通过现实世界漏洞利用理解并刻画智能网联汽车漏洞

Yuelin Wang[1], Yuqiao Ning[2], Yanbang Sun[1], Xiaofei Xie[3], Zhihua Xie[1], Yang Chen[2], Zhen Guo[2],Shihao Xue[2], Junjie Wang[1*], Sen Chen[41]中国天津大学智能与计算学院[2]中国中汽数据（天津）有限公司、中国汽车技术研究中心有限公司[3]新加坡新加坡管理大学[4]中国南开大学

arXiv:2601.00627v1 [cs.CR] 2 Jan 2026

摘要

智能网联汽车（ICV）是现代交通运输系统的核心组成部分，其安全至关重要，因为这直接关系到用户安全。尽管已有相关研究，但由于智能网联汽车本身的复杂性，现有研究大多仅关注其特定子组件。因此，人们对智能网联汽车漏洞缺乏系统性认识。此外，当前文献大多依赖人工主观分析，例如问卷调查和访谈；这类分析通常较为宏观且未经验证，导致理论研究发现与现实世界攻击之间存在显著差距。

为解决这一问题，我们开展了首个针对智能网联汽车漏洞的大规模实证研究。我们首先分析了现有的智能网联汽车安全文献，并从漏洞位置和类型两个方面总结了当前主流的分类体系。为评估这些分类体系在现实中的适用性，我们收集了共计649个可利用漏洞，其中592个来自2023年1月至2024年4月期间举办的八场智能网联汽车漏洞发现竞赛 Anonymous Cup，涉及48种不同的车辆。其余57个漏洞由研究人员日常提交。基于该数据集，我们评估了现有分类体系的覆盖范围，并发现了若干缺漏，包括一个新的漏洞位置和13种新的漏洞类型。我们还将这些漏洞归为6种威胁类型（例如隐私数据泄露）和4个风险等级（从低到严重），并分析了竞赛参与者的技能以及涉及的智能网联汽车类型。本研究对智能网联汽车漏洞进行了全面的数据驱动分析，为研究人员、行业从业者和政策制定者提供了可付诸行动的见解。为支持未来研究，我们已公开发布漏洞数据集。

CCS概念

•**安全与隐私 → 系统安全**。

*Junjie Wang 是通讯作者。

授予免费制作本作品全部或部分内容的数字或纸质副本的许可，仅限个人或课堂使用，且不得为盈利或商业利益制作或分发副本；副本首页须附有本声明及完整引文。对于本作品中由作者以外人员拥有版权的组成部分，必须尊重其版权。注明出处后可进行摘要。若需以其他方式复制、重新出版、发布到服务器或分发至列表，须事先获得具体许可和/或支付费用。请向 permissions@acm.org 申请许可。*Conference'17,* 美国华盛顿特区 © 2026年版权归所有者/作者所有。出版权已授权给 ACM。ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM https://doi.org/10.1145/nnnnnnn.nnnnnnn

关键词

智能网联汽车，漏洞实证研究。

ACM 引用格式：

Yuelin Wang，Yuqiao Ning，Yanbang Sun[1], Xiaofei Xie[3], Zhihua Xie[1], Yang Chen[2], Zhen Guo[2], Shihao Xue[2], Junjie Wang[1*]，Sen Chen[4], [1]天津大学智能与计算学院，中国；[2]中汽数据（天津）有限公司、中国汽车技术研究中心有限公司，中国；[3]新加坡管理大学，新加坡；[4]南开大学，中国。2026年。《通过现实世界漏洞利用理解和表征智能网联汽车中的漏洞》。载于. ACM，纽约，纽约州，美国，13页。https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 引言

随着人工智能和 5G 通信技术的快速发展，智能网联汽车（ICV）正日益成为现代交通运输系统的重要组成部分 [21]。与传统车辆不同，智能网联汽车集成了云平台、移动端应用程序、车载信息娱乐系统、高级驾驶辅助系统以及多样化网络，显著提升了智能化水平 [46]。然而，这种复杂的多组件架构也带来了显著的安全风险，可能造成严重后果。例如，2018年，一辆自动驾驶优步车辆因高级驾驶辅助系统未能正确识别一名行人而将其撞死 [1]。2024年9月，Rivera 等人 [2] 发现起亚智能网联汽车存在授权漏洞，攻击者仅凭车牌号码就能远程控制车辆，对用户安全构成严重威胁。

为应对智能网联汽车安全与保障方面的挑战，研究人员对智能网联汽车安全开展了广泛探索，并提出了若干理论攻击分类体系和威胁模型 [17, 24, 33, 34, 39]。例如，Pekaric 等人 [33] 系统总结了现有研究，识别出 48 种攻击向量，并将其归为五种类型（如物理攻击），为制定防御策略奠定了理论基础。此外，Jing 等人 [27] 对汽车安全从业者开展了问卷调查和访谈，并将智能网联汽车的攻击面系统地划分为七大类（如车内组件），从而构建了智能网联汽车的结构化攻击面模型。这些早期分类体系为理解智能网联汽车安全提供了有价值的框架。

然而，现有分类体系存在两个主要局限。首先，其所依据的攻击与分析往往并不完整，且仅关注智能网联汽车的特定方面，例如物理

攻击和基于网络的攻击 [33]，或 Apollo 等自动驾驶系统中的问题 [23, 43]。因此，人们对智能网联汽车整体安全态势缺乏全面认识。其次，大多数分类体系基于专家知识和文献综述构建，形成了对攻击面的高层次概念抽象。这些分类体系在很大程度上仍停留在理论层面，尚未通过现实世界攻击数据进行系统验证。尤其是，现有分类体系中的哪些类别确实反映在现实世界攻击中、又有哪些潜在类别完全缺失，目前仍不明确。弥补这一差距对于评估现有分类体系的实际覆盖范围，以及确定需要完善或扩展的领域至关重要。

为此，我们开展了首个针对智能网联汽车漏洞的大规模实证研究。为弥补现有研究的局限性，我们首先收集并分析了 13 篇具有代表性的智能网联汽车安全论文，手动提取其中报告的攻击方法、漏洞和安全问题。在此基础上，我们构建了统一分类体系，聚焦于两个关键维度：漏洞位置和漏洞类型，涵盖 11 种位置类别和 35 种类型类别。这一统一分类体系全面总结了文献中现有的智能网联汽车漏洞分析。

为评估这些分类体系在现实世界中的适用性，我们投入大量精力收集并分析现实世界漏洞利用。在 16 个月的时间里，我们通过研究人员的每日提交以及八场“Anonymous Cup”智能网联汽车漏洞发现竞赛，收集了 890 份漏洞报告。这些竞赛采用黑盒测试方法，对整车进行测试，涉及来自 19 家制造商的 48 款车型，涵盖了广泛的车辆架构（例如分布式电子控制单元）和安全机制（例如 QNX 管理程序）。

所有提交的报告均经过严格的验证流程，包括真实车辆复现、专家审查和去重，最终确认了 649 个独特且可利用的漏洞。整个数据收集与分析工作历时 98 人月，车辆租赁费用共计 51,000 美元，漏洞奖励金额超过 340,000 美元。这些工作确保了数据集的规模、多样性和可靠性，为验证和扩展现有的智能网联汽车漏洞分类体系奠定了坚实基础。

基于收集到的分类体系和现实世界中可利用的漏洞，我们系统地将 649 个现实世界漏洞映射到这些分类体系中，从而能够评估这些实证漏洞与现有安全分类体系的契合程度。我们的分析表明，收集到的漏洞覆盖了基于位置的分类体系中 91% 的子类别，以及基于攻击类型的分类体系中 89% 的子类别，显示出很强的代表性和广泛的适用性。此外，我们发现了若干在现实世界攻击中频繁出现、但当前分类体系尚未涵盖的关键维度，其中包括一个此前未定义的位置（即 T-Box）和 13 种新的攻击类型（例如文件访问漏洞）。这些发现不仅揭示了现有漏洞分类系统中的盲点，也为其未来更新提供了明确的数据驱动方向，从而帮助安全研究更好地贴合现代智能网联汽车系统的实际威胁态势。

进一步分析结果表明，漏洞主要集中在云平台（37.8%）和IVI模块（32.0%）。在漏洞类型方面，授权漏洞（36.4%）和信息泄露漏洞（17.3%）最为常见，对用户隐私和车辆控制构成严重威胁。我们还观察到漏洞类型与模块之间存在很强的相关性。例如，全部26个Web相关漏洞都出现在云平台中。更重要的是，我们发现不同车辆类型的漏洞分布存在显著差异。例如，与轿车和多用途汽车相比，SUV车型的漏洞数量显著更多，且漏洞尤其集中在IVI模块中。这些发现揭示了不同模块和车辆类型面临的具体安全风险，凸显了制定模块化、差异化安全防护策略的重要性。基于这些发现，我们向智能网联汽车利益相关者（包括制造商、研究人员和监管机构）提出了有针对性的建议。通过落实这些建议，利益相关者可以更好地降低安全风险，加强对不同智能网联汽车模块的防护，并最终为构建更安全的智能交通生态系统作出贡献。

