2025 年度智能网联汽车漏洞态势分析报告

白帽黑客驱动汽车安全

指导单位：上海市车联网协会 SHANGHAI V2X ASSOCIATION

主编单位：泽鹿安全 SECDEER.COM

发布日期：2026 年 6 月

本报告立足产业实践、汇聚多方智慧，由上海车联网协会指导、山东泽鹿安全技术有限公司主编，联合多家单位、安全战队及行业专家共同编制完成。在此，谨向以下联合编制单位、安全战队及特邀行业专家致以诚挚感谢。

同时，向参与本年度 18 场攻防演练与实车漏洞挖掘赛事的 210 支战队、792 名白帽子表示衷心感谢。正是各位白帽子以攻击者视角在实战环境中发现并上报漏洞风险，为报告提供了最具价值的原始漏洞数据与技术洞察。

联合编制单位：

排名不分先后，按首字母排序

北京航空航天大学、CCF 智能汽车分会、国家计算机病毒应急处理中心、上研智联智能出行科技（上海）有限公司、上海车云数据科技有限公司、上海机动车检测认证技术研究中心有限公司、上海铸盾网络和数据安全治理研究中心、谈思实验室、招商局检测车辆技术研究院有限公司、郑州大学网络空间安全学院、中汽研汽车检验中心（宁波）有限公司、中汽研汽车科技（上海）有限公司、中汽研临港数据科技（上海）有限公司

联合编制战队：

排名不分先后，按首字母排序

安全脉脉战队、Geely Zero 战队、梅花 K 战队、嵩山实验室、天问实验室

特邀行业专家：

排名不分先后，按首字母排序

范鹏、郭峰祥、潘悟君、潘翔、任方英、孙权、辛鹏、张嘉华

一、前言：凝聚"黑客"实战智慧，构筑行业安全共识

智能网联汽车安全本质上是一场持续的攻防对抗。随着云-管-端架构的深化部署以及 AI 与自动驾驶技术的加速落地，新型攻击面与风险形态不断涌现。在此背景下，单一机构或厂商的视角已难以完整刻画智能网联汽车安全的真实态势——真正能够反映产业安全水平的，是活跃在实战一线的白帽子们通过每一次渗透测试、每一场攻防演练、每一个漏洞发现所积累的集体智慧。

报告中的漏洞案例与攻击链分析并非源自实验室环境下的理论推演，而是在 18 场真实攻防演练与实车漏洞挖掘赛事中沉淀的技术研究与实战经验。这是一份立足白帽黑客实战、面向行业协同共享的年度态势分析报告，白帽子团队以攻击者视角在真实环境中发现漏洞风险，构成了本报告最具实战价值的内容。

过去一年，智能网联汽车安全生态呈现出一个显著变化：产业安全实践正从单企业、单产品的孤立式防御，逐步走向跨品牌、跨平台、跨领域的协同对抗。在上海铸盾行动、重庆招商铸盾、CCF 智能汽车大赛、强网杯车联网安全专项赛等 18 场赛事演练中，来自高校、企业、科研院所及社会战队的白帽子同台竞技，在真实车辆与云平台上检验安全能力。赛事共计覆盖 22 个品牌、75 款车型，全面反映了当前主流智能网联汽车的安全水位。这一"以实战演练验证防御能力、以竞赛机制促进体系建设"的模式，正成为推动行业安全水位提升的核心动力。

本报告遵循"开放协作、多方共治"原则，我们期望以本报告为起点，与白帽黑客及产业伙伴建立长期合作机制，以年度为周期持续输出态势研判与技术洞察，推动智能网联汽车安全从"被动响应"向"主动治理"转型。

二、报告摘要

本报告面向智能网联汽车场景中车端、云端、移动端与通信链路等典型业务形态（见图 1），围绕漏洞风险评估、年度态势与根因机理展开系统分析，旨在为整车企业、零部件供应商、车联网平台服务商及安全厂商提供统一预警与共享参考。报告在参考通用漏洞评分要素并结合国内外漏洞分类分级相关标准框架基础上，构建低危/中危/高危/严重四级漏洞分级体系，并强调场景感知、就高不就低、攻击链视角与可操作性原则，以适配智能网联汽车“云-管-端”耦合、高敏感指令远程可达、资产分区复杂等特点。

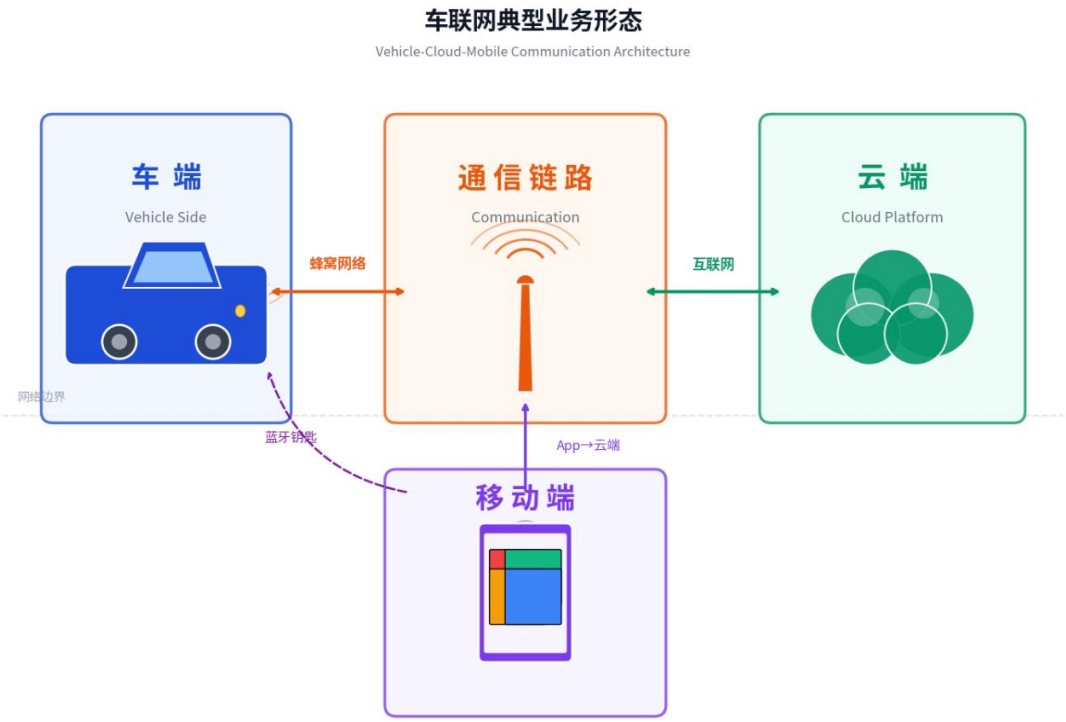


图 1 智能网联汽车典型业务形态

本报告基于近一年 18 场攻防演练、实车漏洞挖掘赛事及公开披露信息的综合样本，报告共纳入具有代表性的智能网联汽车漏洞 834 个（见图 2），总体分布呈现“中低危漏洞普遍存在，高危与严重漏洞危害集中、攻击链价值突出”的结构特征:低危 343 个（约 41.1%）、中危 387 个（约 46.4%）、高危 76 个（约 9.1%）、严重 28 个（约 3.4%），其中高危与严重合计占比 12.5%，集中指向远程车辆控制、权限绕过、大规模数据泄露等关键风险场景。

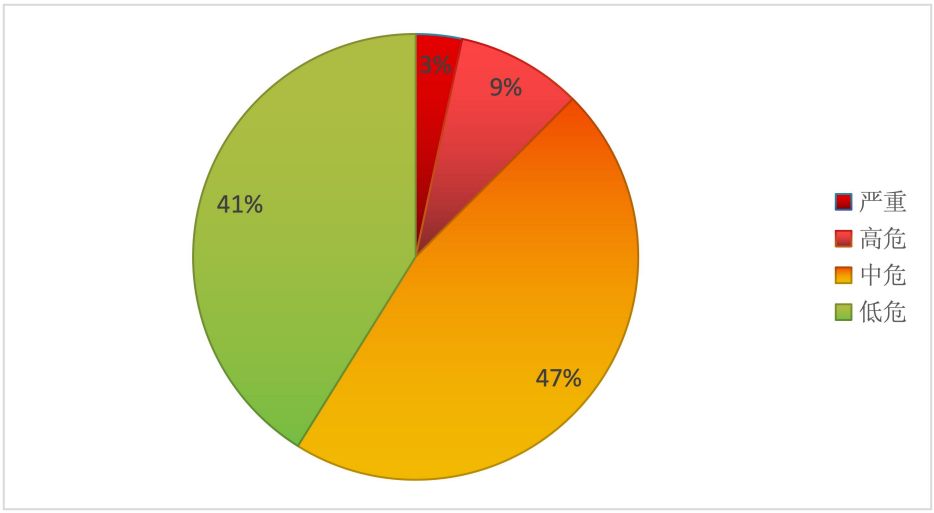


图 2 漏洞等级占比

分析表明，中低危漏洞主要作为攻击链的攻击链入口节点，通过信息泄露、

配置缺陷等降低后续攻击成本；而高危与严重漏洞高度集中于云-管-端关键链路，其根因可归纳为身份认证与会话管理缺陷、访问控制与权限模型设计不当、系统配置基线薄弱、通信与协议安全设计不足、网络暴露面与边界隔离治理缺失五大类，并常沿“中低危—高危—严重”路径逐级放大，最终形成远程车辆控制或海量数据泄露的完整攻击链。

报告提出以“攻击链治理”为核心的安全建设原则，建议产业各方优先管控高敏感指令链路、强化服务端可信边界、治理工程接口与信息暴露面，并推动面向合规的漏洞分级管理与协同监管机制落地。

关键词：智能网联汽车安全；漏洞态势；风险分级；远程车辆控制；越权访问；会话管理；权限模型；工程模式；协议安全；数据泄露；攻击链治理

三、年度漏洞总体态势

报告基于近一年 18 场车联网攻防演练赛事、实车漏洞挖掘赛事及安全研究活动所积累的漏洞样本，涉及 22 个品牌、75 款车型，并结合企业内部测试数据与公开披露信息，对年度漏洞态势进行总体刻画。统计口径涵盖车端、云端、移动端及通信链路等典型场景，全年共纳入具有代表性的智能网联汽车安全漏洞 834 个。

从形态与风险指向看，中低危漏洞主要聚集于安全基线与配置治理薄弱、接口与日志信息过度暴露、短距无线与外设接口加固不足、消息通道与链路加密配置不当等问题。这类漏洞往往难以单点直接造成“控车级”后果，却在攻击链中扮演“铺垫入口”和“情报支撑条件”的角色，显著降低后续撞库、会话劫持、越权访问与接口滥用的门槛。

相比之下，高危与严重漏洞更集中出现在云-管-端关键链路与高敏感资产环节。在根因框架上，报告将智能网联汽车漏洞高频根因归纳为五类（见图 3）：身份认证与会话管理缺陷、访问控制与权限模型设计不当、系统安全防护薄弱、通信与协议安全设计不足、网络暴露面与边界隔离治理缺失，并强调这些根因往往沿“中低危—高危—严重”的路径逐级放大，最终形成远程车辆控制或海量数据泄露的完整攻击链。

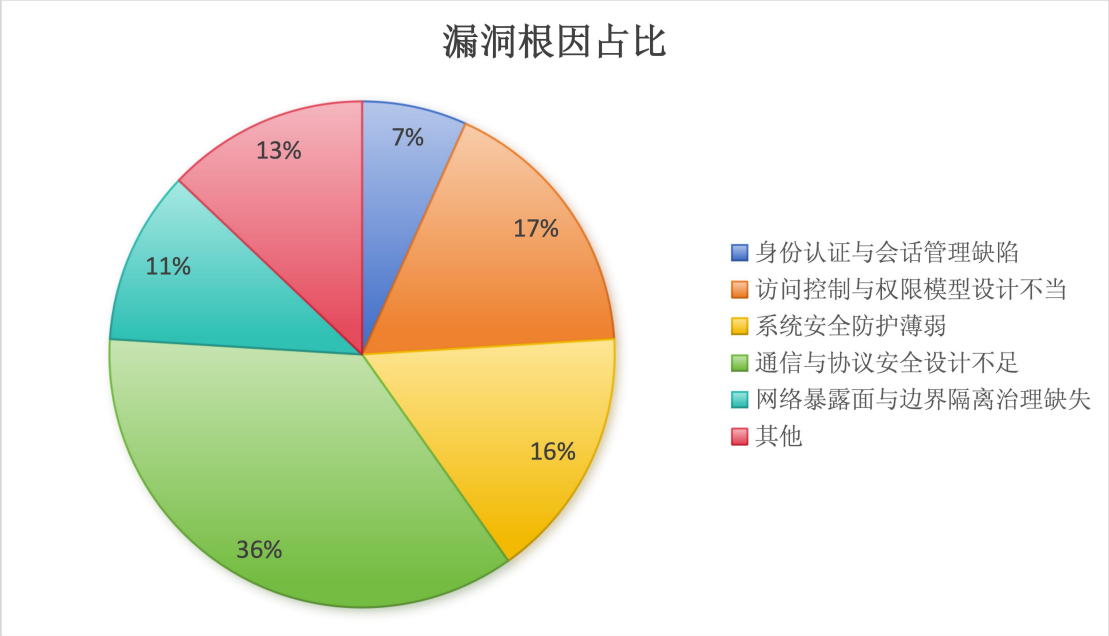


图 3 高频漏洞根本原因结构占比

3.1 漏洞数量

从年度规模看，834 个样本反映的并不是单一系统或单一环节的局部问题，而是云-管-端全链路在快速迭代、生态扩张背景下的暴露面覆盖广泛。值得注意的是，不同发现渠道对漏洞画像的影响明显：在各类活动中，中低危漏洞始终占主导，但以攻防演练、实车漏洞挖掘为主的演练更容易触达关键链路与核心资产，因此高危与严重漏洞占比会显著上升，部分活动中高危+严重占比接近 20%。这意味着年度趋势的判断不能只看“数量”，更要看“发现环境是否贴近真实业务”和“漏洞是否落在关键链路”。

3.2 高风险漏洞占比

按前述四级分级标准对年度样本进行定级，本年度漏洞总体呈现“中低危占多数，高危与严重占比较小但风险影响更大”的结构：低危 343 个（约 41.1%）、中危 387 个（约 46.4%）、高危 76 个（约 9.1%）、严重 28 个（约 3.4%）。中低危合计约 87.5%，主要反映安全基线、配置治理与信息保护方面的薄弱；高危与严重合计约 12.5%，虽然数量有限，却往往直接关联远程车辆控制、权限提升、诊断安全绕过和大规模数据泄露等高风险场景，对行车安全构成实质威胁。

从风险成因看，高危与严重漏洞在样本中呈现出较强的跨链路关联性特征：它们往往不是传统意义上的单点技术缺陷，而是与身份认证与会话管理、指令授

权模型、无线通信链路、OTA/诊断信任链及供应链安全等系统性问题交织，承担着攻击链从“入口”走向“控制权”的关键作用。这也是为什么在更贴近真实业务的实车环境中，高危/严重比例会上升：关键链路一旦被触达，漏洞的“放大效应”会更快显现。

3.3 应用场景漏洞分布

从场景覆盖看，本年度样本同时包含车载系统、通信链路、云端接口、移动端以及第三方，智能网联汽车应用场景漏洞分布见图 4，智能网联汽车漏洞等级场景占比图见图 5。

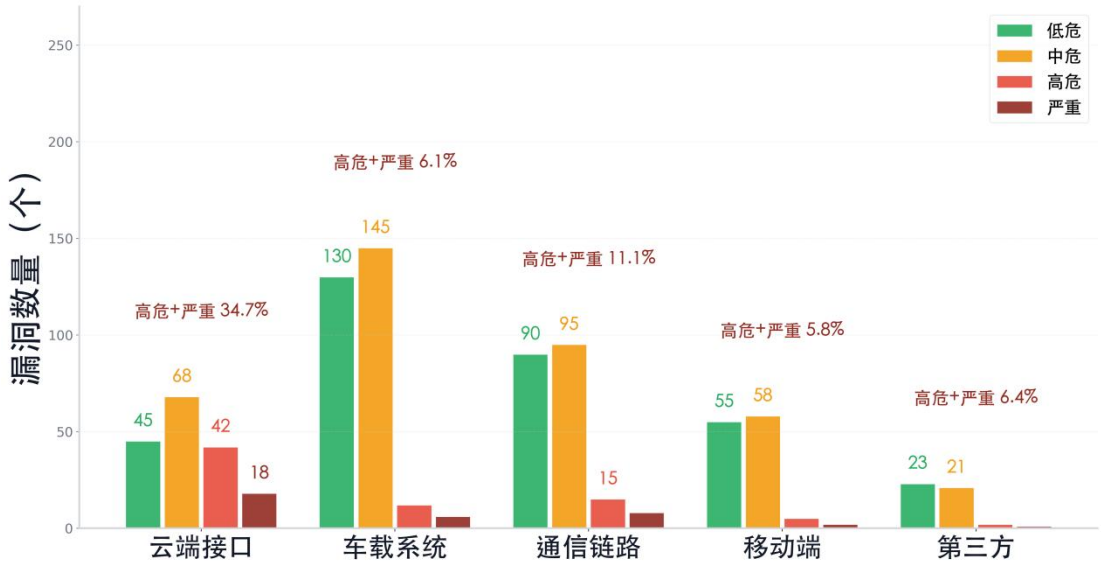


图 4 智能网联汽车应用场景漏洞分布图

图 5 智能网联汽车漏洞等级应用场景占比图

在总体结构上，中低危漏洞更分散，往往体现为“基线缺失”与“暴露面治理不足”：单点虽仅表现为资产暴露或信息泄露，但在攻击链中具有明显铺垫作用，一方面扩大攻击者可利用的入口范围，另一方面为后续凭据窃取、会话劫持、接口滥用等高危行为提供必要的信息与环境。

