系统搭载 Android 操作系统。由于 Android 操作系统某些版本默认开启 USB 调试模式，如 Android 4.x.x 操作系统，从车载信息交互工程模式进入后发现调试模式默认开启（见图 15），使用 USB 接口连接 PC 后可以进行调试。

防护建议：建议车辆将 USB 接口切换至 device 模式，限制 USB 外接鼠标、键盘等设备。避免 USB 接口处于 host 模式下，并且禁止开启 USB 调式模式。

图 15：USB 调试默认开启

六、永不过时的安全建议

现如今，在互联网时代下的任何行业对于信息安全的基本要求，无论是在团队建设层面、流程管理层面还是技术要求层面，永远都不会过时，智能网联汽车行业也不例外。

组建信息安全团队，明确各主体细分职责。目前很多车联网企业，包括产品服务供应商还没有实现建立专职的技术团队负责设计、实施、运维智能网联汽车信息安全。做到信息安全专业化是任何企业都需要解决的第一步，之后则是细化内部团队工作职责。同时受限于自身成本、技术能力等因素，可以考虑请专业团队开展相关安全解决方案咨询、代码安全加固、整车渗透测试等服务，发挥产业链各主体技术优势，实现资源互补。

“安全左移”，建立“动态”安全管理流程。“安全左移”，即在设计阶段考虑更多安全因素，是降低安全风险、实现低成本高回报的解决办法。随着软件定义汽车的普及，智能网联汽车信息安全逐渐向 DevSecOps 转变。微软提出的安全开发生命周期（SDL）流程在设计阶段提出安全需求，在验证阶段测试需求是否满足，软件发布后进行应急响应，给出了组建一个从安全需求、防护措施与检测到应急响应的动态安全管理流程的有效思路，构建标准化安全开发全生命周期管理，提高产品安全质量。

“自上而下，由内向外”，加强技术防护。随着智能网联汽车软件化程度逐步上升，加强数据、应用到底层物理硬件“自上而下”的纵向防护愈加重要。同时网联化也伴随着“由内向外”的车辆自身外部接口安全防护及车辆对外通信安全保障需求提

升。建议遵循最小权限设计原则，保证应用及服务的用户都只能访问必须的信息或资源；加强操作系统原生安全，选项默认处于开启状态并合理配置；实现纵深防御，将不同安全防护手段应用于智能网联汽车的每个技术层面，提高攻击门槛；减少暴露非必要的接口，裁剪非必要组件，从而减少攻击面。

智能网联汽车测评工程技术中心（赛迪汽车）

地　址：北京市海淀区紫竹院路 66 号赛迪大厦 12 层

电　话：86-18600230827（邹博松）

010-88559269（朱科屹）

邮　箱：zoubosong@cstc.org.cn（邹博松）

zhukeyi@cstc.org.cn（朱科屹）