本文作出以下贡献：

- **大规模智能网联汽车漏洞数据集构建**。我们汇集了一个包含649个经验证的智能网联汽车漏洞的数据集，这些漏洞来自2023年1月至2024年4月期间举办的八场竞赛，并逐一与参与者进行核验，以确保准确性。该现实且经过标注的数据集显著大于以往研究所使用的数据集，已公开提供 [3]，为未来的智能网联汽车安全研究奠定了坚实的实证基础。
- **现有分类体系的总结、映射与扩展**。我们总结并统一了从现有文献中提取的漏洞分类体系。我们将收集到的漏洞映射至这些分类体系，以评估其覆盖范围和相关性。在此过程中，我们识别并补充了此前未涉及的漏洞类型和位置，从而扩展了现有的分类系统。
- **系统性的多维漏洞分析**。我们从多个维度对漏洞特征进行了深入分析，揭示了各种分布模式及维度间的相关性，从而为智能网联汽车开发与测试提供了更精准、更具实用性的指导。

2 背景

为加深对智能网联汽车安全的理解，本节介绍智能网联汽车的整体架构及相关工作。

2.1 智能网联汽车架构

如图1所示，智能网联汽车系统由多个关键组件构成，共同支持其智能化和互联功能。其中，应用程序（❶）是用户与车辆之间的重要接口。通过智能网联汽车企业开发的应用程序，车主可以远程控制车辆，从而提升整体用户体验。这些应用程序已成为智能网联汽车软件系统的核心组成部分。云平台（❷）作为中央枢纽，不仅支持远程控制、高级驾驶辅助系统、OTA更新和事故救援等服务，还为企业提供数据管理和生产力提升能力。另一个重要组件是电子控制单元（❸），它负责控制各种车辆子系统的运行。典型的智能网联汽车配备了

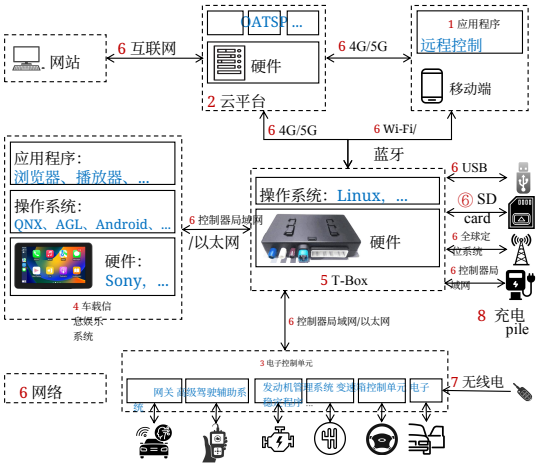


图 1：智能网联汽车的总体架构。

通过数百个电子控制单元确保系统协调运行。车载信息娱乐系统（❹）提供信息和娱乐服务，支持通过触摸屏和智能语音助手进行交互，并运行 QNX 或 Android 等操作系统。

此外，T-Box模块（❺）负责管理智能网联汽车内部与外部组件之间的通信，包括通过4G/5G连接云平台、通过Wi-Fi或蓝牙连接移动设备，以及通过CAN总线与电子控制单元通信。智能网联汽车依靠多种网络技术（❻）来执行数据传输和定位任务，包括用于定位的GPS、用于短距离通信的Wi-Fi和蓝牙，以及用于车内高带宽数据交换的CAN总线和以太网。无线电组件（❼），例如非接触式钥匙和GPS接收器，主要用于车辆解锁和定位。最后，作为电动智能网联汽车的重要基础设施，充电桩（❽）支持通过射频识别卡、应用程序或二维码进行用户身份验证，并在云平台验证后，使用ISO 15118等协议与车辆协商充电参数，以确保充电过程安全高效。

2.2 相关工作

2.2.1 自动驾驶安全与防护。许多研究聚焦于自动驾驶系统（ADSs），这类专用子系统由感知、预测、规划和控制模块组成，旨在借助先进的人工智能模型实现自动驾驶车辆运行。例如，Cheng等人提出了 BehAVExplor [15]，，Li等人 [28] 则推出了 AV-FUZZER——两者都旨在发现自动驾驶系统中可能导致车辆碰撞或响应超时的问题。这些工作主要针对规划模块，强调功能正确性（如模型鲁棒性），而非典型的安全漏洞。Tang等人 [43] 系统性地综述了自动驾驶系统在模块级和系统级的测试方法。虽然其综述涉及传感器和感知模块中的一些攻击场景，但这些场景主要用于说明测试优化目标，而非全面分析安全威胁。因此，由于该论文着重探讨自动驾驶系统的测试方法，许多智能网联汽车安全的一般方面并未涵盖。

此外，Pham等人开展了一项关于自动驾驶车辆攻击与防御策略的实证调查 [34]，涵盖激光雷达/雷达干扰以及针对自动驾驶系统感知模块的对抗性攻击等威胁。Gao等人 [22] 从四个维度分析了攻击面：传感器（如摄像头）、操作系统（如 Apollo）、控制系统（如控制器局域网）和 V2X 通信（如车与车通信、车与基础设施通信），这些都是自动驾驶所必需的。Garcia等人 [23] 开创性地研究了 Apollo [9] 和 Autoware [19], 等开源自动驾驶系统中的一般软件缺陷，而这些问题通常并不属于漏洞。

2.2.2 智能网联汽车安全。 除了自动驾驶系统特有的安全问题外，多项研究还探讨了智能网联汽车更广泛的攻击面和威胁。Pekaric 等人 [33] 进行了文献综述，从现有论文中识别出 48 种攻击类型，并按访问级别——物理访问、近距离和远程访问——进行分类，随后又按目标进一步细分，例如电子控制单元、无线电系统和 Wi-Fi。类似地，Sommer 等人 [39] 提出了一种更简明的分类方法，依据安全威胁进行划分，包括欺骗攻击、篡改、抵赖、信息泄露、拒绝服务攻击（DoS）和权限提升。

Thing 等人 [44] 提出了一种分类体系，涵盖物理访问攻击（如代码修改和注入）以及远程攻击（如信号欺骗和干扰攻击）。Sun 等人 [41] 将网络安全风险分为车载网络攻击、车联网通信攻击及其他威胁，包括全球定位系统欺骗、CAN 总线漏洞、拒绝服务攻击和重放攻击。Limbasiya 等人 [29]综述了多个类别的攻击检测和防御技术，包括冒充攻击、拒绝服务攻击、Sybil 攻击、中继、注入和侧信道攻击。Gupta 等人 [25] 从软件、硬件和网络角度对智能网联汽车攻击进行分类，并指出常见类型包括注入、拒绝服务攻击和侧信道攻击。

Niroumand 等人 [32] 提出了攻击与缓解策略的分类体系，将车辆视为一个控制系统，并重点关注拒绝服务、干扰攻击、中间人攻击和数据注入等攻击。Bouchelaghem 等人[11] 提出了自动驾驶汽车攻击面的分类体系，并综述了近期真实世界攻击实验，涵盖六大类别。Luo 等人 [30]对汽车网络安全测试进行了系统综述，重点关注测试方法和工具。

尽管这些研究为理解智能网联汽车面临的威胁及分类体系构建提供了宝贵见解，但它们主要依赖文献综述、专家分析或行业访谈。因此，这些研究在很大程度上仍停留在概念层面，缺乏通过真实世界漏洞利用进行的实证验证。本文旨在整合这些研究的发现，构建一个全面的分类体系，并利用一组已确认的真实世界可利用漏洞数据集，对各个类别进行验证。

2.2.3 其他领域的缺陷研究。众多实证研究分析了各种软件系统中的软件缺陷，重点关注其症状、根本原因及更广泛的特征[13, 14, 27, 35, 38, 40, 45]。这些研究包括对编译器（如 GCC [40]）中的软件缺陷、深度学习框架中的缺陷 [38], 以及容器运行时问题 [45]的分析。我们的研究目标与此类似：基于大规模现实世界漏洞利用，系统地描述并评估智能网联汽车领域的漏洞。

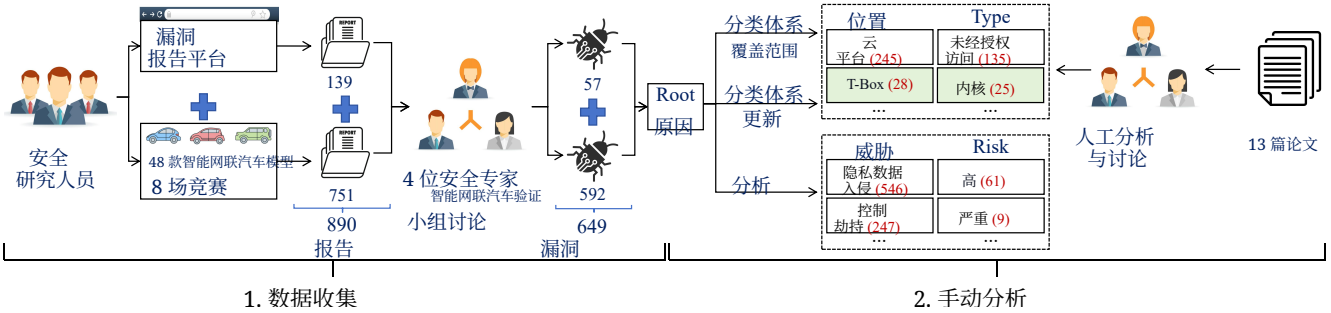


图2：我们的方法论概述。

3 方法论

为了系统地了解智能网联汽车的安全状况并识别其主要威胁，需要对智能网联汽车漏洞进行全面分析。如图 2 所示，这一过程分为两个主要阶段：数据收集和手动分析。首先，我们通过在线报告平台收集了总计 890 份漏洞报告，其中包括研究人员日常提交的 139 份报告，以及来自漏洞发现竞赛的 751 份报告。每份报告都经过严格核验，并在真实车辆上进行测试，最终确认了 649 个可复现的漏洞。其次，我们收集了 13 篇与智能网联汽车安全相关的代表性论文，其中大多数是综述论文，本身总结了广泛的既有智能网联汽车研究。由于这些论文关注智能网联汽车安全的不同方面，我们手动提取并分析了其中关于漏洞位置和类型的分类体系，并将其统一整合为一个分类体系。第三，我们将收集到的漏洞映射到这些既有分类体系中，以评估其覆盖范围并识别缺口，从而将新发现的类别纳入更新后的分类体系。此外，我们还按照威胁类型和风险等级对漏洞进行分类，以便更全面地了解其安全影响。