与之相比，高危与严重漏洞更集中于云-管-端关键链路及能够直接影响车辆控制与海量数据安全的环节，呈现出更明显的场景集中特征。

云端接口与平台侧是高风险的集中区域之一。典型形态包括：通过逆向接口签名算法、绕过防重放机制，配合窃取或伪造的 Token 实现批量远程车辆控制（见图 6）；或者利用后门账号/调试接口，在缺乏二次确认与操作分级的情况下直接执行开关锁、启停、空调等高敏感指令（见图 7）；以及"退出登录后 Token 未失效、服务端缺乏使用上下文校验"导致攻击者单次获取后长期保有远程控制能力（见图 8）。这类问题的共同点是：服务端将“请求格式合法”错误地等同于“请求来源可信”，导致指令授权模型与会话治理被系统性削弱。

图 6 远程车辆控制的典型形态一

图 7 远程车辆控制的典型形态二

图 8 远程车辆控制的典型形态三

车载系统与零部件侧的高风险往往以“本地入口—提权—横向移动”为主线：如通过恶意 U 盘文件或特制文件在车机上执行代码获取 Root 权限并植入持久化后门；或利用车机命令注入/权限校验缺陷实现从普通应用到系统/Root 的提权；以及零部件诊断安全访问控制绕过，使未授权主体执行高危诊断指令。一旦上述能力与远程访问入口叠加，风险将由车机层面扩展到整车控制域。

通信链路与协议栈侧既包含大量“看似低中危”的数据可信度与窃听风险，也包含少量但后果严重的协议栈缺陷。在车云架构中，MQTT 等消息通道若配置不当，攻击者可匿名连接 Broker、订阅主题批量窃取车队数据，甚至向控制主题发布伪造指令干扰远程控制逻辑；其根源往往是匿名连接、弱口令、主题权限控制配置宽松以及暴露在公网/薄弱网段。当通信链路未启用 TLS、或存在明文/加密双协议且缺乏严格降级防护时，中间人攻击窃取 Token 与指令的成本会被显著降低，进而为云端车辆控制链路的利用提供必要的前置信息。在更严重的情

形下，协议栈的内存安全缺陷可能直接从通信层跨越到执行层：例如蓝牙协议栈在处理 Profile 报文时存在缓冲区溢出/越界访问等内存安全缺陷，并伴随状态机校验不足与隔离缺失，攻击者可在特定条件下实现代码执行并作为车内网络渗透中间节点。

移动端与业务链路侧的风险更多体现为“会话与签名体系、绑定与授权流程”的系统性缺陷。文档给出的典型案例表明，当签名算法可复现、客户端可控随机数不参与服务端唯一性校验、统一密钥被逆向后可为任意用户伪造合法签名，再叠加 Bearer Token 泄露与缺乏设备/IP/地理等上下文绑定时，就会出现“一次截获、多次滥用”的攻击路径。

3.4 主要漏洞类型统计

在年度样本中，漏洞类型如果仅按传统“CWE 名称”罗列，往往难以解释智能网联汽车场景的风险放大机制。本报告侧重于攻击链与治理可落地角度进行归纳：高频问题集中于认证会话、访问控制、设备固件、通信协议与数据保护等根因类别，并沿着从低危到严重的路径逐级放大，最终形成远程车辆控制或大规模数据泄露的攻击链。

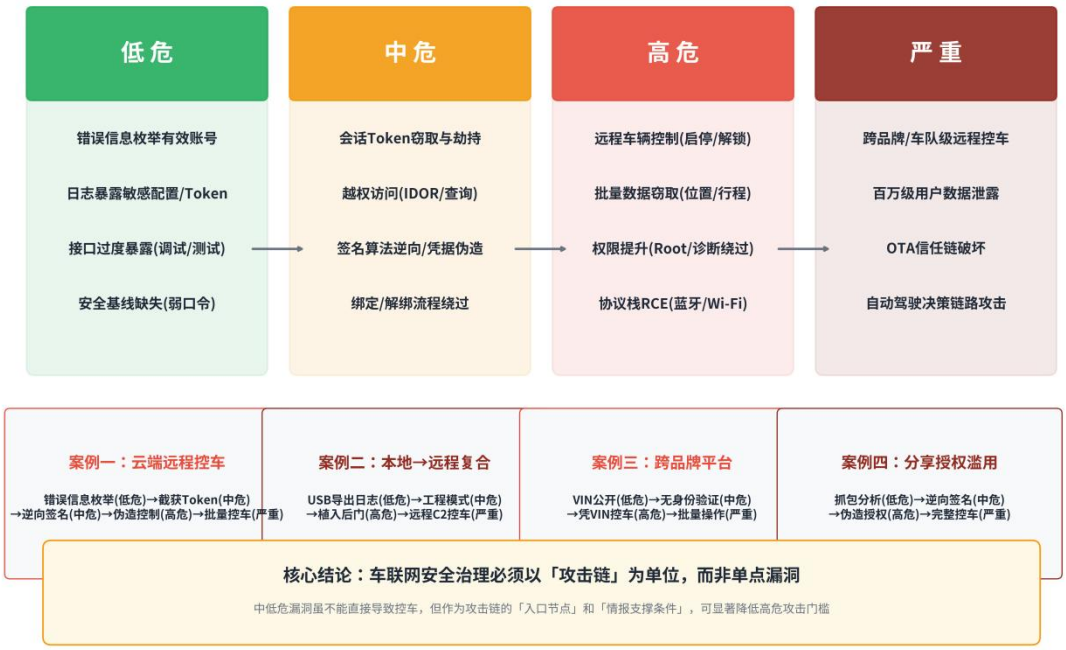


图 5 攻击链逐级放大路径图

认证绕过及会话治理缺陷是触发高危、严重安全事件的高频因素，突出表现在：签名与防重放机制未能有效生效、Token 生命周期过长且会话退出后仍不失

效、服务端缺乏上下文绑定与二次确认等。这些缺陷使得原本依赖强交互的车辆控制功能，可被攻击者脚本化、批量化地远程操控，从而显著放大风险。

其次，输入验证不足与命令注入/脚本执行更常见于车载系统与零部件侧，当其与工程模式、调试接口暴露相互叠加时，可导致演化为提权与持久化能力，并成为进入车内网络乃至控制域的中间节点。

再次，协议解析与链路安全问题通常以“配置与部署缺陷”形态出现，例如 MQTT Broker 开放匿名连接、弱口令与主题权限控制不足，或车云链路未启用 TLS、存在可降级的明文通道，带来窃听、伪造与指令干扰的现实风险。在车机侧，私有协议“只做格式校验、不做身份校验”的设计缺陷也会成为典型入口：例如 Wi-Fi 配网协议缺乏发送方身份校验与车主交互，攻击者在热点内网可下发任意配网指令，使车机连接恶意 Wi-Fi，进而实现流量劫持与进一步渗透。使车机重新连接恶意 Wi-Fi 的典型有效攻击方式为 DeAuth 泛洪攻击。在攻防演练活动中高频出现。

最后，内存安全缺陷更多集中在协议栈与底层组件，一旦触发往往直接越过业务层防护，造成代码执行级后果。PerfektBlue 相关分析指出，蓝牙协议栈在报文处理中的缓冲区溢出/越界访问等问题可被链式利用，结合状态机处理不当与隔离缺失，最终导致车机侧代码执行并成为后续攻击跳板。

四、典型漏洞技术分析

本章在每个案例中，将按照“影响 → 成因 → 利用示例”的结构进行描述，以便不同背景的读者既能抓住问题要害，又能理解技术实质。

4.1 身份认证与会话管理缺陷

身份认证与会话管理是车主 App、车联网云平台及车联网服务平台的基础安全保障环节。近年来披露的多起远程车辆控制与位置跟踪事件表明，该环节的安全缺陷已从"中低危风险"逐步演化为可直接导致大规模车辆被远程控制和长期跟踪的高危根因。根据 Upstream《2024 年全球汽车网络安全报告》的数据，针对车载远程通信与应用服务器的攻击约占全部汽车网络攻击的 43%，且绝大多数为远程攻击；而 Upstream 在《2025 年全球汽车与智能出行网络安全报告》中进一步指出，该比例已 43% 升至 约 66%，其中 API 驱动型攻击占比约 17%，

远程攻击占比达 92%，呈现出攻击面持续向后端服务器与 API 集中、规模与频率同步放大的态势。

4.1.1 凭据暴露与会话治理缺陷导致的中低危风险

这一层面的漏洞通常不会立刻带来远程车辆控制能力，但会显著降低攻击门槛，为字典攻击、会话劫持和中间人窃取 Token 提供前提条件。

4.1.1.1 错误信息过度暴露与账号枚举

影响:登录、找回密码等接口返回过多细节，如明确提示“账号不存在/密码错误”，或在错误响应中携带内部校验逻辑、用户标识等字段，使攻击者可以批量枚举有效账号，构建字典暴力破解，对车主账户实施大范围探测。

成因:在设计认证接口时，为了提升用户体验，系统往往将不同错误类型分别提示给用户，却忽略了攻击者可以自动化收集这些提示，将其作为判断账号有效性的辅助判断依据。

利用示例:攻击者利用脚本对手机号、邮箱、车牌号等进行批量提交，根据返回消息区分有效与无效账号，再结合历次数据泄露中的密码字典实施撞库。一旦少量账号被接管，就可以在车企 Web 门户或 App 中查询车辆位置、行程等敏感数据，为下一步攻击提供前提。

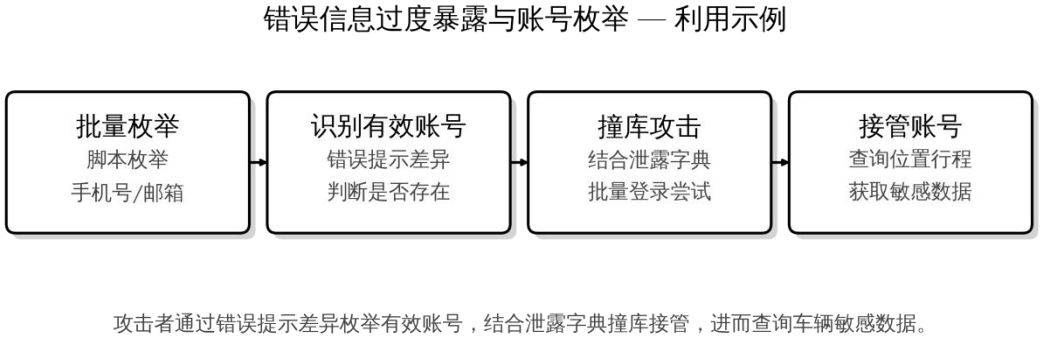


图 9 错误信息过度暴露利用示例

4.1.1.2 一次性凭据与多因素认证保护不足

影响:登录、绑定/解绑车辆、重置密码等关键操作中使用的短信验证码、邮件链接或一次性 Token，在有效期设置、使用次数限制、传输加密等方面保护不足，可能被拦截、重放或暴力猜测，导致账号被劫持或车辆绑定关系被篡改。

成因：一次性凭据通常被视为“临时安全”的，开发时倾向于设置较长有效期或允许多次尝试；同时，如果短信/邮件链路未启用充分的 TLS 验证，或客户

端对链接点击缺乏来源校验，就存在被中间人攻击利用的可能性。

利用示例：攻击者在公共 Wi-Fi、恶意基站等环境下实施中间人攻击，拦截车主用于登录或绑定车辆的短信验证码，再配合前述账号枚举结果，在短时间内接管车主账号。被接管的账号可直接用于远程解锁、启动车辆或查看位置历史。

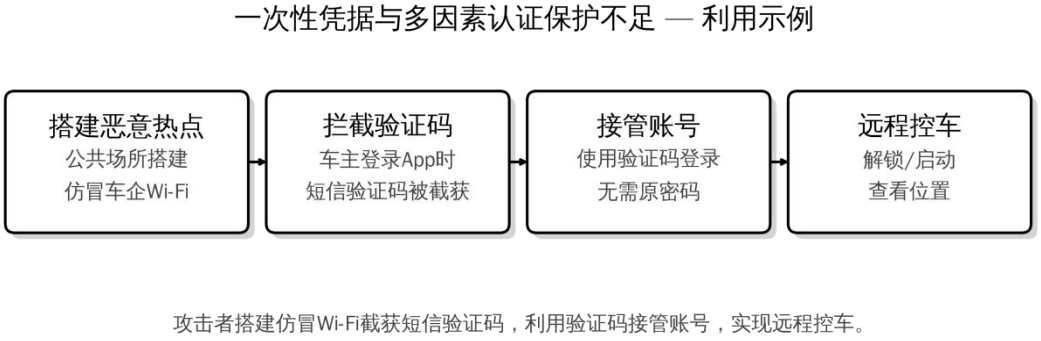


图 10 一次性凭据的利用示例

4.1.1.3 日志与调试接口中的敏感会话信息泄露

影响：在实际运维中，为了方便排查故障，部分系统会在日志或调试接口中记录完整的访问令牌、Session ID、重置链接等敏感信息；当这些日志存储在防护薄弱的服务器、对象存储或开发者终端上时，相当于为攻击者提供了可直接获取的有效凭证。

成因：安全开发生命周期与日志规范不完善，导致开发阶段用于调试的详细日志在上线后仍保持开启；同时，日志平台与生产系统隔离不足，访问控制粒度粗糙，很多内部账号都能查看包含敏感 Token 的调试信息。

利用示例：攻击者首先通过弱口令、已知漏洞或供应链渗透等方式获取日志平台访问权限，然后在日志中搜索关键词，如“Authorization”“Bearer”“token=”等，批量提取仍在有效期内的访问令牌。由于大多数平台仅根据 Token 本身进行鉴权，攻击者即可在任意终端重放这些 Token，模拟车主或运维人员调用远程控制与查询接口。

图 11 敏感信息泄露攻击路径示例

4.1.1.4 会话生命周期与退出机制设计不合理

影响：访问令牌生命周期过长、缺乏强制续期机制，或者“退出登录”仅在客户端本地清理缓存而非真正使服务器端会话失效，导致 Token 一旦泄露，攻击者可以在很长时间内保持对账号的控制。

成因：出于减少频繁登录、提升体验的考虑，不少车主 App 和 Web 门户采用“Token 鉴权 + 自动续期”设计；而安全设计中未对高敏感操作建立与普通浏览操作不同的会话策略。

利用示例：在登录或日志泄露环节获取 Token 后，攻击者可以长期、隐蔽地调用后台接口。例如，在一段时间内定期查询车辆位置或行程记录，而车主仅仅看到 App 正常工作，无法察觉有其他终端正在并行使用其会话。

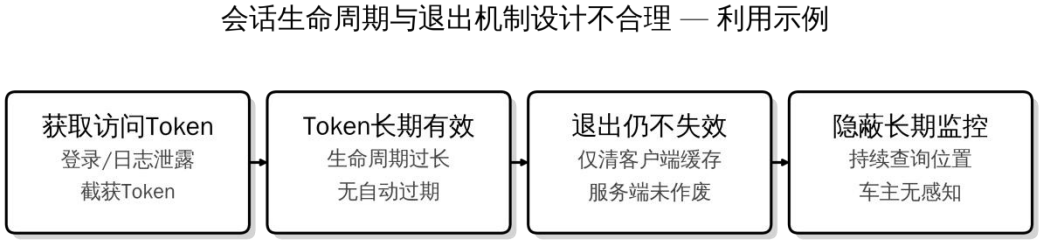


图 12 会话生命周期不合理的利用示例

4.1.2 中低危风险组合导致的高危与严重风险

当身份认证与会话管理缺陷与接口设计问题叠加时，攻击者不再只是获取更多数据，而是可以直接在云端完成远程启停、解锁、控制车窗和空调等高敏感操作，形成典型的云端认证环节一旦被突破，车辆端即失去安全保障的场景。下面选取三个国内实车安全演练中的典型案例以及 SiriusXM 公开事件，对其影响、

原理和利用路径进行分析。

4.1.2.1 移动端会话被窃取 + 可复现签名算法，实现远程车辆控制

影响：获得车主全部的车辆控制权限。

在某品牌车型的实车安全测试中，测试人员发现其车主 App 与 TSP 平台之间的车辆控制接口仅依赖 App 侧计算的签名与 Token 进行认证。通过搭建恶意 Wi-Fi 热点并实施中间人攻击，成功获取车主手机与云端之间的 HTTPS 流量，在替换证书后解密出完整的认证 Token。掌握签名算法后，攻击者可以构造任意远程控制请求，完成车辆远程启停、车门解锁/上锁、车窗开闭等操作。

成因：签名与会话的实现均位于终端侧，存在暴露风险，技术分析表明，该车型的车辆控制接口使用如下签名机制：

sign = MD5(appId + 请求体 JSON + 随机串 + 时间戳 + appKey)

其中 appKey 固定保存在 App 内部，签名随机串和时间戳完全由客户端生成并上送。只要攻击者掌握了 appId、appKey、请求体格式以及从中间人流量中截获的 Cookie/Token，即可在任何终端复现签名逻辑，生成看上去“合法”的请求报文。这反映出三个根本性问题：