3.1 数据收集

为确保数据集的全面性和多样性，我们通过在线漏洞报告平台收集智能网联汽车漏洞，其中包括研究人员每日提交的漏洞，以及来自智能网联汽车漏洞发现竞赛的漏洞。

3.1.1 智能网联汽车漏洞报告平台。 我们建立并运营了一个用于漏洞报告和跟踪的在线平台。该平台使安全研究人员能够提交漏洞，并帮助制造商实时监控其产品的安全状况。在本研究期间，该平台每天收到研究人员提交的139份漏洞报告。经过验证，确认其中57个漏洞符合以下标准：可复现、属于智能网联汽车安全范围内、不重复，且通过在真实车辆上测试得到验证。

3.1.2 智能网联汽车漏洞发现竞赛。为全面收集智能网联汽车漏洞，我们于2023年1月至2024年4月在中国组织了8场漏洞发现竞赛，统称为“Anonymous Cup”。

伦理考量。 我们谨慎处理了与竞赛相关的潜在伦理问题。所有活动均严格遵循伦理标准：使用智能网联汽车已获得相应制造商的充分授权；参与者签署了保密协议；所有已确认的漏洞均在公开发布前负责任地向制造商披露，以便进行修复。这些措施确保了最低程度的安全风险，并完全符合法律和伦理准则。

每场比赛持续约15天，涉及6种不同车型，共有48辆智能网联汽车参与。这些智能网联汽车代表了19家制造商，包括Bavarian Motor Work（宝马）、特斯拉和奥迪等品牌。为保护机密，未披露具体品牌和车型。这些智能网联汽车由制造商直接提供，或通过当地租赁公司租用。日均租金为71美元，总费用约为51,000美元。所有智能网联汽车均支持网络连接，其中34辆（70.8%）配备了远程控制应用程序。

竞赛分为两个阶段：测试阶段和演示阶段。在测试阶段，参与者采用黑盒测试方法，不提供详细文档或配置信息。每个团队都获准合法使用一辆测试车辆及其配套的移动端应用程序，以模拟典型的渗透测试环境。一些参与者还运用了社会工程技术（例如收集公开信息）来辅助侦察。在随后的演示阶段，参与者必须在一辆同品牌、同型号但未经授权使用的车辆上重现其攻击，从而模拟针对毫无防备受害者的真实攻击场景。

参与者通过在线平台提交漏洞报告。在八场竞赛中，共收到751份提交。为尽量减少不同车辆之间的数据冗余，去重依据为操作系统版本（通过车载信息娱乐系统接口识别）和底层硬件型号（通过竞赛结束后的固件提取确定）。对于最初无法验证的漏洞，提交者必须提供更多信息，直至漏洞得到确认。

3.1.3 参赛智能网联汽车与参与者概况。由于保密和商业方面的考虑，我们无法公开有关漏洞及具体参赛智能网联汽车的详细信息。不过，为了提高本研究的可复现性

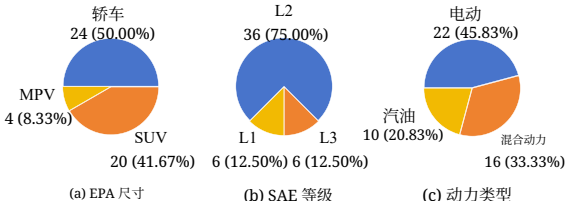


图 3：智能网联汽车类别的分布。

并为测试对象提供更好的背景信息，我们介绍参赛智能网联汽车的概况。具体而言，我们从四个维度对参赛车辆进行分类：首先，根据美国环保署（US EPA [6]）广泛采用的分类标准，这些车辆分为轿车（50.00%）、标准型运动型多用途汽车（41.67%）和多用途汽车（8.33%），如图 3 (a) 所示。其次，根据驾驶自动化 SAE 等级 [8],，这些车辆涵盖 L1 、 L2 和 L3 级，其中 L2 级最为常见，占总数的 75%，如图 3 (b) 所示。第三，按动力类型划分，这些车辆包括电动汽车（45.83%）、汽油汽车（20.83%）和混合动力汽车（33.33%），如图 3 (c) 所示。最后，从制造国来看，这些车辆来自六个国家，其中排名前三的是中国（58.33%）、美国（12.5%）和德国（12.5%）。

大多数参与者来自中国，因为竞赛在当地举办。他们主要来自网络安全公司和学术机构，具备扎实的技术基础和丰富的实践经验。根据注册数据，约95%的参与者曾参加过国家级或企业级安全竞赛，超过85%的参与者从事智能网联汽车安全研究已有三年以上。尽管我们未在竞赛前开展正式的技能调查，但我们对参与者的技术背景与其提交的漏洞进行了相关性分析。这有助于支持人为因素研究中的可复现性。

为便于进一步分析，我们已在数据集 [3] 中公开所有原始数据。其中包括智能网联汽车编号、参与者编号、每个漏洞所涉及的主要技能，以及每辆智能网联汽车的高级特征（例如美国环保署类别、SAE 等级、动力类型）。这些关联有助于开展更深入的分析，例如探究参与者的技能组合与漏洞类型之间的关系，或漏洞与车辆特征（例如美国环保署分类）之间的相关性。更多详细讨论请参见第7节。

3.1.4 现有智能网联汽车漏洞。为更好地了解现有智能网联汽车漏洞，我们收集了13篇近期论文 [11, 22, 23, 25, 29,30, 32–34, 39, 41, 43, 44] ，这些论文聚焦于 ICV攻击和分类体系构建。其中大多数是综述论文，总结了该领域大量相关文献。我们手动提取了每篇论文中报告的攻击和漏洞类型，以形成综合视图。各来源中提取的漏洞类型详细列表可在我们的项目网站 [4]上查看。

3.2 手动分析

根据从每篇论文中提取的漏洞和攻击，我们手动将它们归纳为两个分类体系：漏洞位置和漏洞类型。这项工作相对直接，因为许多攻击在不同论文中的概念相似。总体而言，该分类体系借鉴了既有标准（如 CWE） [7],，同时针对智能网联汽车的具体情境进行了调整。对于使用不同术语描述相似攻击的情况，我们将其归入同一个统一类别。分类体系构建由三位安全专家协作完成。任何分歧都通过讨论解决，直至达成共识。统一分类体系的详细内容见第 4 节和第 5 节。

3.3 现有漏洞映射

我们进一步分析了所收集漏洞的根本原因，并将其映射到现有分类体系中。分析由四位安全专家共同开展，他们在智能网联汽车漏洞审计和竞赛评审方面均拥有五年以上经验。分析采用协作讨论的方式，以确保严谨性和可靠性。分析基于来自48辆智能网联汽车的890份漏洞报告，其中649个被确认为有效漏洞。专家们分别对每个漏洞进行分析，确定其根本原因并拟定描述，随后进行分类。如有意见分歧，团队会进行多轮讨论，直至达成共识，从而确保分类结果的一致性和准确性。

我们的分类遵循多维分类框架：❶**基于位置的分类**：为分析漏洞的分布情况，我们首先将其映射至统一的基于位置的分类体系。❷ **基于类型的分类**：为支持有针对性的缓解策略，我们将每个漏洞映射至统一的基于类型的分类体系。❸ **基于威胁的分类**：为识别潜在的安全后果，我们进一步将漏洞划分为六类威胁类别，包括隐私数据泄露和控制劫持。❹ **基于风险的分类**：为指导修复优先级，我们根据每个漏洞的潜在影响为其分配风险等级（严重、高、中或低）。

对于无法映射至任何现有类别的漏洞，我们提出了新的类别，并将其纳入更新后的分类体系。这一数据驱动、专家主导的多维分类框架系统地概述了现实世界中的智能网联汽车漏洞，并为未来的安全研究和缓解工作提供了实践指导。组织竞赛、审查提交内容并开展漏洞分析共投入了98人月，参与人员包括四名安全专家和两名支持工作人员。

4 位置分类体系

图 4 展示了基于位置的分类体系，其中包含 11 个叶类别。白色类别表示以往研究也涉及的类别，绿色类别则是我们基于现实世界漏洞在本研究中新发现、以往研究未曾纳入的类别。虚线边框的类别不在我们的分析范围内，因为我们只考虑软件中的漏洞。每个数字表示所收集的漏洞中属于该类别的数量。接下来，我们将简要介绍每个类别。

4.1 车外

车外类别包括云平台、应用程序和充电桩等外部但对安全至关重要的系统，共有321个漏洞，占数据集中所有漏洞的49.5%。

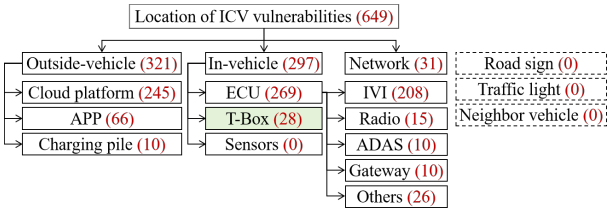


图 4：智能网联汽车漏洞的位置分类体系。

发现 1： 总体而言，我们收集的漏洞覆盖范围广，涵盖了所考虑的11个位置类别中的90.91%（10个）。唯一未覆盖的类别是 Sensors。此外，我们的分析还识别出1个此前分类体系中未包含的新位置类别。我们还将覆盖范围与13篇现有论文进行了比较，发现这些论文各自的覆盖范围为27.27%至63.64%，显著低于我们的数据集所达到的覆盖范围。

4.1.1 云平台。 云平台共有 245 个漏洞，占车外漏洞的绝大多数（76.3%）。作为核心支持系统，云平台负责远程控制、OTA（空中）更新和身份验证等关键功能，涉及多个子系统和通信协议，因此显著扩大了攻击面。研究表明，每辆智能网联汽车平均连接 5.1 个云平台。制造商之间标准不一致，以及集成过程中的安全设计和权限管理薄弱，进一步加剧了漏洞数量。

4.1.2 应用程序。 作为负责远程控制的主要车外组件，应用程序也存在一定的漏洞，占所有车外漏洞的 20.6%。我们的研究发现，智能网联汽车应用程序在数据传输方面往往存在严重缺陷，例如仅通过车辆识别号码（VIN）绑定控制命令而未进行额外加密，因此容易导致隐私泄露并遭受重放攻击。请注意，有关应用程序相关分类体系的更多详细信息可供查阅。由于篇幅有限，详细的分类体系信息请参见我们的数据集 [3]。

4.1.3 充电桩。充电桩虽然占比较小，但仍构成显著风险，占车外漏洞的 3.1%。充电桩系统与云平台和车辆交互，以管理身份验证、计费和充电过程，并依赖 ISO 15118 和 OCPP 等复杂协议 [18]。这些协议的开放性及其与多个系统的连接扩大了攻击面 [31],；身份验证和加密措施不足可能导致信息泄露和权限提升等安全风险。

4.2 车内

车内漏洞共计 297 个，占漏洞总数的 45.8%。这些漏洞分为六个子类别：车载信息娱乐系统、无线电、高级驾驶辅助系统、网关、其他和 T-Box，详情如下。

4.2.1 车载信息娱乐系统。车载信息娱乐系统漏洞占车内漏洞的 70.0%。为支持蓝牙、Wi-Fi 和语音助手等功能，车载信息娱乐系统开放了大量网络端口和调试接口，其中许多并非正常运行所必需，却为攻击者提供了入侵入口。此外，调试模式可能遭到泄露，一些制造商为方便维护而让调试端口保持开放，从而增加了安全风险。此外，为了降低成本，一些制造商仍在使用过时的软件组件和通信协议，进一步扩大了攻击面。

4.2.2 无线电。无线电漏洞占车内漏洞的 5.1%。无线电使用 RFID 或 NFC 等无线技术传输信号。尽管采用了加密，无线通信固有的开放性仍使其容易遭受拦截和重放攻击 [16]。此外，基于近距离、无需接触的无钥匙进入功能扩大了攻击面；该功能会自动检测指定范围内的密钥，因此尤其容易受到中继和重放攻击 [10]。

4.2.3 高级驾驶辅助系统、网关及其他。 此类别包括高级驾驶辅助系统、网关以及蓝牙钥匙信号接收器等较简单的电子控制单元，共发现46个漏洞，占所有车内系统漏洞的15.5%。高级驾驶辅助系统中的漏洞源于其对外部传感器、高精度地图以及来自云平台的实时数据的依赖；开放的数据接口和多源数据融合增加了受到干扰或遭到篡改的风险 [26]。网关电子控制单元的漏洞则与其作为中央通信枢纽的作用有关。其开放的接口（如防火墙和入侵检测接口）扩大了攻击面，而复杂的安全配置可能导致配置错误或加密不足 [37]。蓝牙钥匙信号接收器等较简单的电子控制单元因不同智能网联汽车车型而异，缺乏共同特征，面临多种不同的安全挑战 [36]。

4.2.4 T-Box。 T-Box漏洞占车内漏洞的9.4%。作为核心通信接口，它负责接收和验证远程控制命令。其使用多种通信协议（尤其是MQTT（消息队列遥测传输）），再加上较高的访问权限，扩大了攻击面 [47]。证书管理中的配置错误或信息泄露会进一步加剧安全风险。

发现2： 智能网联汽车漏洞普遍存在，并且深受各个模块功能的影响。车外部分，尤其是云平台，由于连接广泛且依赖数据，占据了相当大比例的漏洞。车内漏洞在车载信息娱乐系统中最为突出，这是由其暴露于外部数据输入以及复杂的软件架构所导致的。尽管网络漏洞相对较少，但由于其在车辆系统通信中发挥着关键作用，仍会带来重大风险。

4.3 网络

网络漏洞共31项，约占总数的4.8%。作为智能网联系统的核心通信骨干，网络组件集成了多种协议（如 CAN、Telnet 和 SSH），以实现功能模块之间的互操作与通信。然而，这些协议缺乏统一的安全设计，导致传输的数据容易遭到拦截和篡改。此外，车内网络（如

CAN总线）通常默认信任所有已连接设备，使攻击者能够通过物理接口（如 OBD-II）轻松访问系统并发起恶意操作，从而暴露出访问控制和数据完整性方面的严重弱点。

5 类型分类体系

为促进针对性检测技术的开发，以应对智能网联汽车面临的各种安全挑战，我们根据漏洞的类型对其进行描述。如图 5 所示，我们在漏洞类型分类体系中共确定了 35 个类别。与基于位置的分类体系类似，其中 22 个类别（以白色显示）已被现有研究涵盖。此外，我们还发现了 13 个此前未曾报告的新类别（以绿色显示）。其中三个类别被标记为范围之外，因为它们与自动驾驶汽车组件有关，或涉及通常需要用户交互的恶意软件类型。下文将介绍这些类型。

❶ **授权漏洞**。表 1 显示，授权漏洞是最常见的类型，共有 236 起，占所有漏洞的 36.4%。这些漏洞通常由配置错误或设计缺陷导致，并可能引发隐私泄露等高风险问题。具体包括未经授权的访问（135 起）、弱密码（75 起）、权限提升（18 起）和身份欺骗（8 起）。这些漏洞主要存在于外部模块（例如云平台）和车载模块（例如车载信息娱乐系统）中，表明这些组件因授权管理不完善而面临显著的安全风险。

❷ **信息泄露漏洞**。 共有 112 个信息泄露漏洞，占总数的 17.3%。这些漏洞大多由实现错误引起，容易导致车辆识别码和密钥等敏感信息泄露。由于云平台和应用程序等外部模块经常处理大量敏感数据，因此这些模块中尤其常见信息泄露漏洞。

❸ **注入漏洞**。 注入漏洞共 79 个，占所有案例的 12.2%，主要包括 SQL 注入（45 个案例）和命令注入（34 个案例）。SQL 注入通常是由输入验证不足导致的，使恶意代码得以执行并造成隐私数据泄露。我们将其归类为一般注入漏洞，而不局限于 Web 场景，因为它也出现在车载信息娱乐系统和应用程序等非 Web 环境中。命令注入是由于对外部输入验证不足所致，使攻击者能够执行未经授权的命令。如表 1 所示，注入漏洞主要出现在云平台和车载信息娱乐系统中；这些系统经常处理用户输入和数据库操作，因此更容易遭受攻击。

❹ **操作系统漏洞**。操作系统漏洞由系统级安全缺陷引起，共有55起，占所有漏洞的8.5%。它们主要分为五种类型：内核漏洞（25起）、任意软件安装（23起）、USB 漏洞（3起）、调试接口暴露（2起）和升级伪造（2起）。其中，内核漏洞和 USB 漏洞是我们类型分类体系中特有的。作为最常见的操作系统漏洞类型，内核问题可能导致隐私泄露或控制劫持，风险等级最高可达中级。这些漏洞主要存在于车内模块中，尤其是车载信息娱乐系统，它们对内核漏洞和恶意软件安装尤为敏感。

❺ **拒绝服务漏洞**。 共有 47 个拒绝服务漏洞，占漏洞总数的 7.2%（见表 1）。这些漏洞主要出现在车载信息娱乐组件中，占所有拒绝服务漏洞的 55.3%。其根本原因包括组件配置错误、内核缺陷和逻辑设计缺陷，例如协议栈漏洞或资源耗尽攻击，这些问题可能导致受影响组件发生系统损坏。

❻ **文件操作漏洞**。 文件操作漏洞是我们分类中的一个新高级类别，共有 38 个案例，占所有漏洞的 5.9%。该类别包含若干子类型，例如文件访问（14 个案例）、文件下载（8 个）、文件篡改（7 个）、文件上传（5 个）、文件遍历（3 个）和文件删除（1 个）。如表 1 所示，这些漏洞主要出现在云平台和车载信息娱乐系统中。云平台处理大量文件数据，因此容易受到访问控制不足的影响；车载信息娱乐系统经常执行本地文件操作，因此面临篡改和未授权下载等风险。

其中，文件访问漏洞通常由云平台中的分区管理不当或车载信息娱乐系统中的权限配置错误导致，使攻击者能够读取敏感文件并造成隐私泄露 [12]。文件下载漏洞允许攻击者通过修改 URL 或利用未经验证的下载路径获取敏感文件；文件遍历漏洞则通过构造恶意路径绕过目录限制，访问非预期文件。尽管这三类漏洞都涉及未授权访问，但它们在技术机制、攻击目标和攻击链阶段方面各不相同，因此代表了三种不同类型的漏洞。