1)会话保护不足：Token 通过中间人攻击即可获得，未与设备指纹、TLS 会话等绑定；

2)签名算法暴露：签名完全在客户端实现，并使用固定、易逆向的密钥；

3)服务端缺乏场景校验：服务端不校验客户端证书、不校验请求来源环境，只要签名和 Token 匹配即认为合法。

利用示例：

1)攻击者在公共场所搭建仿冒 Wi-Fi 热点，引导车主手机连接；

2)向手机下发伪造根证书，对 App 与云端的 HTTPS 通信进行中间人解密，截获车辆控制请求中的 Token 和请求体结构；

3)通过逆向 App 或分析脚本，恢复签名算法和参与签名的参数；

4)在攻击者控制的终端上构造任意车辆控制请求，使用截获 Token 与自制签名向 TSP 平台发送指令，从而对目标车辆进行远程启停、解锁、开闭车窗等操作。

图 13 复现签名算法的利用示例

4.1.2.2 统一签名密钥 + 可控随机数，防重放机制形同虚设

影响：任意数据包重放实现远程车辆控制。

在另一款车型的车辆控制接口测试中，研究人员发现云端接口虽然实现了“签名 + 随机数”的防重放机制，但签名算法和密钥均内置于 App 中，且所有用户共用同一密钥。攻击者在获取一次合法的 Bearer Token 后，即可根据逆向得到的算法生成任意控制指令，实现 解锁后备箱、控制车窗、空调开关、鸣笛闪灯 等操作。

成因：伪随机与统一密钥导致“防重放”失效

该接口的签名大致流程为：

1)生成 x-nonce：由“时间戳 + 伪随机字符串”拼接而成；

2)构造签名串：HTTP 方法 & 请求路径 & 排序后的头部参数(x-app-key/x-nonce/x-timestamp) & 查询参数 & 请求体 JSON；

3)对签名串进行 URL 编码后，用统一的 APP_SECRET 做 HMAC-SHA256 运算，再 Base64 编码得到 x-signature。

在这种设计下，x-nonce 虽然看上去随机，但完全由客户端控制，不参与服务端“是否已见过”的唯一性校验；所有用户共享同一 APP_SECRET，一旦被逆向，攻击者即可为任意用户伪造合法签名；服务端对签名与 Token 之间没有更细粒度的绑定，导致一旦 Bearer Token 泄露，将与其他任意参数组合都被认为是“可信请求”。

利用示例：一次截获，多次车辆控制

攻击链如下：

1)攻击者通过中间人攻击或终端恶意软件获取目标车主的 Bearer Token；

2)逆向 App 中的签名类，恢复签名字符串构造逻辑以及统一的 APP_SECRET；

3)在自制脚本中自由构造车辆控制请求体并生成合法 x-nonce、x-timestamp 和 x-signature；

4)使用上述参数向云端接口发送 POST 请求，即可绕过防重放机制，对目标车辆执行任意次数的云端车辆控制操作。

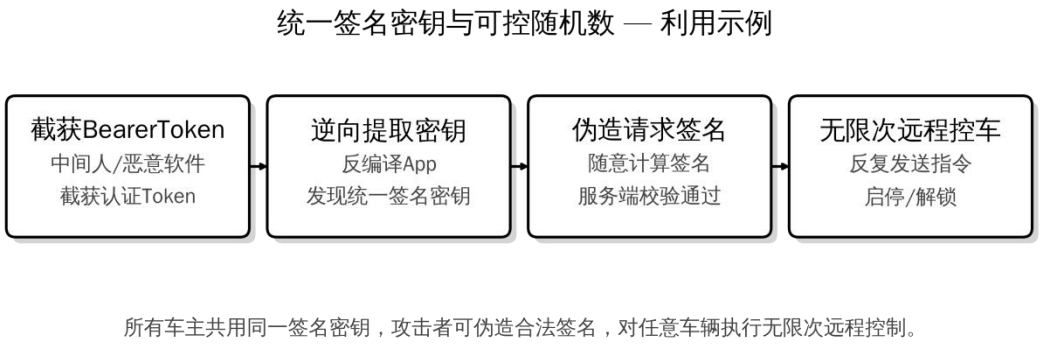


图 14 密钥统一且无可控随机数的攻击原理

4.1.2.3 工程模式日志泄露有效 Token，导致远程未授权车辆控制

影响：攻击者凭单一 Token 即可对目标车辆实施多次远程控制。在某车型的 T-BOX 安全测试中，研究人员发现车辆工程模式导出的系统日志中，存在明文存储的用户访问 Token。通过分析 App 与车云通信加密逻辑并提取密钥后，只需在控制脚本中填入日志中的 Token 与目标车辆 VIN，即可对车辆执行关闭车窗等远程控制操作，且可多次复现，构成严重级远程未授权车辆控制问题。

成因：Token 有效期设置不合理 + 工程日志缺乏脱敏与隔离

1)会话生命周期过长：Token 在较长时间内保持有效，且云端对其使用次数和调用环境几乎不做限制；

2)工程模式日志未脱敏：工程模式导出的日志文件中包含完整 Token，且日志获取过程不要求车主强认证，维修人员或任何能进入工程模式的主体均可导出。

在这种情况下，一旦日志文件被复制或泄露，攻击者便拥有了长期有效的访问凭据。

利用示例：线下获取日志，线上实现远程车辆控制

1)在维修、租赁或共享使用等场景中，攻击者通过工程模式导出车辆系统日志；

2)从日志中提取明文 Token，并结合逆向得到的加密参数；

3)编写控制脚本，对请求体进行加密并带上 Token 与 VIN，向云端 T-BOX 接口发送控制指令；

4)在未获得车主授权的情况下，多次远程控制车窗等功能，且车主难以及时察觉异常来源。

图 15 Token 长期有效的利用示例

4.1.2.4 SiriusXM 远程信息处理平台认证缺陷导致跨品牌远程车辆控制

影响：只凭 VIN 即可远程解锁/启动车辆

2022 年公开的 SiriusXM 车联网服务漏洞，是另一类跨品牌远程车辆控制事件。研究人员在分析多家车企的联网汽车服务时发现，SiriusXM 提供的远程信息处理平台在授权上严重依赖车辆识别码：攻击者只需知道某辆车的 VIN，即可通过平台接口对多家品牌的车辆执行解锁车门、启动车辆、定位、鸣笛和闪灯等操作，并获取部分车主信息。

成因：将静态标识误当作强认证因子

1)接口将 VIN 视为主要授权凭据，只要请求参数中的 VIN 与平台记录匹配，即认为该请求与对应车辆关联；

2)调用方缺乏强身份验证，未在服务端执行多因素或设备认证；

3)未对调用行为进行细致的风控与频率限制，导致攻击者可以自动化尝试大量 VIN。

大部分车型的 VIN 直接印在挡风玻璃下方或车身外部，任何人站在车旁就能读取，该设计实质上等同于 用一串公开可读的编号替代了真正的身份认证机制。

利用示例：从街头采集 VIN 到批量远程操作

1)攻击者在停车场等地点采集目标车辆 VIN，或通过黑市数据获得大量 VIN

列表；

2)根据逆向分析掌握 SiriusXM 车辆控制接口格式；

3)构造携带目标 VIN 的 HTTP 请求，模拟合法客户端调用平台 API；

4)对对应车辆执行远程解锁、启动车辆、定位和鸣笛等操作。

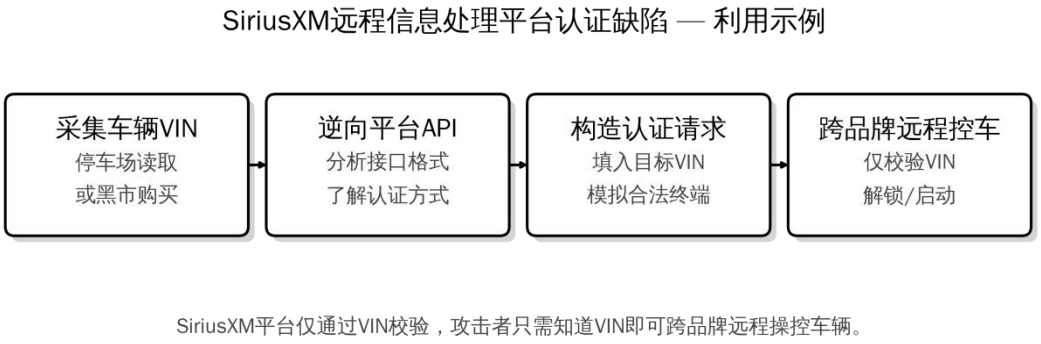


图 16 SiriusXM 远程信息处理平台缺陷攻击链

4.2 访问控制与权限模型设计不当

访问控制与权限模型解决的核心问题为“谁可以在什么条件下对哪辆车/哪类数据做什么操作”。智能网联汽车安全事件表明：一旦访问控制设计不当，攻击者往往可以在已登录或看似“合法”的前提下，跨账号、跨车辆甚至跨车队地滥用功能，从中低危的数据越权演变为到远程车辆控制与大范围位置跟踪。

4.2.1 越权访问导致的中低危风险

这一层面的漏洞通常被归类为“越权访问”，但从攻击链角度看，它们是后续批量车辆控制和大规模跟踪的“起始条件”。

4.2.1.1 车辆与用户数据的 IDOR 越权查询

影响：在车主 App、Web 门户或车队管理门户页面中，常见的情况是：攻击者只需替换 URL 或请求体中的车辆 ID、VIN、用户 ID，即可查看其他车辆的基础信息、实时位置或部分状态数据；在车队场景中，运维人员账号可以越权查看不属于其车队的车辆列表与行驶轨迹。

Sam Curry 等安全研究者在对多家车企和车联网服务进行测试时，就在多个厂商的远程信息处理 API 中发现类似 IDOR 缺陷，可以在未获授权的情况下访问其他车主的车辆信息和个人资料。

成因：这是典型的 IDOR/越权访问问题：

应用直接使用用户提供的 vehicleId、vin 等参数查询后台对象；

没有在服务端按“当前登录用户/角色”做二次访问控制校验，只要 ID 存在就返回对应对象。

利用示例：攻击者登录自己的车主账号，抓取查看车辆详情或轨迹的请求；将请求中的 vehicleId、vin 等替换为猜测或枚举到的其它车辆信息；观察返回结果，如果能成功看到其他车辆的状态/位置，即可批量脚本化扫描整个车队或地区的车辆信息；这些数据随后可用于选择目标车辆、推断车主作息，为车辆控制、盗窃或跟踪攻击奠定基础。

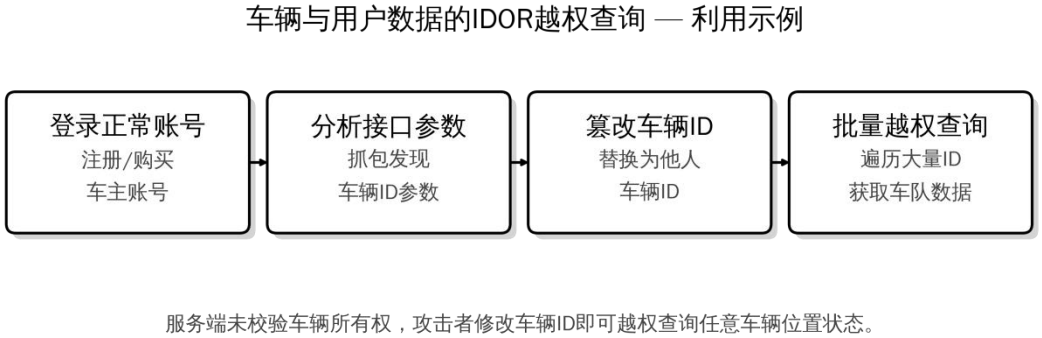


图 17 车辆与用户数据的 IDOR 越权查询

4.2.1.2 绑定/解绑流程中的所有权校验不足

影响：在部分车企的账户体系中，车辆与车主账号的绑定/解绑流程过度依赖弱验证信息，例如：

仅通过输入 VIN 部分位、车牌号或简单验证码就允许绑定车辆；

解绑和转移车辆所有权时，不强制原车主确认或多因素认证。

这将导致攻击者在掌握有限车辆信息时，就有机会将车辆“绑定至攻击者控制账号”，获得对该车的远程控制与数据访问权限。

成因：业务逻辑设计中，将“能提供车辆标识 + 能收短信”视作充分的所有权证明；未充分考虑二手车、租赁车、共享车等复杂场景，缺乏针对“高价值操作”的独立权限模型和风险校验。

利用示例：通过 IDOR/社工等方式获取目标车辆 VIN、车牌或原车主手机号；在 App 或 Web 门户中发起“绑定车辆”或“申请成为车主”的流程；利用流程设计缺陷绕过原车主确认，完成车辆转让；新账号作为“合法车主”调用所有远程控制与数据接口；结合其他越权问题，可进一步查询原车主历史轨迹和行程信息。

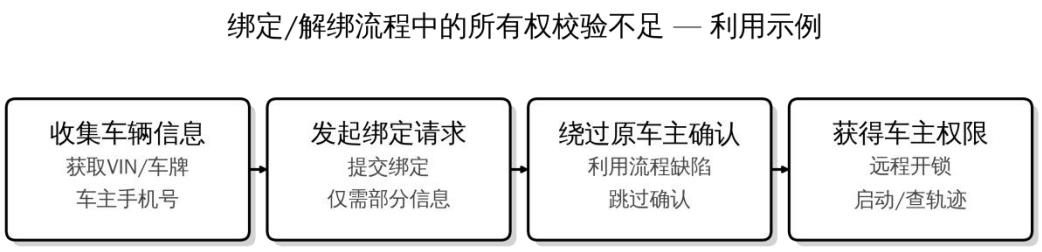


图 18 绑定/解绑所有权校验不足的影响

4.2.1.3 后台权限划分粗放、缺少最小权限原则

影响：在运营后台或经销商/服务商门户中，常见问题包括：

普通客服或经销商账号可以查询全国范围内的车辆与车主数据；

技术支持账号被授予“任意车辆远程操作”权限，而无需按区域/车队/品牌等维度进行限制；

后台没有对“导出全部车辆数据”“批量下发指令”等敏感操作设置额外审批或双人确认。

这使得一旦某个后台账号被攻破，攻击者可以在极短时间内批量获取整个平台的全部车辆和用户数据。

成因：权限模型从角色设计到实现阶段都以“方便运营”为主，未落实最小权限原则；缺乏基于租户、区域和职能的多维访问控制；高敏感操作与普通查询操作共用同一权限集合。

利用示例：攻击者通过钓鱼、弱口令、认证缺陷等手段获取一个后台账号；发现该账号在界面或接口层面并未被严格限制，能够查询大量与自身职能无关的数据；利用导出、批量操作功能，获取大规模车主数据或对多个车辆执行控制命令；在日志审计不完善的情况下，这类越权操作甚至可能长期不被发现。

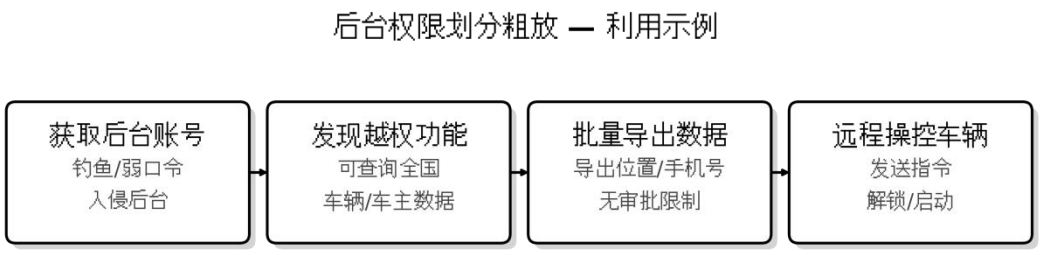


图 19 后台权限划分粗放等利用路径示例

4.2.2 高危与严重风险：车队级控制与位置跟踪

当访问控制与权限模型缺陷叠加认证问题时，攻击者往往可以以“合法身份”对大量车辆和用户执行高敏感操作，典型表现为车队级远程控制与大范围精细位置跟踪。

4.2.2.1 利用车牌号远程控制和跟踪数百万台 Kia 车辆

影响：2024 年，安全研究者在对 Kia 车联网服务进行测试时发现，攻击者只需在手机上扫描目标车辆的车牌号，即可通过后端接口获取车辆 VIN，并在 30 秒内完成以下操作：

远程解锁/锁闭车门；

远程启停发动机；

精确定位车辆位置；

触发鸣笛和闪灯等功能。

这一漏洞影响所有配备车联网服务的 Kia 车型，攻击者几乎可以在街边任意选择目标车辆实施“远程未授权控车”。

成因：问题集中在访问控制与权限模型上：

应用服务在后台通过车牌号查询车辆 VIN 和车联网账号信息时，缺乏对调用主体的强身份验证与授权校验；

远程控制接口仅以 VIN 和简单会话参数作为授权依据，未核实调用者是否为该车的合法用户，也未限制不同租户之间的访问范围；

整个流程可由攻击者模拟合法客户端自动化执行。

利用示例：攻击者在停车场使用手机拍摄目标车辆车牌号；

在攻击工具中调用后端接口，根据车牌号获取对应 VIN 和账号信息；

构造携带 VIN 与伪造身份凭据的控制请求；

对目标车辆执行解锁、启停和定位操作，实现车辆盗窃或跟踪。

图 20 手机扫描车辆获取车辆信息

4.2.2.2 车辆绑定接口缺陷导致越权绑车

影响：任意账号可将他人车辆“绑到自己名下”