❼ **拦截漏洞**。表 1 显示，共有 36 个拦截漏洞，占所有漏洞的 5.5%。它包括六个子类型：中继（11 个案例）、重放（8 个）、中间人攻击（8 个）、GPS 欺骗（5 个）、流量劫持（3 个）和 DNS 劫持（1 个）。拦截漏洞主要集中在车载信息娱乐系统、电子控制单元和无线电模块中。车载信息娱乐系统和电子控制单元涉及车辆内部通信，容易受到拦截攻击；而 T-Box 和无线电等网络模块由于具有无线通信特性，也容易受到信号劫持。在这些漏洞中，中继攻击是我们分类中特有的一种漏洞类型。这些漏洞通常源于系统未能对传输的信息进行加密或身份验证，使攻击者能够利用中继通信执行未授权操作，甚至可能未经授权解锁车辆 [20], ，风险等级达到高。

❽ **特定于 Web 的漏洞**。 如表 1 所示，共有 26 个特定于 Web 的漏洞，占总数的 4.0%。这些漏洞分为四种类型：跨站脚本攻击（17 起）、反序列化（7 起）、网络钓鱼（1 起）和 XML 外部实体注入（1 起）。特定于 Web 的漏洞仅发现于云平台中，表明此类问题主要局限于云环境。跨站脚本攻击漏洞源于制造商的云平台未能正确处理用户输入（例如缺少输入验证），从而允许

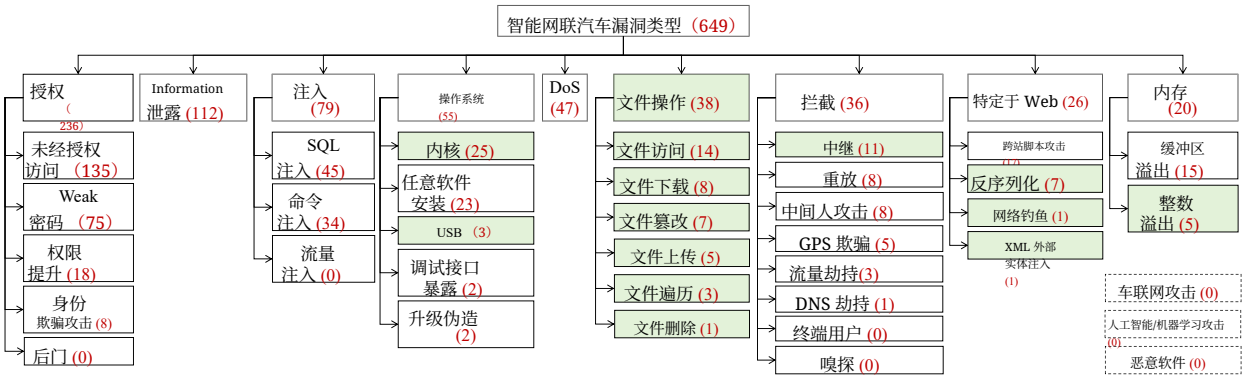


图 5：智能网联汽车的类型分类体系。

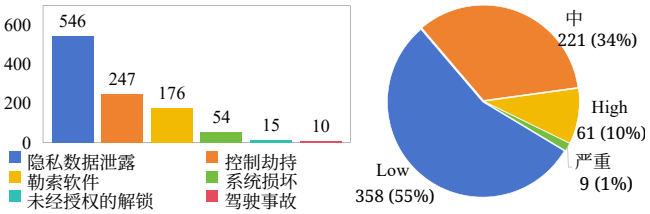
表 1：各位置的漏洞类型频次。

Type	子类型	云平台	IVI	APP	ECU	网络	T-Box	无线电	充电桩	Sum	
		#N T R	#N T R	#N T R	#N T R	#N T R	#N T		R		
❶ 授权	未经授权的访问	57 16 C	45 12 H	19 12 C	1 ① L	6 ①② H	7 ② C	- - -	- - -	135	236
	弱密码	31 16 C	14 12 H	2 ①② L	7 12 M	15 12升	6 ①② M	- - -	- - -	75	
	权限提升	- - -	16 12 H	- - -	1 2 M	- - -	1 ② M	- - -	- - -	18	
	身份欺骗	7 ①⑥ C	- - -	1 ①② L	- - -	- - -	- - -	- - -	- - -	8	
❷ Information泄露	-	53 16 H	13 ① H	27 ① H	7 ① L	1 ① L	3 ① M	- - -	8 ① L	112	112
❸ 注入	SQL 注入	31 ① H	11 ① M	1 ① L	- - -	- - -	- - -	- - -	2 ① M	45	79
	命令注入	16 16 H	5 12 H	6 12 M	3 ① M	- - -	4 ② H	- - -	- - -	34	
❹ OS	内核	- - -	25 12 M	- - -	- - -	- - -	- - -	- - -	- - -	25	55
	任意软件安装	1 ①⑥ M	17 12 H	- - -	5 ⑤ M	- - -	- - -	- - -	- - -	23	
	USB	- - -	3 ①② L	- - -	- - -	- - -	- - -	- - -	- - -	3	
	调试接口暴露	- - -	1 ①② M	- - -	- - -	1 ② M	- - -	- - -	- - -	2	
	升级伪造	- - -	- - -	- - -	1 ② H	- - -	1 ② M	- - -	- - -	2	
❺ 拒绝服务	-	1 ③ L	26 ③ L	7 ③ L	5 ③ H	5 ③ M	1 ③ M	2 3 M	- - -	47	47
❻ 文件操作	文件访问	7 ① H	7 ① L	- - -	- - -	- - -	- - -	- - -	- - -	14	38
	文件下载	7 ① M	- - -	- - -	1 ① L	- - -	- - -	- - -	- - -	8	
	文件篡改	- - -	7 ①② M	- - -	- - -	- - -	- - -	- - -	- - -	7	
	文件上传	4 ①⑥ M	- - -	- - -	- - -	1 ② M	- - -	- - -	- - -	5	
	文件遍历	3 ① L	- - -	- - -	- - -	- - -	- - -	- - -	- - -	3	
	文件删除	1 ③ L	- - -	- - -	- - -	- - -	- - -	- - -	- - -	1	
❼ 拦截	中继	- - -	- - -	- - -	2 ④ M	1 ② M	- - -	8 ④ H	- - -	11	36
	重放	- - -	- - -	2 ①② H	- - -	1 ③ L	- - -	5 ④ C	- - -	8	
	中间人攻击	- - -	7 ①② M	1 ①② M	- - -	- - -	- - -	- - -	- - -	8	
	全球定位系统欺骗	- - -	- - -	- - -	5 ③⑤ L	- - -	- - -	- - -	- - -	5	
	流量劫持	- - -	3 ①② M	- - -	- - -	- - -	- - -	- - -	- - -	3	
	DNS 劫持	- - -	1 ①② M	- - -	- - -	- - -	- - -	- - -	- - -	1	
❽ 特定于 Web	XSS	17 ① L	- - -	- - -	- - -	- - -	- - -	- - -	- - -	17	26
	反序列化	7 ①⑥ M	- - -	- - -	- - -	- - -	- - -	- - -	- - -	7	
	网络钓鱼	1 ① L	- - -	- - -	- - -	- - -	- - -	- - -	- - -	1	
	XXE	1 ① L	- - -	- - -	- - -	- - -	- - -	- - -	- - -	1	
❾ 内存	缓冲区溢出	- - -	4 ①② M	- - -	6 ② H	- - -	5 ② L	- - -	- - -	15	20
	整数溢出	- - -	3 ①② H	- - -	2 ①② H	- - -	- - -	- - -	- - -	5	
Sum		245	208	66	46	31	28	15	10	649	

威胁（T）：1 隐私数据泄露；2 控制劫持；3 系统损坏；4 未经授权的解锁；5 驾驶事故；6 勒索软件；风险（R）：低（L）；中（M）；高（H）；严重（C）；注："风险"列表示此位置此类型漏洞可能达到的最高风险等级。

攻击者注入恶意脚本，这些脚本会通过其他用户的浏览器执行，从而导致隐私数据泄露。其余漏洞类型，例如反序列化、网络钓鱼和 XML 外部实体注入，是我们分类中特有的。

❾ **内存漏洞** 共识别出 20 个内存漏洞，可进一步分为两类：缓冲区溢出（15 起）和整数溢出（5 起）。缓冲区溢出漏洞主要是由于开发人员未能妥善处理用户输入或数据，使攻击者能够触发数据溢出并破坏内存。整数溢出是我们分类体系中特有的一种漏洞类型，源于未充分考虑数据类型边界，这可能导致内存损坏，进而造成隐私泄露，风险等级可达高。内存漏洞主要出现在车载信息娱乐系统和电子控制单元模块中，因为这些模块涉及复杂的数据处理，且容易因输入验证不足或资源管理不当而出现内存错误。



(a) 威胁分布。 (b) 风险分布。

图 6：威胁与风险分布。

发现 3： 已识别的漏洞覆盖范围很广，涵盖了所考察类型类别的 88.57%（35 类中的 31 类）。未覆盖的类别包括后门、流量注入、终端用户和嗅探。与先前的研究相比，我们的分析发现了 13 种新的漏洞类型。我们还将分类体系的覆盖范围与现有的 13 篇论文进行了比较，发现它们各自的类型覆盖率介于 11.43% 至 40.00% 之间，进一步凸显了我们数据集的全面性。

发现 4： 新发现的漏洞位置和类型凸显了我们收集到的现实世界中的智能网联汽车漏洞的多样性和复杂性，也强调了数据驱动分析作为现有基于概念和文献的方法的补充的重要性。这种实证分析有助于完善和扩展当前的漏洞分类体系。

发现 5： 授权漏洞（36.4%）和信息泄露漏洞（17.3%）最为常见，反映出智能网联系统在访问控制和数据保护方面存在系统性缺陷。此外，不同模块面临着不同类型的漏洞（全部 26 个 Web 特定漏洞均出现在云平台中），这凸显了实施有针对性的漏洞检测策略的紧迫性。

6 威胁与风险分类体系

为识别具体的安全后果并支持威胁建模，我们按威胁对漏洞进行分类，得出 6 种威胁类别，如表 1 所示。其中，隐私数据泄露是指对敏感个人或车辆数据的未授权访问，从而损害机密性；控制劫持是指攻击者未经授权控制车辆的严重功能（如转向或制动），危及驾驶安全；系统损坏是指故障或中断导致车辆功能暂时或永久丧失，影响运行安全；未经授权的解锁使攻击者能够在未经许可的情况下访问或解锁车辆，增加盗窃风险；驾驶事故是指系统操纵导致碰撞或不安全驾驶状况，给车内人员及其他人带来风险；勒索软件则是指恶意软件锁定车辆系统或数据，并要求支付赎金才能恢复，导致车辆功能受损。这些不同类别凸显了智能网联汽车面临的严重安全威胁，因此亟需制定有针对性的策略。

某些漏洞可能导致多种后果。例如，某些控制劫持漏洞也可能造成隐私泄露。如图 6-(a) 所示，84.13% 的漏洞涉及隐私数据泄露，38.06% 可能导致控制劫持，另有 27.11%、8.32%、2.31% 和 1.54% 分别与勒索软件、系统损坏、未经授权的解锁和驾驶事故有关。这些多方面的风险凸显了智能网联汽车面临的严重安全挑战，也表明亟需制定有针对性的防御策略。

为了根据影响严重性确定修复优先级，我们按照风险对漏洞进行分类，划分为 4 个风险等级：低（L）、中（M）、高（H）和严重（C）。具体而言，我们从两个维度评估漏洞的严重性：实施攻击的难易程度和攻击影响。采用 1 至 4 的相对评分系统，并根据漏洞风险等级判定表确定风险等级。每个漏洞的评分由专家和提交者协作完成，分为三个步骤：提交者初步评分、专家审查和最终共识，以确保公平性和准确性。例如，如果实施攻击的难易程度和攻击影响的评分均为 4，则该漏洞被归类为严重。如图 6-(b) 所示，55.16%、34.05% 和 9.34% 的漏洞分别被评为低、中和高风险。其余 9 个漏洞被评为严重风险，分布于云平台（4 个）、无线电（3 个）、车载信息娱乐系统（IVI，1 个）和 T-Box（1 个）。这些漏洞之所以被归类为严重，主要是因为其影响范围涵盖某个特定品牌或车型的所有车型，或影响超过 300,000 辆车辆。

7 参与者技能与智能网联汽车类型

为了进一步支持潜在的复现工作（这主要取决于发现漏洞的参与者以及发现漏洞的智能网联汽车类型），我们进一步分析了参与者概况和车辆特征。

7.1 参与者技能

如第3.1.3节所述，尽管我们没有明确收集参与者的技能信息，但我们通过分析参与者、他们发现的漏洞以及发现这些漏洞所需技术技能之间的关系，提供了参与者的专业能力信息。表2展示了主要漏洞位置/类型与所需技能之间的整体对应关系。

总体而言，我们发现所识别的漏洞涉及10类技术技能。其中，最常用的是逆向工程、代码审计和渗透测试，分别出现260次、260次和249次。

对于车外组件，云平台漏洞所需的主要技能是渗透测试（243次），这反映出深入分析通信协议和业务逻辑的必要性。应用程序漏洞通常需要结合使用逆向工程（63次）、代码审计（63次）和脱壳（63次），有时也会用到流量分析（59次）。这表明，要发现软件逻辑缺陷和隐私问题，需要结合静态分析和动态分析技术。

对于车内组件，车载信息娱乐系统漏洞需要大量运用逆向工程（146）和代码审计（146），以及固件提取（135）和漏洞复现（39）。

表2：技能集的映射结果。

位置与类型		①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩
位置	云平台	-	-	243	-	-	32	-	2	-	-
	IVI	146	146	-	135	1	13	11	9	39	5
	APP	63	63	-	-	59	-	63	-	-	-
	ECU	19	19	-	19	5	12	-	13	6	3
	网络	7	7	-	7	1	15	-	15	-	7
	T-Box	21	21	-	21	-	6	-	7	-	-
	无线电	-	-	-	-	14	1	-	1	-	-
	充电桩	4	4	6	-	-	-	4	-	-	-
Type	授权	90	90	94	68	23	72	22	37	1	4
	信息泄露	49	49	58	21	28	1	28	3	-	1
	注入	32	32	47	13	7	-	19	-	-	-
	OS	23	23	1	22	-	3	1	4	27	-
	DoS	27	27	1	20	1	1	7	1	9	8
	文件操作	13	13	22	13	-	-	-	-	2	1
	拦截	13	13	-	12	21	-	1	-	1	1
	特定于 Web	-	-	26	-	-	-	-	-	-	-
	内存	13	13	-	13	-	2	-	2	5	-
Sum		260	260	249	182	80	79	78	47	45	15

1 逆向工程；2 代码审计；3 渗透测试；4 固件提取；5 流量分析；6 暴力破解；7 脱壳；8 端口扫描；9 漏洞复现；10 模糊测试；

表3：ICV 类别分类体系的映射结果。

位置与类型		EPA 尺寸			SAE 等级			动力类型		
		运动型	多用途汽车	轿车	多用途汽车	L1	L2	L3 电动	混合动力	汽油
位置	云平台	63	38	4	6	95	4	44	37	24
	IVI	111	82	8	10	183	8	74	93	34
	APP	17	41	-	-	46	12	49	1	8
	ECU	27	13	-	8	28	4	26	6	8
	网络	16	15	-	2	25	4	22	6	3
	T-Box	17	8	-	-	25	-	9	6	10
	无线电	2	13	-	-	15	-	8	5	2
	充电桩	-	-	-	-	-	-	-	-	-
Type	授权	98	75	4	8	161	8	95	58	24
	信息泄露	37	35	3	9	57	9	45	9	21
	注入	22	20	1	2	39	2	13	26	4
	OS	40	13	1	2	50	2	19	26	9
	DoS	17	26	-	2	35	6	25	9	9
	文件操作	16	3	3	2	19	1	3	11	8
	拦截	12	24	-	1	32	3	21	9	6
	特定于 Web	7	4	-	-	10	1	2	6	3
	内存	4	10	-	-	14	-	9	-	5
Sum		253	210	12	26	417	32	232	154	89
汽车数量		20	24	4	6	36	6	22	16	10
#漏洞/车辆		12.7	8.8	3.0	4.3	11.6	5.3	10.5	9.6	8.9

这些技能表明，需要对服务和接口进行静态检查和动态测试。电子控制单元漏洞发现通常涉及逆向工程、代码审计和固件提取（各19次），并辅以暴力破解（12次）、端口扫描（13次）、漏洞复现和流量分析。这些要求意味着需要直接访问硬件，并具备分析嵌入式固件的专业知识。

对于网络组件，分析主要依赖暴力破解（15）、端口扫描（15）和代码审计（7）。研究人员通常使用 CANoe 等工具检查控制器局域网、LIN 和 FlexRay 等通信协议，并尝试伪造控制消息或发送畸形数据包，以触发系统故障。

参与者会根据所发现漏洞的类型采用多种不同的技术方法。授权漏洞是分析频率最高、涉及技能范围最广的漏洞类型。最常用的技术包括渗透测试（94）、逆向工程（90）和代码审计（90）。这不足为奇，因为此类漏洞通常需要全面分析身份验证机制、访问控制模型和通信协议。

信息泄露和注入攻击也很常见，主要依赖逆向工程和代码审计等静态分析技术，且通常结合渗透测试。这些发现表明，此类漏洞通常源于通信逻辑或输入验证方面的缺陷，因此需要深入了解应用层业务流程。

拒绝服务攻击涉及更多样化的技能组合。除了传统方法之外，这类攻击通常还需要复现漏洞（9）和进行模糊测试（8），凸显了测试驱动技术在验证系统稳定性和鲁棒性方面的价值。对于特定于 Web 的漏洞，唯一采用的技术是渗透测试（出现 26 次），这表明关注重点在于与 Web 界面和业务逻辑进行动态交互，而非固件或代码层面的弱点。

发现 6： 智能网联汽车的漏洞发现涵盖软件层和硬件层，要求研究人员具备端到端分析能力和跨学科专业知识。总体而言，不同的漏洞位置往往需要不同的技能组合，这凸显了汽车安全培训应全面且模块化的必要性。

发现 7： 不同类型的漏洞需要不同的技能组合。总体而言，渗透测试、逆向工程和代码审计是几乎适用于所有漏洞类型的核心能力，展现出很强的通用性。相比之下，模糊测试、流量分析和脱壳等技术更依赖具体情境，这表明需要根据漏洞性质和攻击面调整技能组合。