在某乘用车品牌的车联网账户系统中，车主 App 所调用的“添加车辆”接口存在设计缺陷：

接口只要求调用方是已登录用户，并没有校验该用户是否对目标车辆拥有合法所有权；

车辆识别码被直接当作绑定条件，只要 VIN 合法就会将对应车辆加入当前账号名下。

在这种情况下，攻击者只要知道任意一辆车的 VIN，就可以在自己的账号中成功“绑车”，随后以“合法车主”身份使用远程开锁、查看状态等敏感服务，风险等级为高危。

成因：资源标识替代所有权校验，权限模型缺失

从访问控制的角度看，这一漏洞体现了典型的授权模型缺失：

授权判断只回答了“这个请求是不是来自一个合法登录用户”，但没有回答“这个用户是不是这辆车的合法车主”；

系统默认“能提供 VIN 的就是车主”，缺乏任何所有权证明；

高敏感操作的接口与普通查询接口使用同一套鉴权机制，没有额外分级、审计和限速控制。

利用示例：登录自己的账号 → 构造绑定请求 → 批量越权绑车

典型的攻击步骤可以概括为：

攻击者注册或获取一个正常车主账号，登录后获得访问令牌；

通过流量分析或逆向“绑定车辆”接口的请求格式，仅包含 VIN 等基础字段；

将请求中的 VIN 替换为目标车辆的 VIN，并保持其它字段格式不变后发送；

后端在未做所有权校验的情况下返回成功，该车辆即被添加到攻击者账号；

攻击者据此调用远程控制和车辆信息查询接口，实现对他人车辆的越权控制；

若攻击者掌握大量 VIN，还可以批量执行上述操作，形成车队级风险。

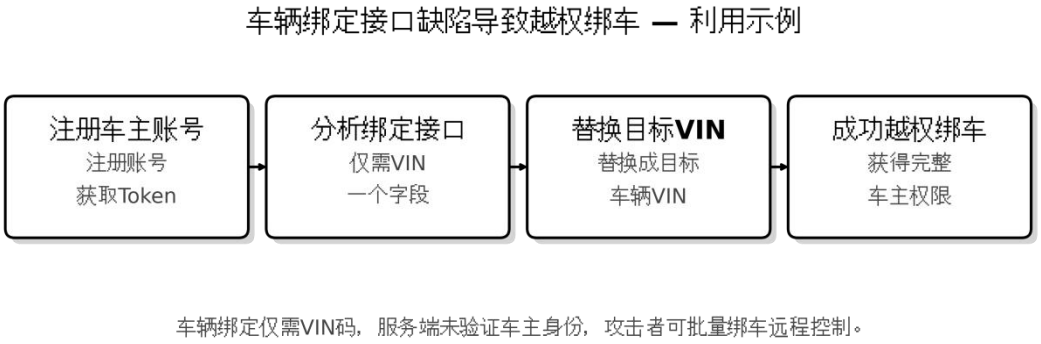


图 21 车辆绑定接口缺陷的典型影响

4.2.2.3 “分享授权”接口设计不当导致远程未授权车辆控制

影响：伪造分享关系，远程控制任意车辆

在某品牌的车控 App 中，平台为支持“车主将车辆使用权限分享给家人/朋友”而设计了一个授权接口，用于在云端创建“账号 ↔ 车辆”的分享关系。实际实现中存在以下问题：

任意已登录账号都可以直接调用该授权接口，只要提交合法格式的 VIN 和被授权手机号，后端就会记录一条新的授权关系；

接口并不要求当前账号是该车辆的原始车主，也不要求原车主确认此次分享；

请求使用的时间戳/签名校验逻辑较弱，经过逆向后可以在离线环境中伪造。

在漏洞验证中，攻击者通过伪造授权请求，可以在自己的账户下对任意目标车辆获得远程控制能力，包括远程启停、解锁车门、开关车窗、控制空调、鸣笛闪灯、管理蓝牙钥匙等高敏感操作，并可横向扩展到该品牌的多款量产车型。

成因：授权流程与业务语义脱节，“分享功能”变成创建账号与车辆绑定关系的创建通道，从根本原因来看，这是一个授权模型和接口设计结合不当的典型问题：

在业务语义上，“分享授权”应该建立在已有“车主 ↔ 车辆”关系基础上，由车主主动发起；

在实现上，接口却变成“任何登录用户都可以为任意 VIN 新建授权关系”，

后端仅做参数完整性和简单时间戳检查；

为防止重放引入的签名/随机数机制，在实现中只被用作形式校验，攻击者通过脱壳和逆向很容易还原并复用签名算法。

利用示例：抓包逆向 → 伪造授权请求 → 远程车辆控制

攻击路径可以描述为：

在测试环境中，攻击者使用已 Root 的终端对车控 App 抓包，找到“分享/授权车辆”的接口调用；

逆向客户端代码，分析用于生成时间戳、随机数和签名的逻辑，发现只要本地构造满足格式即可通过服务端校验；

编写脚本，仿照 App 请求格式构造 HTTP 请求，将其中的 VIN 字段替换为目标车辆的 VIN，将被授权手机号替换为攻击者控制的号码；

使用任意一个合法账号的访问令牌发送请求，后端创建新的授权关系并返回成功；

攻击者随后在自己的 App 账号中看到目标车辆，便可直接调用远程启停、解锁、空调、车窗、鸣笛等控制功能，实现无人车辆控制；

由于接口缺乏频次限制和风控，攻击者可以针对海量 VIN 重复上述过程，形成车队级远程车辆控制能力。

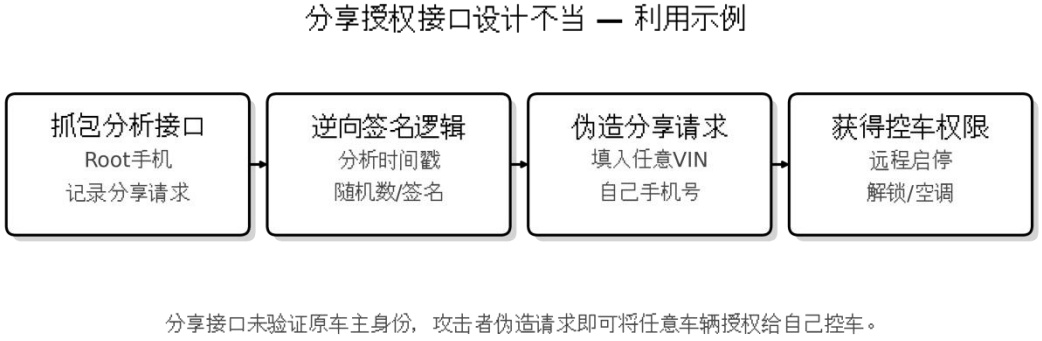


图 22“分享授权”接口设计缺陷的利用路径示例

4.3 设备与固件安全防护薄弱

在车机、T-Box、网关 ECU 等车端设备上，固件安全防护不足、工程模式长期保留以及诊断安全设计不当，是近年来智能网联汽车安全测试中高频暴露的根因之一。很多问题在设计时被假定为“需要物理接触、风险有限”，被评为中低危；但在共享出行、无人车测试、远程诊断与 OTA 普及的背景下，这些本地漏洞

越来越多地被用作提权入口和攻击链中枢。

4.3.1 中低危风险：本地信息获取与工程接口暴露

这一层面的问题以“可读、可看、不易立即车辆控制”为特征，但会给攻击者提供大量系统内部信息和潜在利用面。

4.3.1.1 USB/调试接口可直接导出日志与配置

影响：部分车型在出厂或维保场景中，为方便诊断会保留 USB、串口或隐藏调试口，允许工程师导出系统日志、配置文件甚至部分用户数据。典型风险包括：

获取车机和 T-Box 的日志、配置、密钥片段、访问令牌等敏感信息；读取 Wi-Fi/蓝牙配对信息、导航历史、联系人和通话记录等隐私数据；获知进程列表、服务端点和调试开关，为后续构造利用点提供详尽“完整的系统信息基础”。

最近针对 Mazda Connect 车机系统的一组研究就指出，通过插入特制 U 盘，可触发日志与配置导出，并进一步利用文件解析缺陷在信息娱乐系统上执行任意代码，说明 USB 端口一旦和“信任错误”叠加，风险会迅速升级。

成因：安全开发生命周期中缺乏对“日志敏感度”的分级要求，导致开发阶段启用的详细日志在量产阶段仍保持开启；USB/调试接口权限控制依赖物理接触假设，缺乏进一步认证或加密保护；日志导出功能多以内置命令脚本实现，未对导出的内容进行脱敏处理。

利用示例：在租赁、维修或共享车辆场景下，攻击者通过 USB 或工程菜单导出系统日志；对日志和配置文件进行离线分析，提取其中的访问 Token、后台域名、接口路径、加密密钥等；将这些信息与移动端逆向、网络抓包结合，构建完整的“车云攻防视图”，为后续中间人攻击、签名复现或命令注入准备条件。

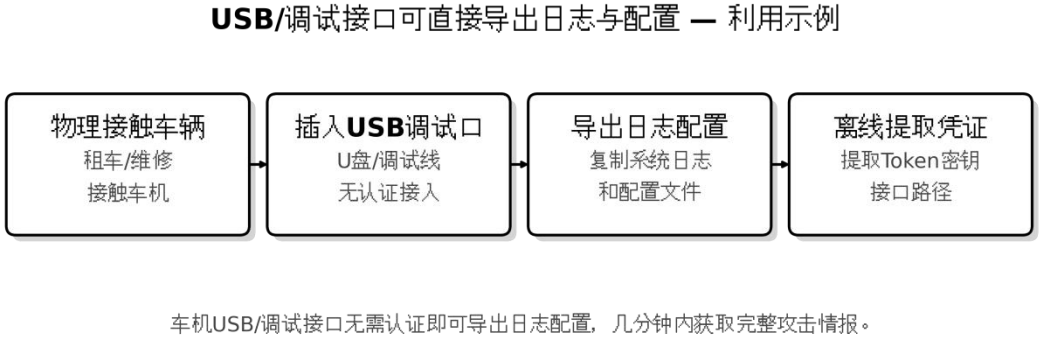


图 23 USB/调试接口利用路径示例

4.3.1.2 工程模式易进入，暴露大量调试功能

影响：许多车机为生产测试与售后维保保留“工程模式”，通过固定密码、隐藏菜单或特定按键组合即可开启，常见功能包括：

修改网络和服务器配置、切换测试环境；

开启/关闭调试日志、抓包能力；

启用包括 ADB、SSH 在内的远程调试服务。

攻击者掌握工程模式入口后，即便初始权限有限，也可以借此扩大攻击面，如启用调试服务、降低安全检查等级，从而更容易实施提权和后门植入。

成因：工程模式设计时以“内部使用”为前提，认证强度普遍偏低；量产阶段未按安全策略进行“功能管控”，工程模式在整车生命周期内一直可用；缺乏对工程模式操作的独立审计与告警。

利用示例：通过社工、内部泄露或逆向固件获取工程模式入口和口令；进入工程模式后开启调试端口、提高日志等级或启用额外服务；结合 USB/网络接口，进一步尝试命令注入、文件上传等攻击；将工程模式作为“后门控制台”，长期保留访问能力。

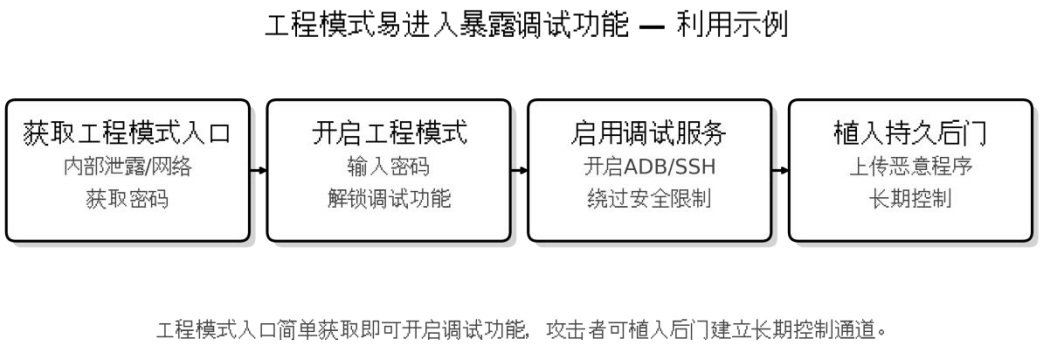


图 24 工程模式缺陷的影响

4.3.1.3 诊断服务基于静态 seed/key 或简单密码

影响：在 UDS/DoIP 等诊断协议下，许多车辆仍依赖传统的“SecurityAccess + seed/key”方式进行安全访问控制：

诊断工具向 ECU 发送"请求种子"，ECU 返回随机数；

工具用某种算法计算密钥回复给 ECU，通过就进入"扩展会话"，可以执行刷写、配置修改或执行高风险例程。

如果 seed/key 算法过于简单或实现泄露，就可能被攻击者逆向或暴力破解，

从而在需要物理接触的场景下获得对关键 ECU 的完全控制权。近年来的研究和工具表明，部分商用车和乘用车的 seed/key 算法已经被公开实现，一旦被滥用，就能对制动、转向等关键系统执行任意诊断命令。

成因：传统 UDS SecurityAccess 设计未强制要求使用成熟密码协议，实现的 seed/key 算法许多为简单的异或、线性变换或表查找；ECU 资源受限、联网能力有限，证书校验和在线授权难以落地，主机厂倾向于采用“离线固定算法”；认证失败次数与锁定机制配置不当，给暴力尝试留下空间。

利用示例：攻击者通过 OBD 接口或诊断插头连接车辆内部总线；抓取合法诊断工具与 ECU 之间的 seed/key 交互流量，或参考公开逆向代码，还原算法；构造自制诊断请求，向安全访问服务发送 seed 请求并计算正确的 key；在获得安全访问权限后，对 ECU 执行刷写、参数修改或运行高风险例程。

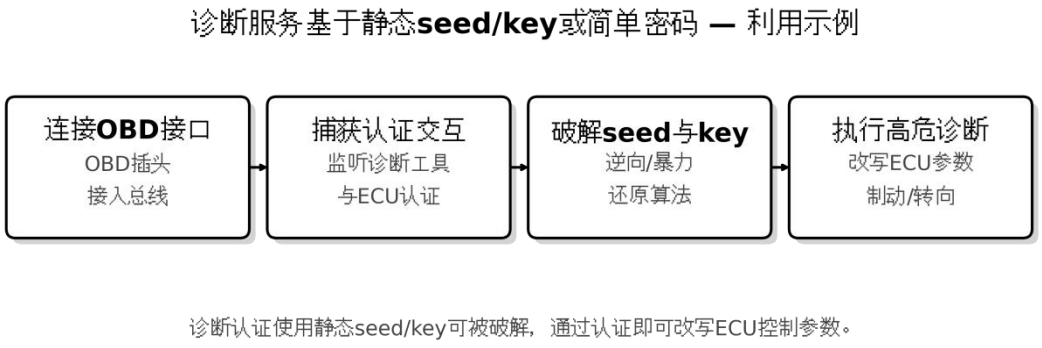


图 25 诊断服务缺陷的典型影响

4.3.2 高危与严重风险：本地攻击上升为远程车辆控制能力

当本地接口和固件缺陷进一步被用来执行任意代码、提升到 Root 或高权限诊断级别，并与无线/远程访问通道结合时，风险会直接上升为高危甚至严重。

4.3.2.1 U 盘自动执行脚本获取车机 Root 权限

影响：任意插入 U 盘即可拿到系统级控制权

在某品牌乘用车的车机系统中，信息娱乐单元支持从 U 盘自动执行特定启动脚本。测试发现，只要在 U 盘根目录放置特定名称的脚本文件，车机在识别 U 盘时就会无提示地执行其中命令，且执行上下文直接为 root 用户。安全测试团队通过这一机制执行 id、whoami、ps 等命令，确认已获得完整的 Root Shell 能力。

这意味着任意能短暂接触车内 USB 口的攻击者，都可以在几秒钟内接管车机

操作系统，后续可植入持久化后门、窃取隐私数据或作为攻击车内网络的跳板。

成因：出厂预留自动运行机制未加任何安全约束

漏洞成因在于车机出厂时保留了 U 盘预定义的调试机制：

系统守护进程在检测到插入 U 盘后，会查找预定义脚本文件并执行；

脚本以 root 身份运行，不做签名校验、白名单限制或交互确认；

该机制在量产阶段仍然开启，普通用户插入 U 盘即可触发。

利用示例：构造恶意脚本 → 获得 Root → 植入后门

攻击者在本地准备一个 U 盘，将恶意 Shell 脚本放置在约定位置；

在停车、维保、租赁等场景下，短暂接触车辆并将 U 盘插入车机 USB 口；

车机识别到 U 盘后自动执行其中的脚本。脚本一方面会调用 id、ps 等命令收集车机当前用户身份与进程信息，并将输出结果写入 U 盘中的隐藏文件，供攻击者拔出 U 盘后离线读取；另一方面，脚本也可使车机主动向攻击者预先部署的远程服务器发起外联，建立一条由车机指向外部的持久通信通道，攻击者借此从远端持续下发指令并实时操控车机；

在拿到 Root 权限后，攻击者可修改系统配置和应用；安装持久化后门；抓取车机与 TSP 之间的通信，窃取 Token 并进一步攻击云端或车内网络。

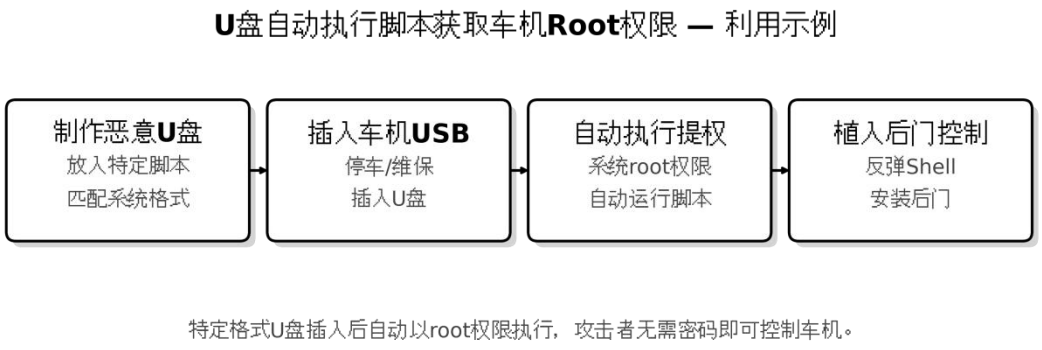


图 26U 盘自动执行脚本获取车机 Root 权限

4.3.2.2 车机底层控制接口缺乏鉴权 + 后门植入导致远程车辆控制

影响：通过恶意后门远程控制车门、车窗等硬件

在某车型的车机系统渗透测试中，发现其底层车辆控制服务对上层调用完全不做权限校验。安全团队为了验证危害，构建了一个模拟恶意后门程序植入车机，使其常驻后台并监听来自远程 C2 的网络指令；后门再本地调用该控制服务，即可绕过 UI 和业务逻辑，直接控制车门、车窗等硬件。