7.2 智能网联汽车特征

如第3.1.3节所述，参赛智能网联汽车按照四个维度进行了分类：国家/地区、EPA 尺寸、SAE 自动化等级和动力类型。本节分析这些类别与漏洞位置及漏洞类型之间的相关性，旨在揭示分布规律，并识别不同类别车辆中常见的安全弱点。如表3所示，我们主要探讨了漏洞与 EPA 尺寸、SAE 等级和动力类型之间的相关性。受篇幅限制，按国家/地区分析漏洞的内容请访问我们的网站 [5]。

EPA尺寸映射。 不同EPA尺寸分类的车辆类型之间，漏洞的平均数量存在显著差异。SUV车型的平均漏洞数量最高（每辆车12.7个），远高于轿车（每辆车8.8个）和多用途汽车（每辆车3.0个）。作为竞争激烈的主流市场细分，多用途汽车通常集成更先进的联网信息娱乐系统和驾驶辅助功能，因此具有更大的攻击面和更高的潜在风险 [42]。从漏洞类型来看，在所有EPA尺寸类别中，授权问题都是最突出的安全弱点。在SUV、轿车和多用途汽车中，授权问题的数量均位居首位。这表明访问

控制和权限管理是普遍存在且具有系统性的安全缺陷，与车辆尺寸分类无关。

SAE 等级映射。 从 SAE 等级的角度来看，L2级车辆的平均漏洞数量（11.6）明显高于 L1（4.3）和 L3（5.3）级车辆。与 L3 系统相比，L2 系统仍然高度依赖接口（例如语音控制），这使车载信息娱乐系统功能更加复杂、接口更加丰富，从而扩大了攻击面。这表明，广泛采用的 L2 级系统由于功能复杂且与车辆深度集成，目前正处于漏洞风险的高峰阶段。

动力类型映射。 从动力类型来看，漏洞平均数量与车辆电气化和智能化程度之间存在明显的正相关关系。电动汽车的平均漏洞数量最高（10.5），其次是混合动力汽车（9.6），而传统汽油汽车最低（8.9）。这表明，随着车辆集成更多电子控制单元、联网服务和远程控制功能，其整体安全风险也随之增加。

发现 8：车辆中的漏洞数量与其智能化程度和功能复杂性相关，这一点在 SUV、L2 级车辆和电动汽车中尤为明显。

8 讨论

本节讨论两个方面：对利益相关方的启示以及有效性威胁。

8.1 对智能网联汽车利益相关方的启示

我们的实证分析表明，智能网联汽车行业面临的主要挑战并非无法抵御高级攻击，而是系统性地忽视基本安全最佳实践。大量漏洞源于基本疏忽，例如 75 起弱密码或明文密码问题、112 起信息泄露事件和 36 起拦截攻击（合计占所有漏洞的 34.36%），以及未受保护的调试接口和不必要的开放端口（如 SSH、Telnet）。更令人担忧的是，一些早在 2017 年就已修复的已知 CVE漏洞仍未得到处理，因集成过时组件以节省成本而暴露出严重的供应链风险。因此，提升智能网联汽车安全，关键在于严格落实安全软件开发生命周期原则，尤其要做好基本安全卫生和供应链风险管理。提升智能网联汽车的安全性需要所有利益相关方协同努力。为此，制造商应加强基本安全防护和第三方组件管理，同时通过加密确保安全数据传输。研究人员应建立针对智能网联汽车的漏洞数据库，并开发高效的自动化检测工具。监管机构应强制推行统一标准，以统一行业基线安全要求并增强整体系统韧性。

8.2 有效性威胁

尽管我们的研究对现实世界中的智能网联汽车漏洞进行了大规模实证分析，但若干因素可能会影响研究结果的可复现性、可重复性和可推广性。

车辆机密性。 由于保密协议和伦理方面的考量，我们无法披露参与研究的车辆品牌、车型或固件版本的详细信息。这限制了他人精确复现或重复我们的研究结果。此外，我们的发现可能无法完全推广到研究范围之外的车辆。为缓解这一问题，我们选取了来自不同架构和制造商的 48 款市售智能网联汽车，这项工作耗费了大量成本和资源。我们还提供了这些车辆的高级概况，包括 SAE 自动化等级、动力类型和 EPA 车辆尺寸分类，以增进对研究背景的了解。

参与者专业能力。参与者技能组合的差异也可能影响所发现的漏洞类型。不同团队的领域专业能力不同，可能会得出不同结果，使其他人难以组建具备同等能力的团队。为缓解这一问题，我们根据提交的漏洞报告提供了参与者技能信息，并分析了这些技能与不同漏洞类型和位置之间的关联。

CTF 竞赛限制。CTF 式竞赛固有的时间限制和激励机制不同于长期红队演练或现实世界攻击场景中的相应因素。因此，本研究的发现最能代表受控且有时间限制的环境。对于持续性威胁模型或生产系统，其适用性应谨慎解读。为解决这一问题，我们详细分析了漏洞发现过程，提供了分类体系覆盖率统计，并发布了我们的框架，以便未来的 CTF 结果能够不断完善和扩展我们的分类体系。

分类体系构建偏差。我们的统一分类体系基于 13 篇经过仔细筛选的综述论文构建。尽管我们力求纳入最新、全面且高度相关的研究，但筛选过程可能引入偏差，并影响分类体系的初始覆盖范围。尽管如此，所选论文涵盖了广泛的文献，为整合工作提供了坚实基础。

标注主观性。为支持可复现性，我们发布了一个包含 649 个经验证的漏洞的数据集，以及一个多维分类方案。然而，出于伦理和法律限制，我们无法发布概念验证代码等技术材料。此外，标注过程涉及专家判断，这可能引入主观性，并导致数据不完整。为降低这一风险，所有分类和验证任务均由四位在智能网联汽车安全领域经验丰富的专家完成，并经过多轮讨论达成共识。

9 结论

本研究对智能网联汽车中的漏洞进行了系统分析。通过全面测试，我们构建了一个包含649个已验证漏洞的数据集，涵盖48种不同的智能网联汽车车型。基于已有文献，我们从位置和类型两个关键维度提取并统一了漏洞分类体系。随后，我们将收集到的漏洞映射至这些类别，以评估现有分类体系对现实世界威胁的反映程度，并通过实证数据识别尚未涵盖的新兴类别。此外，我们发现漏洞特征与车辆类型之间存在显著相关性，进一步凸显了实施模块化、差异化防护策略的重要性。