在真实攻击者掌握类似能力时，无论车主是否操作车机，都可能在外部被远程解锁车门或执行其它敏感动作，属于严重级车辆控制风险。

成因：车机内部控制接口“默认信任本地代码”

该漏洞体现了车机内部权限模型的典型问题：

车机底层控制服务对所有本地进程开放，只要在同一系统内即可调用敏感 API；

未基于调用者签名、进程权限或 SELinux 上下文做访问控制；

安全机制只存在于上层 UI 与业务逻辑中，一旦攻击者绕过 UI 直接调用服务接口，就不再有任何制约。

本质上，是把“控制车辆硬件”的能力暴露成了“任何本地代码都可以调用”的普通接口。

利用示例：Hook 分析参数 → 植入后门 → 远程发指令控制车辆

前期情报收集：攻击者在测试环境中通过 Frida 等 Hook 工具拦截正常 App 操作车门/车窗时与底层控制服务的交互；记录关键枚举值、函数签名和调用栈。

武器化与植入：将上述参数整理成“控制字典”，编写恶意后门程序，调用底层控制接口并封装为简单命令；通过 ADB、恶意 APP、供应链投毒等方式将后门植入车机，使其随系统启动常驻后台。

远程利用：攻击者在外部通过互联网向后门发出控制指令；后门在车机本地直接调用控制服务接口，修改车辆状态，实现开关车门、车窗、灯光等操作，而无需任何 UI 或车主确认。

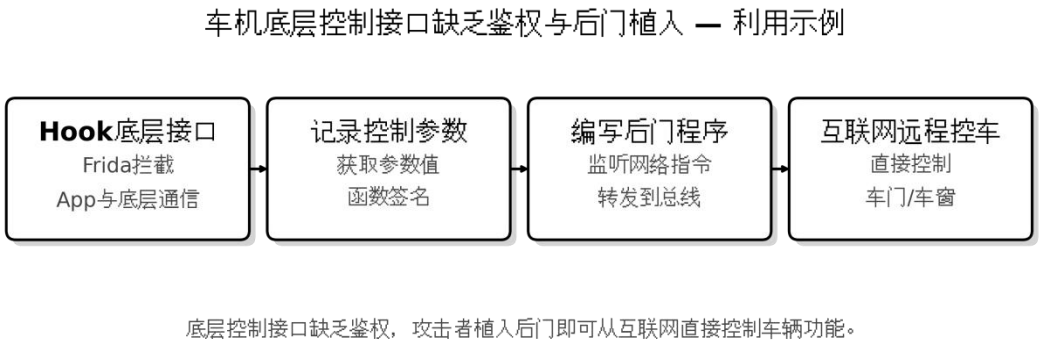


图 27 车机内部控制接口缺陷利用路径示例

4.3.2.3 USB 任意文件读取导致车机敏感信息泄露

影响：通过特制 U 盘读取系统根目录与配置文件

某车机系统支持从U盘读取音乐文件，并对U盘文件系统类型不做限制。测试发现，当插入NTFS文件系统的U盘时，攻击者可以在U盘上创建指向车机本地目录的软链接，车机在扫描音乐/文件目录时会无差别展示这些链接背后的内容。

结果是：攻击者只需插入一个经过特殊构造的U盘，即可浏览和读取车机本地根目录下大量敏感文件，包括配置、密码、证书、日志等信息，构成严重信息泄露。

成因：文件系统特性 + 目录遍历缺乏防护

问题由两部分叠加造成：

车机文件浏览/媒体扫描功能在访问U盘内容时，没有限制可访问的路径范围；

对U盘文件系统类型不做限制，允许使用支持符号链接的NTFS，攻击者因此可以在U盘上创建指向系统目录的软链接；

应用对软链接“无差别处理”，将其当作普通文件夹列出并允许访问内容。

利用示例：构造软链接U盘 → 浏览本地敏感目录

攻击者准备一个U盘，格式化为NTFS；

在电脑上挂载该U盘，创建若干软链接目录指向潜在敏感路径，如：链接到车机根目录/；链接到/etc等配置路径；

将U盘插入目标车辆的车机USB口，打开车机的“音乐”、“文件管理”或类似应用；

车机扫描U盘目录时，会将软链接当成普通文件夹展示，攻击者即可进入并查看/读取目标目录中的文件内容；

被泄露的文件中可能包含：系统配置和账号信息；与云平台通信的证书或密钥；日志中记录的Token、接口地址等，为后续云端或车内网络攻击提供情报。

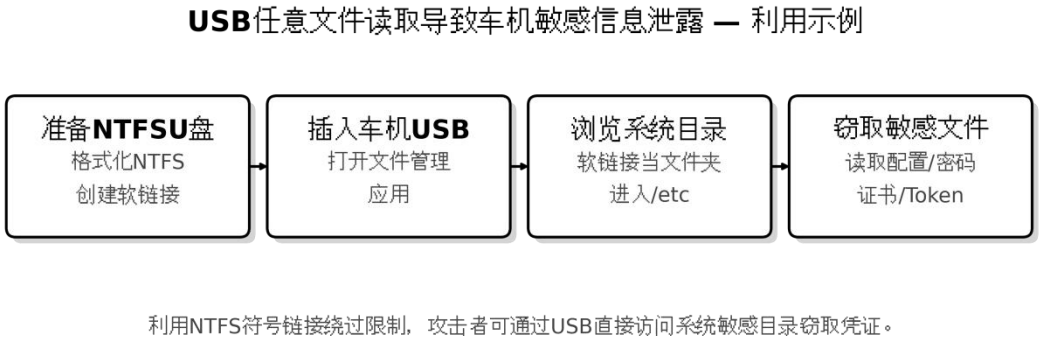


图 28USB 任意文件读取导致车机敏感信息泄露

4.4 通信与协议安全设计不足

在智能网联汽车体系中，从 GNSS/TPMS 等传感链路，到蓝牙/Wi-Fi 短距链路，再到 MQTT 等车云消息协议，共同构成了“车—云—人”的通信基础。一旦协议安全设计不足或实现存在漏洞，攻击者就可以从最外围的数据链路切入，逐步扩展到对车机、平台甚至关键 ECU 的控制。

4.4.1 中低危风险：数据可信度下降与窃听风险

这一层面的漏洞往往只被视为“传感数据不可信”或“链路可被窃听”，通常按低危或中危处理。但在真实攻击链里，它们是后续精准攻击、凭据窃取和错误决策的基础。

4.4.1.1 GNSS/TPMS 传感欺骗：影响导航与自动驾驶决策

影响：攻击者通过伪造 GNSS 或 TPMS 信号，可在车辆系统无法识别的情况下，改变车辆感知到的位置、速度、胎压状态等关键参数；在搭载高级辅助驾驶或自动驾驶功能的车型上，错误的定位和状态信息会直接影响车道保持、自动变道、自动泊车等决策，带来安全风险。

2019 年，Regulus Cyber 的研究人员在对 Tesla Model S/Model 3 进行测试时，通过构造 GPS 欺骗信号，使车辆在 Navigate on Autopilot 模式下出现不符合路线、错误减速甚至误将高速出口当作主路等行为，证明了车载 GNSS 接收机在缺乏有效认证与传感融合防护时，容易被远程欺骗。

成因：GNSS/TPMS 等无线传感协议本身大多未设计端到端身份认证与报文完整性校验；车端在融合传感器数据时，对 GNSS、TPMS 等“外部信号”的可信度缺乏动态评估机制，容易将单一传感器的异常读数直接用于决策。

利用示例：攻击者在目标路段附近布置伪造 GNSS 或 TPMS 信号发射设备；伪

造的信号在功率上覆盖合法信号，使车辆优先锁定攻击者发出的“虚假卫星”或“虚假传感器”；车辆根据错误的位置信息或胎压数据调整速度、方向或触发告警；在自动驾驶场景中，错误感知还可能被用来诱导车辆做出不安全行为。

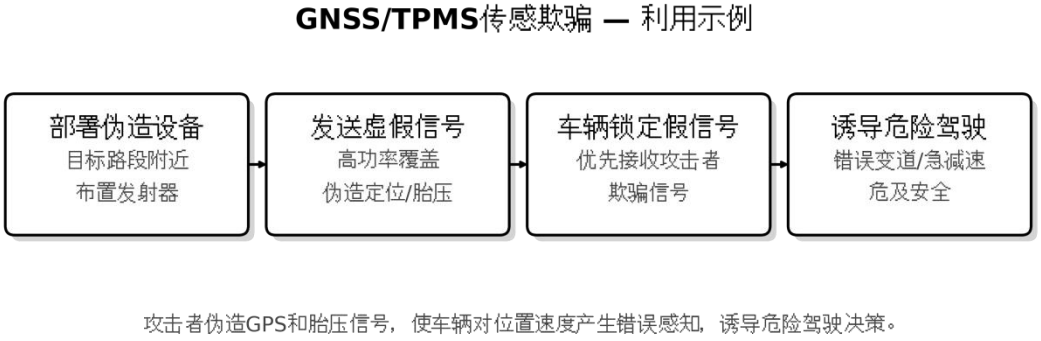


图 29 GNSS/TPMS 传感欺骗

4.4.1.2 蓝牙 HID 注入与 fuzz：从人机界面干扰到敏感操作

影响：蓝牙 HID 未做严格配对控制时，攻击者可通过 HID 注入向车机系统发送按键、触控等操作，干扰或操车辆控制机应用；结合车机上的隐藏调试菜单、工程模式或浏览器等组件，HID 注入有机会进一步触发命令执行或恶意网页加载。

2023 年披露的 CVE-2023-45866 显示，在 Linux BlueZ 协议栈中，攻击者可以在某些配置下以未认证的外围设备身份与 HID 主机建立加密连接，并发送键盘输入而无需用户确认，这一缺陷被多篇技术分析认为在车机信息娱乐系统中同样具有利用潜力。同时，开源工具 BlueFuzz 展示了针对车载 OBD 蓝牙适配器进行 fuzz 测试的可行性，说明短距蓝牙链路在汽车环境中已成为稳定可用的攻击入口。

成因：蓝牙 HID 协议中，主机对“谁可以作为键盘/鼠标连接”缺乏强约束，在某些实现中，只要设备声明 HID Profile 就能发起连接；车机 UI 设计上往往允许键盘快捷键触发系统菜单、工程模式或浏览器等高敏感功能，而这些功能本身缺乏二次认证。

利用示例：攻击者在目标车辆附近伪装成 HID 设备，尝试与车机蓝牙主机建立连接；在漏洞存在的情况下，无需车主确认即可建立加密连接；发送一系列按键/快捷键，打开浏览器或工程模式菜单，访问内置调试页面或执行预设脚本；配合其它漏洞进一步提升权限。

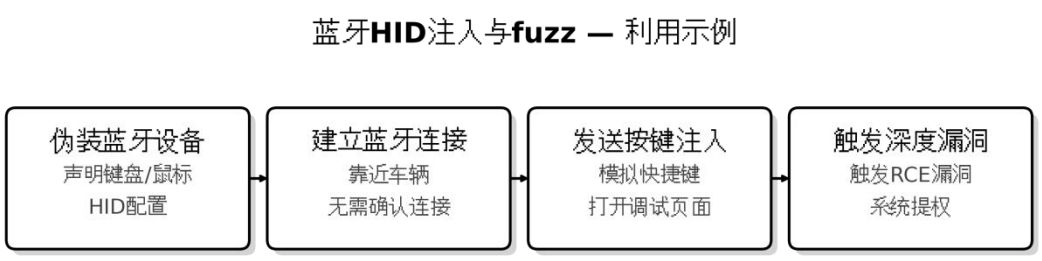


图 30 蓝牙 HID 设计缺陷的原理

4.4.1.3 MQTT 与车云消息通道配置不当

影响：在车云架构中，MQTT 被广泛用于车辆遥测上报、远程控制指令下发等场景。如果 Broker 配置不当，攻击者可以：

以匿名身份连接 Broker，订阅包含车辆位置、状态的主题，批量窃取车队数据；

向目标车辆发布伪造指令，干扰远程控制逻辑或触发大范围异常告警；

利用缺乏 TLS 或弱认证的连接，实施中间人攻击或流量窃听。

成因：MQTT 协议本身只定义了发布/订阅机制，不强制要求认证、授权与加密；实际部署中，为方便调试或快速接入，部分系统开启匿名连接或使用弱密码，且未对主题访问进行细粒度权限控制；Broker 暴露在公网或防护薄弱网段上，缺乏入侵检测与限流机制。

利用示例：攻击者扫描互联网或目标企业网段，寻找开放 MQTT 端口；尝试匿名连接或使用弱口令登录 Broker；枚举或猜测常见主题，订阅后被动收集车队遥测数据；进一步向控制相关主题发布伪造消息，干扰远程控制逻辑或构造 DoS。

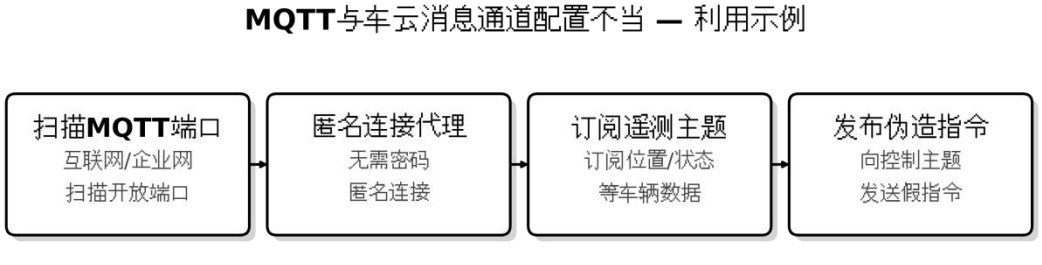


图 31 MQTT 与车云消息通道配置不当利用路径示例

4.4.1.4 车云通信链路加密与配置薄弱

影响：车辆与云端通信未启用 TLS，或者支持明文+加密双协议但缺乏严格降级防护时，攻击者可在车主不知情的情况下实施中间人攻击，窃取 Token、账号密码和车辆敏感数据；在部分旧平台或第三方服务中，使用过时的 TLS 版本和弱加密套件，也会显著降低窃听成本。

行业实践经验表明，早期自研 TCP/HTTP 协议的 TSP 平台，在业务扩展后往往面临“协议私有 + 加密不统一 + 认证逻辑复杂”的问题，进而在升级与维护过程中频繁出现配置错误和回退明文的情况。

成因：为兼容老车型或开发便捷，服务端同时开放 HTTP 与 HTTPS，或支持明文 MQTT 与 MQTT over TLS；终端对证书校验不严格，接受任意受信任 CA 签发的证书，甚至完全忽略证书错误；缺乏严格的 HSTS/ALPN 等机制，易被协议降级攻击利用。

利用示例：攻击者在公共 Wi-Fi、伪基站或车队局域网中充当网关；通过 DNS 欺骗或 ARP 欺骗，将车机或 T-Box 流量引到恶意代理；若系统支持明文或证书校验薄弱，即可实现“透明代理”，记录包含 Token、指令和车辆数据在内的全部通信；利用窃取的 Token 和接口信息，构建更高层的远程车辆控制或数据窃取攻击链。

图 32 车云通信链路设计缺陷利用路径示例

4.4.2 高危与严重风险：协议栈缺陷直接导致远程代码执行

当通信协议栈本身存在严重实现缺陷时，攻击者可以直接从通信层跨越到执行层，实现远程代码执行，风险从“窃听/欺骗”升级为“控制权获取”。

4.4.2.1 PerfektBlue：Blue SDK 蓝牙协议栈一键 RCE 影响 3.5 亿辆汽车

影响：2025 年，PCA Cyber Security 公布了名为“PerfektBlue”的蓝牙漏

洞攻击链。该攻击链源于 OpenSynergy 开发的 Blue SDK 协议栈中四个高危漏洞（CVE-2024-45431～45434），广泛集成于多家主机厂的车载信息娱乐系统。研究估计，受影响范围包括超过 3.5 亿辆汽车和 10 亿台嵌入式设备，覆盖奔驰、大众、斯柯达等多个品牌。

攻击者在特定条件下，通过一次配对交互，即可在目标车机上实现远程代码执行，继而：

访问车机内保存的通讯录、通话记录、短信、Wi-Fi 密码等敏感数据；读取或修改 GPS 位置、行程记录等隐私信息；在车机上植入持久化后门，作为后续攻击车内网络的跳板。

成因：公开技术分析显示，PerfektBlue 攻击链主要利用了以下问题：

内存安全缺陷：Blue SDK 在处理蓝牙 Profile 报文时存在缓冲区溢出和越界访问，攻击者可以构造特制 L2CAP/AVCTP 包触发写任意内存；

状态机处理不当：协议栈在连接建立和服务发现阶段的状态切换校验不足，允许攻击者在非预期状态下发送本应被拒绝的控制报文；

权限划分缺失：蓝牙协议栈与应用层在进程和权限上隔离不足，一旦在协议栈内核中取得代码执行，即可直接操控上层应用与存储。

利用示例：攻击者在车辆附近发起蓝牙配对请求，伪装为手机或常见外设；

车主接受配对，或在某些“免确认连接”场景下自动完成连接；

在服务发现、媒体控制等业务交互过程中，攻击者连续发送构造好的恶意报文，链式触发 Blue SDK 中的多个漏洞，最终劫持程序控制流；

在车机主控进程上下文中执行代码，访问本地数据或作为跳板攻击车载以太网/CAN 网络。

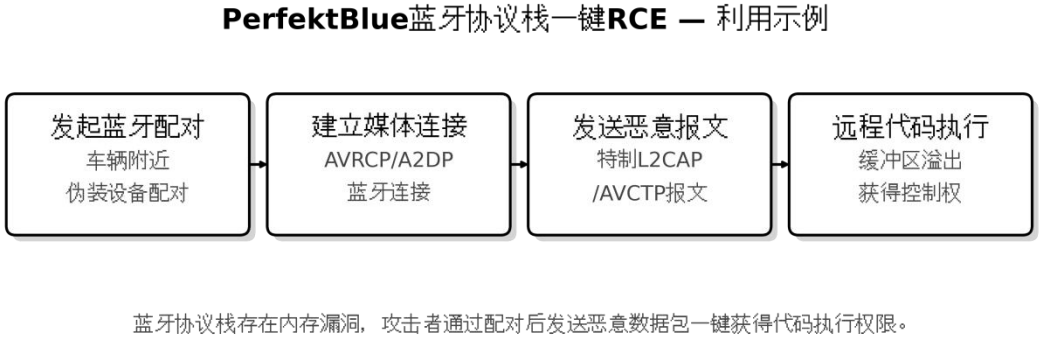


图 33PerfektBlue：Blue SDK 蓝牙协议栈一键 RCE

4.4.2.2 车机 Wi-Fi 配网协议未鉴权导致远程控制车机连接任意外部热点

影响：攻击者可强制车机连接指定恶意 Wi-Fi 网络

在某量产车型的信息娱乐系统中，车机对外提供了一个仅在车载热点内网暴露的 TCP 服务端口，用于与手机等设备交互，实现蓝牙配对、Wi-Fi 配网等功能。安全测试发现：

连接车载热点后，无需任何认证即可与该 TCP 服务建立连接；

通过逆向该私有协议并构造特定“Wi-Fi 配网请求”消息，攻击者可以向车机下发任意 SSID 和密码；

车机会自动断开当前网络，按照攻击者指定的配置连接到目标 Wi-Fi，整个过程无需车主在车机界面上确认。

一旦车辆接入攻击者控制的网络：车机与云端、第三方服务的通信都将经过攻击者网关，便于实施中间人攻击、凭据窃取；如果车机自身还存在远程管理接口或调试服务，攻击者即可在该网络中继续横向渗透，获得更高权限。

成因：热点内 Wi-Fi 配网协议缺乏身份认证与用户确认

未鉴权的 TCP 服务，当车辆开启自身热点后，车机在热点网关地址上监听一个固定 TCP 端口；任何接入该热点的设备都可以与该端口建立连接，不需要账号密码或 Token。

私有二进制协议只做格式校验，不做身份校验。协议以固定开头/结尾字节序列和“消息 ID + 长度 + 数据”的格式封装，比如有“获取车机信息”“Wi-Fi 配网请求”等多种消息类型；服务端仅验证消息结构是否正确，不对发送方身份进行任何校验——只要数据字段合法，就会执行对应操作并返回成功响应。

缺乏车主交互与安全策略，当收到“Wi-Fi 配网请求”消息时，车机直接使用其中的 BSSID/SSID/密码更新配置，并尝试连接目标网络；协议层面没有“是否需要车主确认”的字段，UI 也不会弹出提示，更未实现白名单、证书校验或地理/场景限制。

利用示例：开启热点 → 连接内网服务 → 下发恶意配网指令

进入车载热点网络。攻击者可通过多种方式触发车辆开启热点，例如在短时物理接触场景下经由诊断接口发送指定 CAN 报文开启热点，或利用其它车机漏洞

远程开热点；在热点开启后，使用手机/电脑连接车载热点，获得一个内网 IP。

探测并连通私有协议端口。扫描车载热点网段，发现车机网关 IP 上开放的特定 TCP 端口；根据逆向结果实现协议客户端，构造“HeadUnit 信息请求”等消息，确认协议正常工作并获取车机硬件/软件版本等信息。

构造 Wi-Fi 配网请求。根据逆向分析的协议细节，封装“Wi-Fi 配网请求”消息，在数据区写入攻击者自建 AP 的 BSSID、SSID 和密码；将完整报文通过 TCP 连接发送至车机服务端口，收到表示成功的响应。

车机自动接入恶意 Wi-Fi。车机按照收到的配置连接攻击者的 Wi-Fi 网络；攻击者随即可在该网络中对车机进行流量劫持、端口扫描和进一步利用，例如：伪造云端证书或利用证书校验缺陷窃取访问 Token；扫描车机在新网络上的其它管理端口和服务，实现更深层渗透；若同一 Wi-Fi 覆盖多辆车，还可以对多个目标重复上述过程。

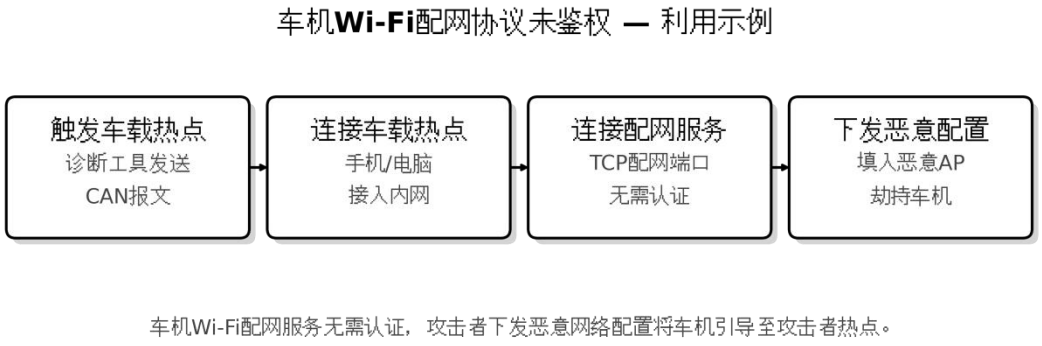


图 34 车机 Wi-Fi 配网协议未鉴权导致远程控制车机连接任意外部热点

4.5 网络暴露面与边界隔离治理缺失

在车联网体系中，云平台、内部网络与数据基础设施构成了车辆与用户服务的关键基础设施。如果网络暴露面与边界隔离治理缺失，攻击者即便无法立刻车辆控制，也可以通过开放端口、扁平网络和数据资产集中暴露，构造出从企业 IT → 车云平台 → 车端设备的完整攻击路径。

4.5.1 中低危风险：攻击面扩展与情报泄露

这一层面的缺陷通常体现为“安全基线缺失”，单点看似只是资产暴露或信息泄露，但会极大扩展攻击面、为后续高危攻击提供关键情报。

4.5.1.1 云端管理端口与服务“超标暴露”

影响：车云平台、远程诊断服务、日志与监控系统等暴露过多管理端口，为

攻击者提供丰富的扫描与攻击目标；开发测试环境与生产环境同时暴露在公网，测试环境往往使用弱口令、默认配置，成为切入真实业务数据和控制面的“非授权访问路径”。

Upstream 的 2024—2025 年度报告显示，车载远程通信与应用服务器已成为汽车网络安全事件中最主要的攻击面之一：2024 年，针对车载远程通信和应用服务器的攻击占比从 2023 年的 43%上升到约 66%，而 2024 年全部事件中约 60%影响范围达到成千上万甚至数百万辆车、充电站或账号，说明以云端和后台系统为中心的“大面攻击”正在成为常态。

成因：资产管理与暴露面治理不完善，缺乏“最小暴露面”原则，未按功能和敏感度分层部署服务；安全与运维职责割裂，开发自建的调试面板、内部监控 UI 没有统一纳入安全审计和访问控制；对公网暴露服务缺少持续的自动化资产盘点与渗透测试，旧版本组件与遗留接口长期在线。

利用示例：攻击者使用端口扫描、搜索引擎或云资产扫描工具，定位车企及其子公司名下的公开 IP 和域名；识别其中的未加固管理端口、测试环境登录页面或旧版本中间件；利用弱口令、默认凭据、已知漏洞实现初始入侵；在获取控制权后，进一步查找与车联网平台、TSP 后台、车机 OTA 管理等相关的内部系统，为后续横向移动做准备。

图 35 云端管理端口与服务“超标暴露”

4.5.1.2 信息娱乐域与控制域隔离不足

影响：部分车型的车内网络仍呈“扁平化”或“弱分区”特征：

信息娱乐域、远程信息处理域与动力/底盘控制域通过网关连接，但网关规则较为宽松；

诊断接口接入的 CAN 总线既能访问舒适域/车身域，又能直接或间接访问动

力/制动等安全关键 ECU；

网关缺少细粒度的报文过滤和基于安全等级的访问控制，导致低安全等级节点可以观察或影响高安全等级域的报文。

这类架构问题在初期常被视作“设计缺陷而非漏洞”，但它让任何一个被攻陷的车内节点都有潜力成为进入安全域的中转站。

Jeep Cherokee 2015 年的经典远程入侵案例就说明了，正是因为信息娱乐单元与控制域之间缺乏足够的网络隔离，研究人员才能从 Uconnect 头单元逐步横向移动到底盘控制 CAN 总线，最终影响转向、制动和油门。

成因：车辆电子电气架构从传统分布式向域控制/集中式演进过程中，历史兼容与成本压力导致“软分区多、硬隔离少”；许多车型的网关更侧重功能路由和诊断方便，而非“安全域边界”，仅做简单 ID 过滤或速率限制；车内总线协议缺乏源地址与认证机制，任何接入同一总线的 ECU 都可以发送伪造报文。

利用示例：攻击者先通过 USB、蓝牙/Wi-Fi、T-Box 等入口获取 IVI 或某个非安全域 ECU 的代码执行；利用该 ECU 上的 socketCAN、D-Bus 或网关 API 发送/监听车内网络报文；在扁平架构下，成功观察到动力/制动等控制域的报文格式与 ID 分布；为后续构造 DoS、注入或重放攻击打下基础。

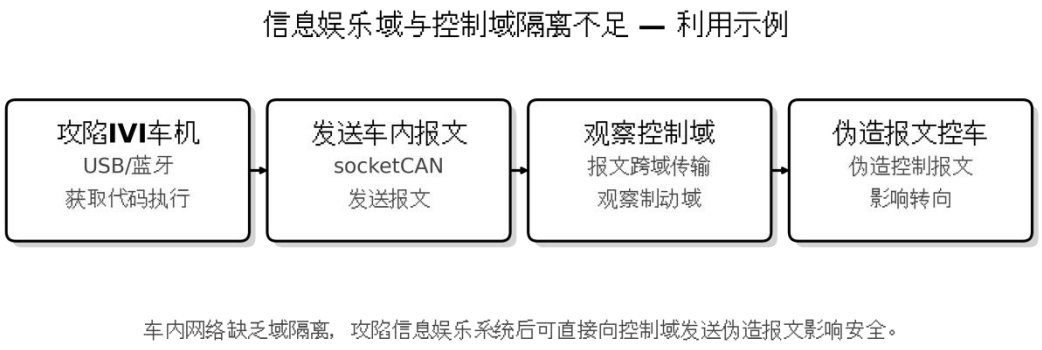


图 36 车内网络扁平化与弱分区风险

4.5.1.3 日志、备份与大数据平台中的隐私和敏感业务数据暴露

影响：车联网平台将车辆定位、行程记录、充电记录、驾驶行为评分等数据集中存放于日志系统、对象存储或大数据平台；若这些平台访问控制、加密与审计薄弱，一旦发生误配置或被攻破，就可能导致数年跨度的海量历史数据被一次性导出。

2023 年 Toyota 多起数据泄露事件中，最受关注的是其云端误配置导致的长

达近十年的车联网数据暴露：约 215 万名日本客户的车辆位置历史、车载终端 ID、VIN 号等数据因为云数据库“公开访问”设置错误，从 2013 年 11 月一直暴露到 2023 年 4 月。随后 Toyota 在全面排查中又发现多个云环境存在类似问题，部分导航数据和客户信息在 2015—2023 年间可被外部访问，暴露用户数量再度增加。

成因：日志与大数据平台在设计时更关注可用性与性能，对“数据最小化”和脱敏未充分考虑；云对象存储、数据仓库等资源采用默认公开或宽松访问策略，缺乏统一的配置基线和自动审计；数据分级与生命周期管理不到位，历史定位、行程和视频数据长年保留且缺乏再评估。

利用示例：攻击者通过搜索引擎或云资产扫描工具枚举出误配置的存储桶、数据库或日志服务；在访问控制缺失或配置错误的前提下，直接下载包含车辆位置、终端 ID、VIN、视频等敏感数据的文件；利用这些数据对特定高价值目标进行行程分析、行为画像或物理跟踪；如与其它漏洞结合，还可将数据与实时远程控制能力叠加，形成更危险的威胁场景。

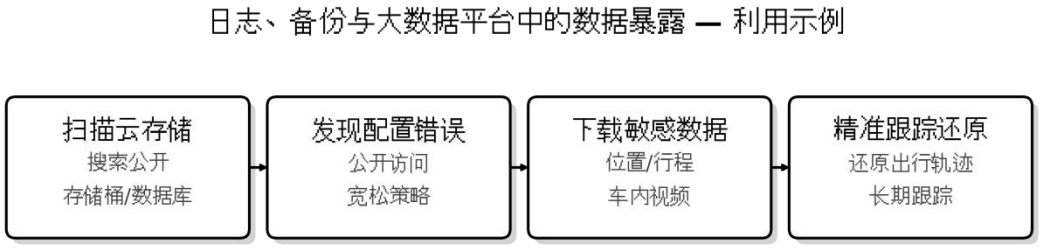


图 37 日志、备份与大数据平台中的隐私和敏感业务数据暴露

4.5.2 高危与严重风险：大规模数据与服务受损

当网络暴露面与数据保护问题与身份认证缺陷、访问控制漏洞、协议栈问题叠加时，攻击者不仅可以大规模窃取数据，更有机会对数百万辆车或关键服务实施远程控制与破坏。

4.5.2.1 云存储与日志平台误配置：Toyota 位置数据十年暴露

影响: Toyota 在 2023 年披露，其用于 T-Connect、G-Link/G-BOOK 等车联网服务的云环境中，由于访问权限配置错误，导致约 215 万名客户的车辆数据在长达约 10 年的时间内暴露于公网。相关数据包括：

车辆的定位信息及到达时间；

车载终端 ID 与 VIN；

部分行车记录仪采集的视频。

后续调查又发现另一起云配置错误，致使约 26 万名车主的车载导航数据和设备 ID 等信息在 2015—2023 年间可被外部访问。

成因：云对象存储或数据库实例被设置为“公开访问”，任何互联网用户无需认证即可访问部分数据；数据集中存放了跨品牌、跨车型、多年的车联网服务日志和位置历史，缺乏分区隔离和最小必要原则；数据处理规则和云配置管理制度未在组织内部得到充分贯彻，导致误配置长期未被发现。

利用示例：攻击者通过云资产扫描或自动化脚本，搜索开启公共访问的存储桶和数据库实例；

在无需认证的情况下，列举和下载其中的数据文件；

通过 VIN、终端 ID、时间戳与位置坐标还原用户多年的出行轨迹；

若与其它数据源结合，可对特定目标进行长期行为画像和物理跟踪。

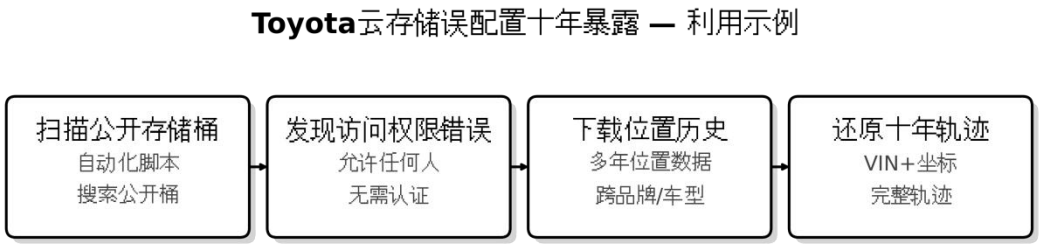


图 38 云存储与日志平台误配置：Toyota 位置数据十年暴露

4.5.2.2 某车企社区小程序接口设计缺陷导致百万级用户数据泄露

影响：百万级用户手机号、用户名等隐私信息被枚举获取

在某车企的车主社区小程序中，安全测试发现其用户资料查询接口存在严重的访问控制缺陷：

接口只要收到包含 userId 的请求参数，就会返回对应用户的完整资料；

返回数据中包含手机号、用户名、用户 ID、注册来源、注册时间、头像地址、发帖/评论统计等多项个人信息；

接口对 userId 参数几乎不做限制，可以被遍历和猜测。

通过简单脚本对该参数进行规律遍历，测试人员验证可以批量获取数量级达到百万的用户信息记录，导致大规模个人隐私数据泄露。对于攻击者而言，这类数据可进一步用于短信诈骗、账号撞库、钓鱼攻击乃至针对车主的定向社工。

成因：缺乏基于主体的访问控制，仅按 ID 返回敏感数据

接口设计为“只要给 ID 就返回数据”。服务端将 userId 视作查询主键，只要参数存在且格式正确，就会查询并返回对应用户资料；没有校验当前请求的登录用户是否为该 userId 对应用户本人，或是否具备查看其完整资料的权限。

缺乏最小化与脱敏。接口返回了手机号、用户行为统计等敏感字段，而非必要的公开资料子集；对于被访问对象与调用场景未进行区分，例如“自己看自己”与“查看陌生用户”返回相同的详细数据。

ID 设计和检测防护不足。userId 呈现出明显的数值区间和递增规律，便于通过简单遍历或邻域扫描枚举大量有效账号；缺乏针对异常访问模式的频率限制、行为风控和告警机制，连续高频查询不会触发阻断。