参考文献

[1] 2018。自动驾驶优步汽车在机器人出没的亚利桑那州撞死行人。https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html。[2] 2024。黑入起亚：仅凭车牌即可远程控制汽车。https: // samcurry.net/hacking-kia。[3] 2024智能网联汽车_漏洞_数据集。https://github.com/Anonymous-People/ICV_ Vulnerabilities/blob/main/ICV_study.csv。[4] 2024智能网联汽车_漏洞_详细类型。https://github.com/Anonymous- People/ICV_Vulnerabilities/blob/main/Summary_of_existing_classification/ Type_summary.csv。[5] 2024智能网联汽车_漏洞_国家分析。https://github.com/Anonymous- People/ICV_Vulnerabilities/blob/main/Car_class/Nation_and_应用程序_分析. pdf。[6] 2025汽车分类。https://en.wikipedia.org/wiki/Car_classification。[7] 2025。CWE——通用缺陷枚举。https://cwe.mitre.org/ [8] 2025。为清晰易懂并面向国际受众而修订的SAE驾驶自动化等级。https://www.sae.org/blog/sae-j3016-update。[9] ApolloAuto。2025年。Apollo——一个开放的自动驾驶平台。https://github. com/ApolloAuto/apollo。[10] James Ashworth、Jason Staggs和Sujeet Shenoi。2023年。利用无钥匙进入系统对车辆和驾驶员进行无线射频识别与跟踪。《国际关键基础设施保护期刊》40（2023），100587。doi: 10 1016 2022 100587 。/j.ijcip. 。[11] Siham Bouchelaghem、Abdelmadjid Bouabdallah和Mawloud Omar。2020年。自动驾驶汽车安全：真实攻击实验的文献综述。载于《互联网与系统的风险和安全：第15届国际会议，CRiSIS 2020，法国巴黎，2020年11月4日至6日，修订版精选论文》（法国巴黎）。施普林格出版社，柏林、海德堡，255 272 10 1007 978 3 030 68887 5_15 – 。2019 [12] doi: 。/ - - - - Miao Cai、Hao Huang和Jian Huang。 。理解文件系统中的安全漏洞。载于第10届ACM SIGOPS亚太系统研讨会论文集（中国杭州）（APSys '19）。计算机协会，纽约，美国纽约州，8–15。doi:10.1145/3343737.3343753[13] Sen Chen、Lingling Fan、Guozhu Meng、Ting Su、Minhui Xue、Yinxing Xue、Yang Liu和Lihua Xu。2020年。全球安卓银行应用安全风险的实证评估。载于2020年IEEE/ACM第42届软件工程国际会议（ICSE）。1310–1322。[14] Zhenpeng Chen、Huihan Yao、Yiling Lou、Yanbin Cao、Yuanqiang Liu、Haoyu Wang和Xuanzhe Liu。2021年。基于深度学习的移动应用部署故障实证研究。载于2021年IEEE/ACM第43届软件工程国际会议（ICSE）。674–685。doi:10.1109/ICSE43902.2021.00068[15] Mingfei Cheng、Yuan Zhou和Xiaofei Xie。2023年。BehAVExplor：面向自动驾驶系统的行为多样性引导测试。载于第32届ACM SIGSOFT国际软件测试与分析研讨会论文集（美国华盛顿州西雅图）（ISSTA 2023）。计算机协会，美国纽约州纽约，488–500。doi:10.1145/3597926.3598072[16] Levente Csikor、Hoon Wei Lim、Jun Wen Wong、Soundarya Ramesh、Rohini Poolat Parameswarath和Mun Choon Chan。2024年。RollBack：针对汽车远程无钥匙进入系统的一种新型与时间无关的重放攻击。ACM《网络物理系统汇刊》8卷1期，第5篇文章（2024年1月），25页。doi:10.1145/3627827[17] Marco De Vincenzi、John Moore、Bradley Smith、Sanjay E Sarma和Ilaria Matteucci。2024年。网联汽车生态系统中的安全风险与设计：车内和边缘平台。《IEEE车辆技术开放期刊》（2024年）。[18] Sanchari Deb、Mikko Pihlatie和Mohammed Al-Saadi。2022年。智能充电：综合综述。IEEE Access 10（2022），134690–134703。[19] Autoware基金会。2025年。Autoware——全球领先的自动驾驶开源软件项目。https://github.com/autowarefoundation/autoware。[20] Aurélien Francillon、Boris Danev和Srdjan Capkun。2011年。针对现代汽车被动式无钥匙进入和启动系统的中继攻击。载于网络与分布式系统安全研讨会论文集（NDSS）。苏黎世联邦理工学院，计算机科学系。[21] Lu Gan、Wenbo Chu、Guofa Li、Xiaolin Tang和Keqiang Li。2024年。面向智能交通系统和自动驾驶汽车的大模型：综述。《先进工程信息学》62（2024），102786。[22] Cong Gao、Geng Wang、Weisong Shi、Zhongmin Wang和Yanping Chen。2022年。自动驾驶安全：现状与挑战。《IEEE物联网期刊》9卷10期（2022），7572–7595。doi:10.1109/JIOT.2021.3130054[23] Joshua Garcia、Yang Feng、Junjie Shen、Sumaya Almanee、Yuan Xia和Qi Alfred Chen。2020年。自动驾驶汽车软件缺陷综合研究。载于2020年IEEE/ACM第42届软件工程国际会议（ICSE）。385–396。[24] Batuhan Gul和Fatih Ertam。2024年。车内通信网络安全：挑战与解决方案综述。Vehicular Communications（2024），100846。[25] Sandeep Gupta、Carsten Maple和Roberto Passerone。2023年。对网联和自动驾驶车辆。IEEE Access 11（2023），90641–90669。doi:10.1109/ACCESS.2023.3307473[26] Linqing Hu、Junqi Zhang、Jie Zhang、Shaoyin Cheng、Yuyi Wang、Weiming Zhang 和 Nenghai Yu。2025年。针对自动驾驶多传感器融合定位的安全分析与自适应虚假数据注入。Inf. Fusion 117，C（2025年2月），17页。doi:10.1016/j.inffus.2024.102822[27] Pengfei Jing、Zhiqiang Cai、Yingjie Cao、Le Yu、Yuefeng Du、Wenkai Zhang、Chenxiong Qian、Xiapu Luo、Sen Nie 和 Shi Wu。2024年。重新审视汽车攻击面：从业者视角。载于2024年IEEE安全与隐私研讨会（SP）。IEEE，2348–2365。[28] Guanpeng Li、Yiran Li、Saurabh Jha、Timothy Tsai、Michael Sullivan、Siva Ku- mar Sastry Hari、Zbigniew Kalbarczyk 和 Ravishankar Iyer。2020年。AV-FUZZER：发现自动驾驶系统中的安全违规。载于2020年IEEE第31届国际软件可靠性工程研讨会（ISSRE）。25–36。doi:10.1109/ISSRE5003.2020.00012[29] Trupil Limbasiya、Ko Zheng Teng、Sudipta Chattopadhyay 和 Jianying Zhou。2022年。网联与自动驾驶汽车攻击检测与防范的系统性综述。Vehicular Communications 37（2022），100515。doi:10.1016/ j.vehcom.2022.100515[30] Feng Luo、Xuan Zhang、Zhenyu Yang、Yifan Jiang、Jiajia Wang、Mingzhi Wu 和 Wanqiang Feng。2022年。汽车领域网络安全测试：综述。Sensors 22，23（2022），9211。[31] Roberto Metere、Myriam Neaimeh、Charles Morisset、Carsten Maple、Xavier Bellekens 和 Ricardo M Czekster。2021年。保障电动汽车充电基础设施的安全。arXiv预印本 arXiv:2105.02905（2021）。[32] Farahnaz Javidi Niroumand、Parisa Ansari Bonab 和 Arman Sargolzaei。2024年。网联与自动驾驶汽车安全：攻击与缓解策略综述。载于SoutheastCon 2024。1197–1204。doi:10.1109/SoutheastCon52093.2024.10500196[33] Irdin Pekaric、Clemens Sauerwein、Stefan Haselwanter 和 Michael Felderer。2021年。汽车领域攻击机制分类体系。Computer Standards & Interfaces 78（2021），103539。[34] Minh Pham 和 Kaiqi Xiong。2021年。网联与自动驾驶汽车安全攻击与防御技术综述。Computers & Security 109（2021），102269。[35] Ali Rezaei Nasab、Mojtaba Shahin、Seyed Ali Hoseyni Raviz、Peng Liang、Amir Mashmool 和 Valentina Lenarduzzi。2023年。微服务系统安全实践的实证研究。Journal of Systems and Software 198（2023），111563 10 1016 2022 111563 。doi: . /j.jss. 。[36] Martin Salfer 和 Claudia Eckert。2015年。汽车电子控制单元的攻击面与漏洞评估。载于2015年第12届电子商务与电信国际联合会议（ICETE），第4卷。IEEE，317–326。[37] N Semiconductor。2018年。汽车网关：保障网联汽车安全的关键组件。[38] Qingchao Shen、Haoyang Ma、Junjie Chen、Yongqiang Tian、Shing-Chi Cheung 和 Xiang Chen。2021年。深度学习编译器缺陷的全面研究。载于第29届ACM欧洲软件工程会议与软件工程基础研讨会联合会议论文集（希腊雅典）（ESEC/FSE 2021）。计算机协会，美国纽约州纽约，968 980 10 1145 3468264 3468591 –。doi: . / 。[39] Florian Sommer、Jürgen Dürrwang 和 Reiner Kriesten。2019年。汽车安全攻击的综述与分类。Information 10，4（2019），148。[40] Chengnian Sun、Vu Le、Qirun Zhang 和 Zhendong Su。2016年。迈向对GCC和LLVM编译器缺陷的理解。载于第25届国际软件测试与分析研讨会论文集（德国萨尔布吕肯）（ISSTA 2016）。计算机协会，美国纽约州纽约，294–305。doi:10.1145/2931037.2931074[41] Xiaoqiang Sun、F. Richard Yu 和 Peng Zhang。2022年。网联与自动驾驶汽车（CAVs）网络安全综述。IEEE Transactions on Intelligent Transportation Systems 23, 7 2022 6240 6259 10 1109 2021 3085297 ( ), –。2020 [42] doi: . /TITS. 。Junko Takahashi、Makoto Iwamura 和 Masashi Tanaka。 。汽车信息娱乐系统的安全威胁分析。载于2020年IEEE第92届车辆技术会议（VTC2020-Fall）。1–7。doi:10.1109/VTC2020-Fall49728.2020. 9348647[43] Shuncheng Tang、Zhenya Zhang、Yi Zhang、Jixiang Zhou、Yan Guo、Shuang Liu、Shengjian Guo、Yan-Fu Li、Lei Ma、Yinxing Xue 等。2023年。自动驾驶系统测试综述：现状与趋势。ACM Transactions on Software Engineering and Methodology 32，5（2023），1–62。[44] Vrizlynn L.L. Thing 和 Jiaxi Wu。2016年。自动驾驶汽车安全：攻击与防御分类体系。载于2016年IEEE国际物联网会议（iThings）、IEEE绿色计算与通信会议（GreenCom）、IEEE网络、物理与社会计算会议（CPSCom）和IEEE智能数据会议（Smart-Data）。164 170 10 1109 2016 52 –。doi: . / iThings-GreenCom-CPSCom-SmartData. 。[45] Jiongchi Yu、Xiaofei Xie、Cen Zhang、Sen Chen、Yuekang Li 和 Wenbo Shen。2024年。容器 Pod 中的缺陷：理解容器运行时系统中的缺陷。载于第33届ACM SIGSOFT国际软件测试与分析研讨会论文集（奥地利维也纳）（ISSTA 2024）。计算机协会，美国纽约州纽约，1364–1376。doi:10.1145/3650212.3680366

[46] Haichun Zhang、Jie Wang、Yijie Wang、Minfeng Li、Jinghan Song 和 Liu Zhenglin。2023年。ICVTest：用于评估智能网联汽车网络安全性的实用黑盒渗透测试框架。*Applied Sciences* 14（2023年12月），204。doi:10.3390/app14010204

[47] Zhen Zhang、Yuezhong Zhang、Jinfeng Zhang、Jichao Xie 和 Shaoxun Liu。2024年。智能网联汽车车载远程信息处理盒的内生安全研究。*IEEE Embedded Systems Letters*（2024年）。