本质上，这是把“按 ID 查用户”的内部管理接口直接暴露给终端，而没有配套的授权与脱敏策略。

利用示例：抓包获取请求样例 → 遍历 userId → 批量导出用户库

获取接口调用方式。攻击者在正常使用车主 App 或小程序时，通过浏览器开发者工具或抓包工具，记录某次查看用户主页/资料时发送的请求；观察到请求体中含有 userId 参数，响应中返回对应用户的详细信息。

验证越权访问。将请求中的 userId 手工改为其他值，再次发送请求；若接口仍正常返回另一名用户的详细信息，则确认存在横向越权和隐私泄露问题。

脚本化批量枚举。攻击者分析 userId 的取值范围和规律，构造遍历策略；使用脚本对大量 userId 进行自动请求，解析响应中的 userPhone、userName、userId 等字段，写入本地数据库；由于缺乏频控与风控机制，这一过程可以在较短时间内收集到百万级用户数据。

后续滥用场景。将收集到的手机号、昵称等信息导出到黑灰产生态，用于短信诈骗、伪装车企客服进行钓鱼、针对车主的精准社工；将泄露的 userId 与其它车联网接口或账号体系中的标识进行关联，为进一步的账号接管、车辆信息查询等攻击提供索引。

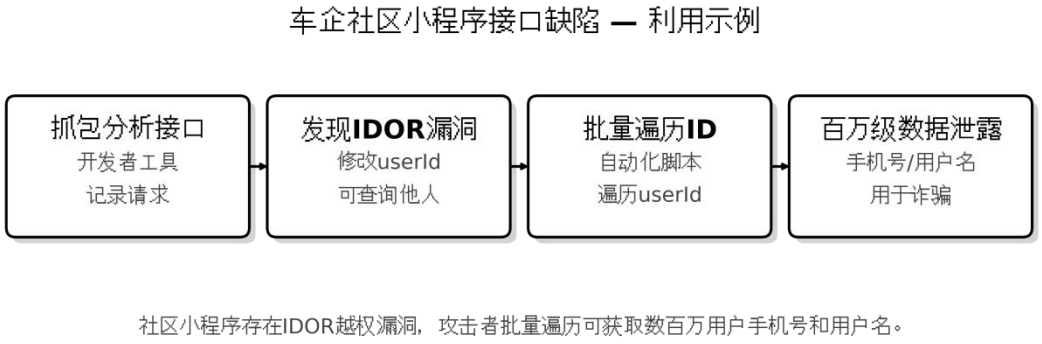


图 39 某车企社区小程序接口设计缺陷导致百万级用户数据泄露

五、技术风险趋势与潜在攻击面研判

本章在年度漏洞样本与典型案例根因分析基础上，进一步回答两个问题：其一，哪些漏洞形态正在成为智能网联汽车体系中的“高频复现的共性薄弱点”；其二，云-管-端架构与新技术引入正在把攻击面扩展方向、以什么方式被放大。总体上看，高危与严重问题的形成越来越依赖“系统性耦合”：认证与会话、授权模型、通信链路、工程接口、云端暴露面与数据治理相互叠加，使得攻击路径从单点缺陷演化为可复用的攻击链。

5.1 高频复现的共性薄弱点

5.1.1 签名与防重放机制的客户端信任误区

在多个车辆控制接口案例中，签名算法完全实现于客户端且密钥固化在 App 内部，随机串与时间戳由客户端生成并上送，服务端缺乏对请求来源环境的校验；一旦攻击者通过中间人或终端侧手段截获 Token，即可复现签名逻辑并构造伪造的合法请求，形成持久化远程车辆控制能力。

更隐蔽的情形是“统一密钥 + 可控 nonce”的伪防重放：nonce 由客户端拼接生成但服务端不做唯一性校验、所有用户共享同一密钥，导致攻击者在获得一次 Bearer Token 后即可长期伪造任意车辆控制指令，绕过防重放并实现任意次数的云端车辆控制操作。这一类问题之所以在今年显著“高频”，本质上与智能网联汽车业务对移动端快速迭代、跨版本兼容的工程实践中的路径依赖有关：普遍将“签名存在”等同于“请求可信”，而没有把强身份、设备绑定、风险控制与指令分级作为服务端的主安全边界。

5.1.2 静态标识替代强认证与业务逻辑缺陷的规模化风险

在远程信息处理平台与车云 API 设计中，把 VIN 等静态标识当作主要授权凭

据的风险在今年仍然突出：只要请求参数中的 VIN 与平台记录匹配即认为请求可信，同时缺乏强身份验证与精细风控，攻击者可自动化尝试大量 VIN 并对对应车辆执行远程操作。

同类风险还体现在 IDOR/对象越权与“车辆绑定/解绑、分享授权”等业务链路中。其危险性并不仅限于“数据越权”，而在于攻击者可以在已登录或看似合法的前提下跨账号、跨车辆甚至跨车队地滥用能力，从中低危迅速升级为大范围位置跟踪或批量车辆控制的攻击起点。

5.1.3 消息通道与遥测协议的配置型缺陷

MQTT 在车云架构中被广泛用于遥测上报与指令下发，但现实部署中为调试与快速接入而开启匿名连接、弱口令、缺乏主题级权限控制的现象仍然常见；一旦 Broker 暴露在公网或薄弱网段，攻击者即可批量订阅车辆位置与状态主题，甚至向控制主题发布伪造指令干扰远程控制逻辑。

与之相伴的，是链路加密与协议降级治理不足：车辆与云端通信未启用 TLS、或同时开放明文与加密协议但缺乏严格降级防护时，攻击者可在公共 Wi-Fi/车队局域网环境中实施中间人攻击，窃取 Token、账号密码和车辆敏感数据，进一步为云端车辆控制与数据窃取攻击链提供必要条件。

5.2 新兴技术栈引入的潜在安全信号

今年的风险信号之一，是攻击面从“业务接口”继续向“协议栈与底层组件”延伸：当通信协议栈本身存在严重实现缺陷时，攻击者可以直接从通信层跨越到执行层，实现远程代码执行，风险从窃听/欺骗跃升为控制权获取。这一趋势与车载系统广泛引入第三方协议栈、SDK 与复杂中间件有关，尤其在蓝牙/Wi-Fi 等短距链路与车机多媒体系统中更为集中。

我们持续跟踪到的一个高风险信号是，传感与融合链路的安全性正在成为自动驾驶/辅助驾驶时代的“潜在攻击面”，GNSS/TPMS 等无线传感协议在身份认证与完整性校验技术应用中缺少使用有效安全强度的校验算法或机制。若车端融合策略对外部信号可信度缺乏动态评估，攻击者可通过伪造信号改变车辆感知到的位置、速度、胎压等参数，进而影响车道保持、自动变道、自动泊车等决策链路。这类问题往往不以传统“漏洞利用”形式出现，却可能直接映射到安全风险，应纳入智能网联汽车整体威胁建模与测试体系。

在车端诊断与维保技术栈方面，UDS SecurityAccess 的 seed/key 机制仍是需要重点关注的长期风险源：当 seed/key 算法过于简单或实现泄露，攻击者在具备物理接触条件下可逆向或暴力破解获取扩展会话权限，进而对关键 ECU 执行高风险诊断命令；相关研究与工具的公开化使这一风险更具现实可行性。

5.3 攻击面扩展趋势与放大机制

5.3.1 云端暴露面治理不足：形成“企业 IT—车云平台”攻击链

车联网云平台、内部网络与数据基础设施作为车辆与用户服务的中枢，一旦网络暴露面与边界隔离治理缺失，攻击者即便无法立刻车辆控制，也可能通过开放端口、扁平网络与数据资产集中暴露，构造从企业 IT → 车云平台 → 车端设备的完整攻击路径。

在样本与事件归纳中，管理端口与服务“超标暴露”、开发测试环境与生产环境同时暴露在公网、测试环境弱口令/默认配置成为后门通道，是反复出现的共性问题；其背后往往是资产管理与暴露面治理不完善、缺乏最小暴露面原则，以及调试面板/内部监控 UI 未纳入统一审计与访问控制。

5.3.2 公共网络与“移动端—云端”链路：形成低门槛攻击入口

在典型车辆控制案例中，攻击者通过公共场所仿冒 Wi-Fi 热点与中间人手段截获 Token 与请求结构，再结合可复现的客户端签名机制，即可在任意终端构造车辆控制请求，形成从“仿冒 Wi-Fi 热点”到“持久远程车辆控制”的攻击链。这类路径的共性在于：弱点不只在“加密是否存在”，更在于服务端缺乏对设备、证书、来源环境与行为异常的校验，使得泄露的会话凭据能够脱离原上下文被反复滥用。

5.3.3 车端“工程接口与日志治理”：仍是攻击链的高价值情报节点

车端 USB/调试接口、工程模式与日志导出能力的长期保留，使攻击者在租赁、维修或共享车辆场景下能够导出日志与配置文件，进一步提取 Token、后台域名、接口路径、密钥片段等关键信息，并与移动端逆向、网络抓包结合拼出完整的车云攻防视图，成为后续中间人攻击、签名复现或命令注入的前置条件。

5.4 安全能力提升与技术建议

本年度样本呈现出一个清晰信号：中低危问题多落在“基线、配置与信息最小暴露”，高危及以上问题则集中在云-管-端关键链路，往往由认证会话缺陷与

接口授权模型叠加触发，最终表现为远程车辆控制、车队级滥用或大规模数据泄露。因此，能力建设不能只停留在漏洞发现与修复的循环，而应面向攻击链进行体系化管控。本章从检测、治理、加固、运营四个维度，提出与前述风险态势逐项映射的体系化建议。

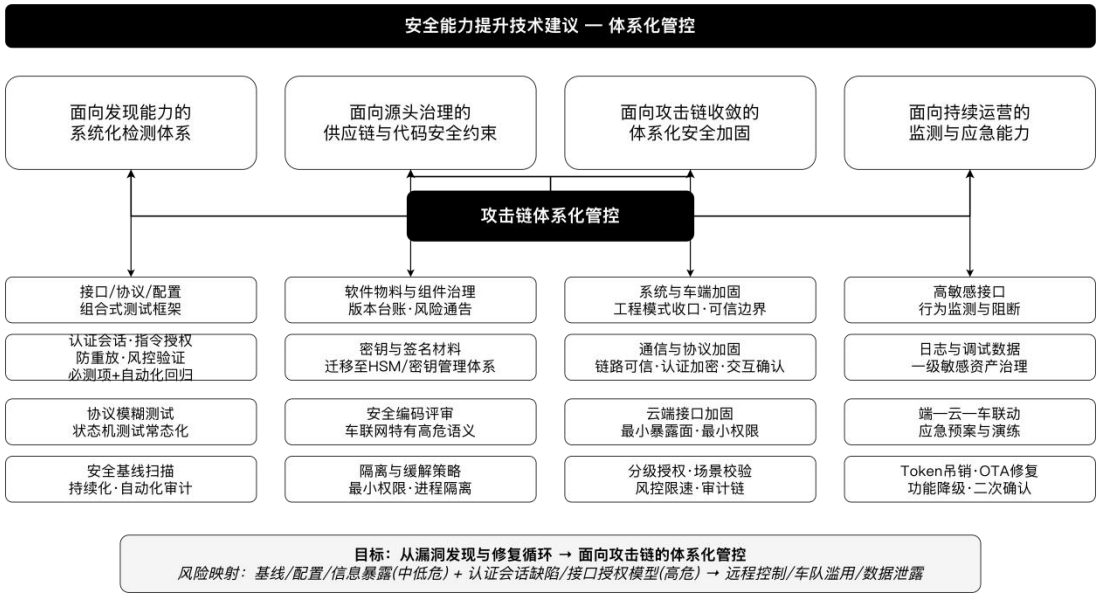


图 40 安全能力提升技术建议进行体系化管控

5.4.1 面向发现能力的系统化检测体系

智能网联汽车系统的测试对象横跨车端固件、车机应用、云端平台、移动端与通信链路，单点扫描或单一阶段的渗透难以覆盖真实攻击路径。建议将年度高频根本原因沉淀为“可复用的测试资产库”，以接口/协议/配置三类对象为核心建立组合式测试框架。

在云端与移动端接口层，应把认证会话、指令授权、防重放与风控验证作为“必测项”，并以自动化回归固化。典型问题如：Token 可被窃取且未绑定设备或 TLS 会话上下文、服务端只校验签名与 Token 匹配即放行、签名算法与密钥暴露在客户端导致可复现伪造请求等，都应在测试框架中形成可执行的检查规则与用例集。另外，车辆绑定/解绑、分享授权等业务接口要按“业务语义”建立测试断言：接口不仅要验证“请求来自已登录用户”，更要验证“调用者是否对该 VIN/vehicleId 具有所有权或被授权关系”，否则很容易从越权访问升级到车队级控制与跟踪。

在车端与通信协议层，应把协议模糊测试与状态机测试常态化。实践表明，

短距链路与私有协议往往因“缺少身份认证 + 缺少用户确认”而成为攻击入口，例如车机热点内网暴露的配网 TCP 服务，连接后无需认证即可下发任意 SSID/密码并强制车机切网，进一步为中间人攻击、凭据窃取与横向渗透创造条件。对 MQTT 等消息通道，应同时覆盖“配置与权限”测试：匿名连接、弱认证、主题 ACL 粗放、缺少 TLS 等问题会直接带来批量数据订阅与控制主题投递风险。

最后，建议把“安全基线扫描”从一次性动作做成持续能力：资产暴露面、端口开放策略、测试环境与生产环境隔离、日志与调试开关等，均可通过自动化基线审计与告警持续收敛，从而降低中低危问题的反复出现，并减少其在攻击链中的“铺垫价值”。

5.4.2 面向源头治理的供应链与代码安全约束

在智能网联汽车场景里，严重事件往往不是“一个 bug”导致，而是第三方组件、配置习惯与研发流程共同放大风险：云端暴露的管理端口与遗留服务、车机/车端保留的工程机制、以及客户端固化的密钥与签名逻辑，都会让攻击者获得稳定可复用的武器化条件。

建议从三个层面做供应链与代码安全的刚性要求：

第一，建立可追溯的软件物料与组件治理。对车机系统、中间件、蓝牙/Wi-Fi 协议栈、消息组件与云端基础组件形成统一的版本台账与风险通告机制，确保高风险组件能被快速定位到车型/版本/部署域并推动升级。对于难以及时升级的组件，必须配套“隔离与缓解”策略（最小权限、进程隔离、接口限权、WAF/网关策略），避免协议栈缺陷直接跨越到执行层。

第二，把“密钥与签名材料”从客户端/普通配置中迁移出去。前文案例中，appKey/APP_SECRET 固化在 App 内，导致签名可被逆向复现；同时服务端缺乏来源环境校验，使得伪造请求具备现实可行性。建议将高敏感指令的认证与签名放在服务端可控边界内完成：密钥进入 HSM/密钥管理体系；对指令下发引入“服务端签发 + 设备/账户上下文绑定 + 一次性挑战”的组合，而不是依赖客户端自证。

第三，把安全编码与评审重点从“通用缺陷”转向“智能网联汽车特有高危语义”。例如：绑定/解绑、分享授权、车辆控制指令的权限分级与二次确认、Token 生命周期与退出失效机制、风控与限速策略等，都是高危漏洞最常出现的

业务土壤。

5.4.3 面向攻击链收敛的体系化安全加固

（1）系统与车端加固：先收口“工程能力”，再建立可信边界。

多起车端问题的共同点是：工程模式长期保留、USB/调试接口可导出日志与配置、甚至存在自动执行脚本等出厂时遗留的调试机制，使得攻击者在维修、租赁或短时接触场景下能够快速获得系统情报甚至 Root 能力。因此建议优先完成两类收口：其一，工程模式与调试服务在量产形态必须默认关闭，并通过强认证、授权审批与审计告警控制开启窗口；其二，日志导出与诊断能力要做权限分级与数据脱敏，避免将 Token、密钥片段、接口地址作为“可复制的万能钥匙”暴露在工程日志中。

同时，车机内部的“本地调用默认信任”需要被系统性纠正：当底层控制服务对所有本地进程开放、缺少基于签名/SELinux 上下文的访问控制时，一旦攻击者通过任意入口植入后门，本地即可绕过 UI 与业务逻辑直接车辆控制。因此应把敏感控制 API 当作“安全边界”设计：调用方白名单、权限标签、最小能力集与行为审计缺一不可，并与远程指令的授权模型保持一致。

（2）通信与协议加固：把“链路可信”落实到认证、加密与交互确认。

针对热点内私有配网协议这类问题，关键不是"协议是否私有"，而是"是否把身份认证与用户确认当作默认要求"。当接入车载热点后无需认证即可建立 TCP 连接并下发配网指令，车机还无需车主确认就自动切网，这等同于给攻击者提供了构造中间人环境的快速通道。因此，配网、绑定、钥匙下发等涉及网络切换或信任关系变更的能力，应引入强身份校验、一次性挑战、以及可感知的车主交互确认，并配套白名单策略与异常切网告警。

对 MQTT 等消息通道，建议从“部署默认安全”入手：禁用匿名连接、强制 TLS、主题 ACL 精细化到车辆/账号/租户维度，并将 Broker 暴露面收敛到受控网段，配合入侵检测与限流策略，避免被互联网扫描直接命中。

（3）云端接口与数据平台加固：从最小暴露面到最小权限。

云端管理端口与服务“超标暴露”、测试环境与生产环境同暴露等问题，会把车联网平台变成“大面攻击”的中心入口。建议以资产治理为抓手：持续资产盘点、暴露面基线、分层分域部署与强访问控制，并将日志平台、对象存储与数

据仓库纳入同等强度的配置审计，避免长期误配置导致的海量数据外泄。

在业务接口层，车辆控制与高敏感指令必须建立“分级授权 + 场景校验 + 风控限速”的组合：仅凭 VIN 或简单会话参数就执行远程操作、退出登录后 Token 不失效、或服务端对 Token 使用上下文缺乏校验，都会让攻击者在获取一次凭据后长期保持控制能力。因此应对车辆控制、位置、钥匙、绑定关系变更等操作配置独立的会话策略与二次校验，并在后台形成可追溯的审计链。

5.4.4 面向持续运营的监测与应急能力

智能网联汽车安全的难点之一在于“问题具有跨域传播性”：一个看似中低危的日志泄露、端口暴露或越权查询，往往在攻击链中承担“情报与入口”的角色，最终与会话缺陷、授权缺陷叠加，形成远程车辆控制或车队级风险。因此持续监测应围绕“攻击链关键节点”设置可操作的检测面，而不仅是泛化的告警堆叠。

一是建立面向高敏感接口的行为监测与阻断能力。对车辆控制、绑定关系变更、授权分享等接口，监测维度至少应覆盖：异常频次与并发、跨地域/跨设备使用、Token 异常复用、请求签名参数异常分布、以及 VIN/vehicleId 的枚举特征。一旦出现“低成本批量化”的迹象，应具备自动限流、强制二次验证、短时封禁与人工复核的联动机制。

二是把“日志与调试数据”当作一级敏感资产治理。前文已指出日志中可能包含 Token、接口信息与内部结构情报，一旦被滥用就会演变为长期可用的后门钥匙。建议建立日志分级、脱敏、访问审批、导出审计与水印追踪机制，并对日志平台自身的账号权限、检索行为和异常下载进行监测。

三是形成面向“云-管-端”联动的应急预案与演练机制。智能网联汽车事件处置往往不是单系统关闭即可解决：既要能在云端快速吊销/轮换密钥与 Token、调整风控策略，又要能对车端进行分批 OTA 修复、对高风险功能进行临时降级或强制二次确认，同时评估对车主体验与行车安全的影响。对“签名材料泄露/可复现”“Token 长期有效”“绑定授权逻辑缺陷”等典型场景，建议形成标准化应急响应流程，并纳入季度演练，以保证真实事件发生时能够在小时级完成风险遏制与风险扩散控制。

六、行业治理与合规风险分析

6.1 漏洞态势的合规映射

本报告所揭示的年度漏洞态势，对已正式实施的 GB 44495-2024《汽车整车信息安全技术要求》与 GB 44496-2024《汽车软件升级通用技术要求》具有直接的合规映射意义。两项强制性国家标准已于 2026 年 7 月 1 日起正式实施，自该日期起，所有新申请型式批准的 M 类、N 类汽车整车产品，均须满足上述标准在整车信息安全管理体系、车内外通信安全、软件升级（OTA）安全等方面的技术要求;对于已获得型式批准的在产车型,则按照标准规定的过渡期安排执行，需在过渡期届满前完成符合性整改与重新申报。

在整车信息安全方面，GB 44495 对“车辆外部连接安全”提出了明确要求。本报告发现的大量云端接口认证会话缺陷、车云通信链路明文传输或降级风险、以及远程车辆控制指令防重放机制失效等问题,直接对应该标准中关于车辆与外部通信的安全性要求。特别是报告中的严重级远程车辆控制案例——包括签名可复现、统一密钥泄露、Token 长期有效且缺乏上下文绑定等——一旦在量产车型中存在，将构成对强制性标准的实质性偏离。

在软件升级安全方面，GB 44496 对 OTA 升级链路的完整性、真实性及安全启动提出了验证要求。本报告中发现的工程模式未收口、U 盘自动执行脚本获取 Root 权限、以及诊断服务 seed/key 算法薄弱等问题，表明部分车型在软件升级信任链的源头仍存在治理缺口，这将直接影响 OTA 安全机制的根基。

从 UNECE R155 的 CSMS 体系角度看，本报告归纳的五大高频根因类别，为企业的网络安全管理体系提供了明确的风险评估输入。CSMS 要求组织具备系统化的风险识别、评估、处置与监控闭环，而本报告所揭示的“中低危漏洞充当攻击链铺垫入口”这一规律，恰恰说明当前许多 CSMS 实践在风险链路评估上存在薄弱环节，往往将中低危漏洞视为可接受的残余风险，而忽视了它们在攻击链中的放大效应。建议企业在 CSMS 体系中将本报告的“攻击链视角”纳入风险评估方法论，对中低危漏洞按其在整个攻击链中的角色进行二次评估。

6.2 面向行业协同的治理建议

基于本报告的四级漏洞分级体系及年度态势发现,提出以下面向行业监管协

同的建议：

一是推动漏洞分级的行业统一。当前智能网联汽车安全漏洞的分级仍存在整车企业、供应商、安全厂商之间口径不一致的问题，导致漏洞数据难以横向比较和聚合分析。本报告所采用的四级分级体系（低危/中危/高危/严重）和双维度判定方法（可获取性×影响程度），与我国《汽车安全漏洞分类分级评价》国家标准项目方向一致，可作为行业共享的参考口径。

二是建立关键漏洞的强制报送与协同披露机制。对于严重级漏洞——特别是涉及远程车辆控制、大规模数据泄露、OTA 信任链破坏等直接影响行车安全与用户隐私的问题——建议在行业层面建立强制报送机制，并借鉴航空业的“安全报告系统”经验，通过匿名化、免责化的方式激励企业和安全研究者主动上报，加速风险收敛。

三是针对五大高频根因制定行业安全基线。报告的五类根因（身份认证与会话管理、访问控制与权限模型、设备与固件安全防护、通信与协议安全设计、网络暴露面与边界隔离治理）覆盖了智能网联汽车安全的主要薄弱面。建议在行业层面针对每类根因制定最低安全基线，如：高敏感指令接口必须实现服务端签名与设备绑定、车辆绑定/解绑必须经原车主确认、工程模式出厂须默认关闭且开启需强认证等，将“事后修复”转向“事前合规”。

四是推动测试能力的行业共享与互认。本报告指出，智能网联汽车安全的测试复杂度高、覆盖面广、专业性强，单一企业难以独立建立完整的测试能力。建议在行业层面推动测试用例库、协议 fuzz 框架、攻击链模拟平台等基础设施的共建共享，并探索整车企业与安全厂商之间的测试结果互认机制，降低整体合规成本。

七、结论与展望

回顾本年度智能网联汽车安全漏洞态势与典型漏洞分析，可以看到风险形态正在从“分散的单点缺陷”向“云-管-端关键链路的系统性耦合”迁移。年度样本中，中低危问题仍占多数，主要集中在安全基线、配置治理、信息最小暴露与调试面管理等层面；这些问题往往难以单点直接触发安全事故，却持续为攻击者提供情报、入口与复用条件，显著降低后续高危行为的成本。与此同时，高危与严重漏洞虽然占比不高，但更集中指向远程车辆控制、权限提升、诊断绕过与规

模化数据泄露等核心场景，其共同特征是信任边界设置不当：把“客户端自证”“静态标识”或“单次会话”误当作长期可信依据，使认证会话、授权语义、链路安全与工程接口在真实对抗中被串联成完整攻击链。

7.1 年度关键技术发现总结

第一，身份认证与会话治理仍是年度高风险问题的起点。多个高危场景表明，一旦 Token 可被窃取、生命周期过长、退出不失效，或服务端缺乏设备/上下文绑定与风险校验，即使接口表面存在签名与“防重放”设计，攻击者仍可在任意终端复现请求并长期滥用能力，从而把车辆控制指令、位置与账号体系暴露在可批量化的攻击路径之下。

第二，授权模型与业务语义缺陷是“规模化风险”的核心放大器。车辆绑定/解绑、分享授权、对象引用等关键链路一旦缺少所有权校验与最小权限边界，漏洞就会从“单用户影响”快速扩展到跨车辆、跨车队甚至平台级影响；而这种风险往往以“看起来合法的调用”呈现，隐蔽性强、难以通过传统漏洞扫描捕获。

第三，车端工程能力与调试面治理仍是攻击链的高价值补给点。工程模式、USB/调试接口、日志导出与诊断能力若长期保留且缺乏强认证与审计，攻击者在维修、租赁或短时接触场景下即可获得系统情报、凭据或提权入口，并将其与移动端逆向、网络抓包结合，形成从本地到远程的复合攻击路径。

第四，通信与协议侧风险正在呈现“两极化”趋势：一类是配置型与链路型薄弱，其特点是门槛低、易规模化；另一类是协议栈与底层组件的实现缺陷，其特点是触发条件更苛刻但一旦成立可能直接越过业务层防护，形成执行层控制权获取。这两类风险分别对应“安全基线缺失”与“供应链/组件治理不足”两个长期治理主题。

本年度的关键技术结论是：智能网联汽车安全不能以修复单个漏洞为主要手段，而需要以攻击链为单位建立设计约束和验证闭环，尤其要把高敏感指令链路、身份凭据、授权语义、工程接口与云端暴露面作为治理优先级的核心依据。

7.2 下一年度 AI 安全风险预警与重点关注方向

随着大模型、语音助手与智能体逐步接入车载座舱，车辆控制、位置查询、账号服务、导航规划等能力正在由传统图形界面操作向自然语言交互与智能体自动执行演进。该模式显著提升了用户体验，但也引入了“自然语言输入—意图识

别—权限判断—工具调用—车辆执行”的新型信任链路。一旦输入内容、插件权限、上下文授权或执行确认机制存在缺陷，攻击者可能通过语音、文本或间接内容注入，诱导系统调用高敏感接口，形成区别于传统 App 接口越权的新型攻击面。

一是关注语音助手与大模型的提示注入风险。车载语音助手可能接收来自车内乘员、车外环境、蓝牙通话、音频播放、网页内容或第三方应用的输入。如果系统无法有效区分用户真实意图与外部注入内容，攻击者可能通过构造特定语音、文本或多轮对话上下文，诱导模型执行非预期操作。对于解锁车门、开启后备箱、控制车窗、修改导航目的地、查询车辆位置、发起账号操作等敏感功能，应验证系统是否能够抵御直接提示注入、间接提示注入、上下文污染与指令拼接等攻击方式，避免将未经可信确认的自然语言内容直接转化为控制指令。

二是核查语音助手是否暴露高危控车接口。语音交互能力不应默认获得与车主 App、车控后台或车机底层服务等同的权限。对于车门、车窗、后备箱、空调、灯光、鸣笛、车辆启动、数字钥匙、充电控制等功能，应明确区分低敏感操作与高敏感操作，并验证语音助手能够调用的接口范围、调用条件与权限边界。特别需要关注是否存在通过语音绕过图形界面限制、绕过锁屏状态校验、绕过车辆状态判断或绕过车主身份校验的情况，防止语音助手成为调用底层控车能力的非授权入口。

三是严格限制大模型访问车辆控制、账号、位置与隐私数据等高敏感能力。大模型不应直接持有长期有效的账号凭据、车辆控制令牌或高权限服务账号，也不应以通用插件形式无限制访问车辆状态、实时位置、历史轨迹、通讯录、行程记录与账号信息。建议采用最小权限原则，对模型可访问的数据范围、接口集合、车辆对象、会话时长和调用频次进行细粒度约束；对于跨账号、跨车辆、跨租户的数据访问，应在服务端执行独立授权校验，避免将模型输出、客户端参数或静态车辆标识作为可信授权依据。

四是建立 AI Agent 调用车控接口的权限边界与二次确认机制。当智能体具备自动规划、连续调用工具和执行多步骤任务的能力时，单次自然语言指令可能被拆分为多个接口调用，并进一步触发实际车辆状态变化。因此，应对 AI Agent 的工具调用建立分级授权模型：普通查询类操作可以在明确授权范围内执行；涉及车辆解锁、启动车辆、数字钥匙管理、位置共享、账号绑定关系变更等高敏感

操作时，应强制进行车主二次确认、设备侧可信确认或多因素认证。对于批量操作、连续操作、跨地域调用、异常时间段调用与高频调用，应触发风控校验、限流阻断与人工复核，避免智能体在被诱导或被劫持后形成自动化控车链路。

五是强化 AI 相关日志与数据生命周期治理。AI 座舱与智能体系统通常会记录用户语音、文本指令、意图识别结果、车辆状态、位置数据、账号信息、工具调用参数与模型响应内容。这些数据能够反映车主身份、出行规律、家庭关系与车辆使用习惯，具有较高敏感性。应明确车端与云端的日志边界，落实数据最小化、分类分级、脱敏存储、访问控制、加密保护、导出审计与生命周期管理，避免在调试日志、模型调用日志、语音转写记录或问题排查数据中长期保留完整 Token、精确位置、账号标识与原始语音。对于用于模型训练、质量分析或算法优化的数据，应建立独立授权、匿名化处理与用途限制机制，防止车载交互数据被过度收集或二次滥用。

六是将 AI 座舱与智能体控车纳入安全测试和持续监测体系。建议建立面向 AI 车载交互链路的专项测试用例，覆盖提示注入、越权工具调用、敏感操作确认绕过、模型幻觉触发错误控制、上下文污染、插件权限滥用、日志敏感信息泄露与异常批量调用等场景。同时，在云端建立针对 AI 工具调用的可观测能力，记录调用主体、车辆对象、授权上下文、工具类型、风险等级、执行结果与确认过程，并对异常频次、跨设备调用、异常地理位置、敏感工具连续调用等行为进行实时监测与阻断。

7.3 面向产业生态的联合行动倡议

面向下一年度，我们向产业各方提出以下联合行动倡议：

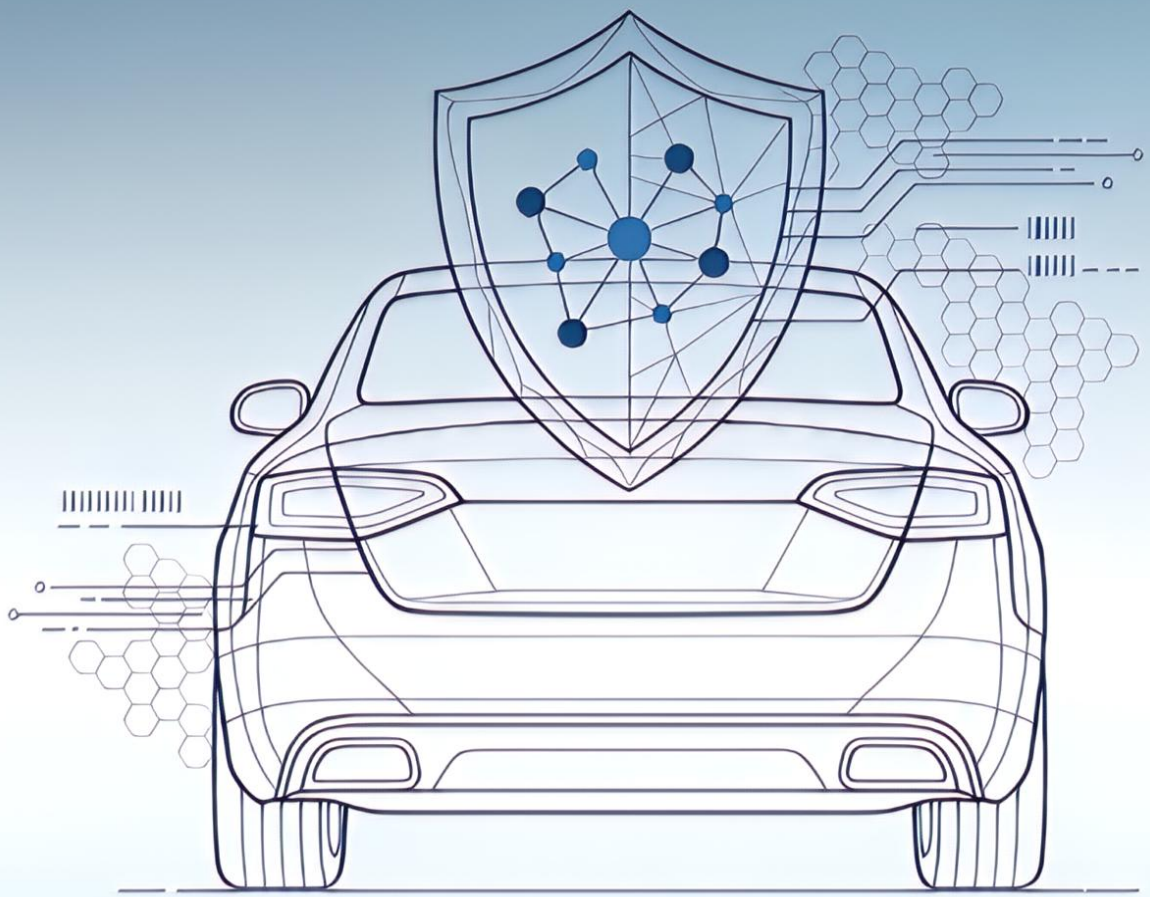
倡议一：共建智能网联汽车漏洞利用链知识图谱。 建议联合行业力量，将此类攻击链知识沉淀为可机读的威胁知识图谱，将孤立漏洞关联为完整攻击路径，赋能自动化防御与风险评估，使“攻击链治理”从方法论走向可落地的技术工具。

倡议二：开展年度跨品牌联合攻防演练。 建议组织更大范围、更多品牌参与的行业级红蓝对抗演练，验证联防联控机制的实效，并推动演练成果向行业安全基线的转化。

倡议三：推动安全设计基线的行业互认与对标。建议通过行业联盟或标准化组织，对遵循“安全默认设计”原则的企业实践进行推广，对高危根因反复出现

的问题进行行业通报与对标整改，形成正向激励与底线约束并重的生态机制，加速行业整体安全水平的收敛。

通过以上方向的持续投入，智能网联汽车安全能力建设将从“发现问题”逐步走向“机制性收敛问题”，从而在保证业务迭代效率的同时，显著降低高危攻击链的形成概率与风险扩散半径。



扫码回复“漏洞报告 2025”获取电子版报告