CCID 赛迪智库 专报

2018 年 3 月 12 日　　第 17 期　　总第 599 期

我国智能网联汽车信息安全管理亟待加强

【内容提要】　新一轮科技革命和产业变革的加速融合，智能网联汽车的快速发展，为消费者提供了便利的使用方式、丰富的应用内容和安全的驾驶环境。但与此同时，由智能网联带来的信息安全问题也更加突出，并已引起各国政府的高度重视，美国、欧洲和日本等主要发达国家和地区都在积极应对。赛迪智库装备工业研究所认为，我国应尽快推进智能网联汽车信息安全技术的研发与应用，建立智能网联汽车信息安全法规标准，制定建立制定智能网联汽车信息安全测试规范。

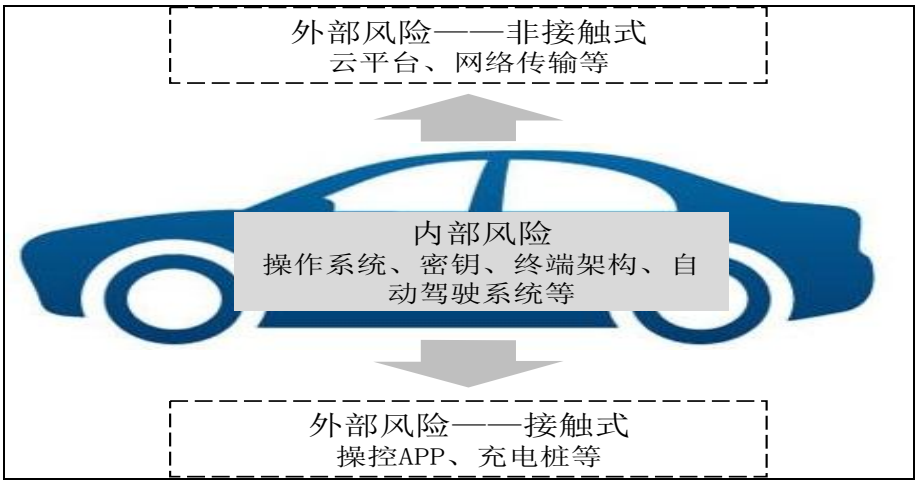
【关键词】　智能网联汽车　信息安全　管理

随着汽车智能化、网联化程度的不断提高，信息篡改、病毒入侵等汽车信息安全问题更加突出。早在2015年美国研究机构Ponemon就曾表示，未来将有60%-70%的车辆会因信息安全漏洞被召回，汽车受到信息安全攻击的威胁逐步提升。我国在大力发展智能网联汽车的同时，必须高度重视可能随之而来的信息安全风险，提高防御网络攻击的能力。

一、智能网联汽车面临多重信息安全风险

相关调查显示，大多数车企信息安保措施不完善，不能实时或主动应对安全入侵。目前，智能网联汽车面临的信息安全风险主要来自于车辆、云端、网络传输，以及相关联的外部设备。

图1　智能网联汽车信息安全风险架构



资料来源：赛迪智库整理

（一）车辆安全风险

一是操作系统安全。作为智能网联汽车的核心部件，操作系统向上承载应用、通信等功能，向下承接底层资源调用和管理。目前，大部分车企采用的都是开源方案，虽可极大降低开发成本，但存在安全漏洞、鲁棒性缺失以及缺乏对操作系统行为监控等安全风险。**二是密钥安全。**保护数据隐私与机密性的通常做法是实施数据加密，一旦密钥被泄露，加密数据的安全性将荡然无存。**三是终端架构安全。**汽车内部相对封闭的网络环境也存在很多可被攻击的安全缺口，如胎压监测系统、距离通信设备、MOST 总线、CAN 总线、LIN 总线等，对于外部攻击的防御能力较弱。**四是硬件安全。**自动驾驶和自动巡航系统，利用微波雷达和激光雷达装置探测前方障碍物，依赖行车信息采集系统将车辆状态及行车环境信息传递给车载中控系统，一旦被攻击，将存在车辆安全事故风险。

（二）云平台安全风险

智能网联汽车管控中心的云平台同样面临着各种恶意威胁。除了需要病毒防护、中间件安全防护以及访问控制防护外，还要重视数据安全防护问题，防止车主存储到云端的数据（特别是隐

私数据）意外丢失、被窃取。目前大部分车联网数据使用分布式技术进行存储，面临的主要安全威胁包括黑客对数据恶意窃取和篡改、敏感数据被非法访问等。随着智能网联汽车持续发展，数据安全、访问控制等威胁也会越来越多，云端安全威胁不容忽视。

（三）网络传输安全风险

V2X（人、车、路、互联网等）通过 Wi-Fi、移动通信网（3G/4G/5G 等）、DSRC 等无线通信手段，与其它车辆、交通专网、互联网等进行连接。车载终端与网络中心进行双向数据传输，主要存在三大安全风险。**一是认证风险**。没有验证发送者的身份信息、伪造身份、动态劫持等。**二是传输风险**。车辆信息没有加密或强度不够、密钥信息暴露、所有车型使用相同的对称密钥。**三是协议风险**。通信流程伪装，把一种协议伪装成另一种协议。在自动驾驶情况下，汽车会按照 V2X 通信内容判断行驶路线，攻击者可以利用伪消息诱导车辆发生误判，影响车辆自动控制，促发交通事故。

（四）外部连接设备安全风险

操控 App、充电桩等外部生态组件频繁接入智能网联汽车，每个接入点都意味着新风险点的引入。驾驶者在购买和安装外接

产品时，有带来外部病毒入侵攻击的风险，尤其是智能手机、平板电脑、PDA、GPS 卫星导航系统等，这些便携设备掺杂着大量仿制、山寨产品和恶意代码应用程序等，并且获取成本低、安全防护能力不足，值得高度重视。汽车制造企业在车辆开发设计时，必须重点考虑用户带入车内的便携和外接设备可能引发的恶性信息安全攻击威胁。

二、各国政府着力加强智能网联汽车信息安全管理

（一）美国全方位信息安全法规标准

美国将汽车信息安全上升到国家安全层面，先于产业发展提前部署法规标准，走在世界前列。在法规方面，2017 年 9 月美国众议院通过《确保车辆演化的未来部署和研究安全法案》(《自动驾驶方案》)，要求车企必须制定详细的网络安全计划，遵循 NHTSA 的网络安全指导，否则法案将阻止其制造、销售或进口高度自动化车辆、全自动化车辆或自动驾驶系统。在标准方面，美国率先推出了 SAE J3061/IEEE 1609.2《汽车系统网络安全指南》等系列标准，内容涉及汽车信息安全完整性等级、测试方法和工具等，以保证汽车在全生命周期中都可获得有效的信息安全

保护。同时，美国 SAE 与 ISO/TC22 道路车辆技术委员会以联合工作组的形式成立了汽车信息安全工作组，正式启动了 ISO 层面的国际标准法规制定工作。2016 年，美国 NHTSA 发布了《现代汽车信息安全最佳实践》，针对快速发展的智能网联汽车信息安全及隐私保护等问题，推出了最佳实践框架结构。

（二）欧洲汽车零部件及网络通信安全

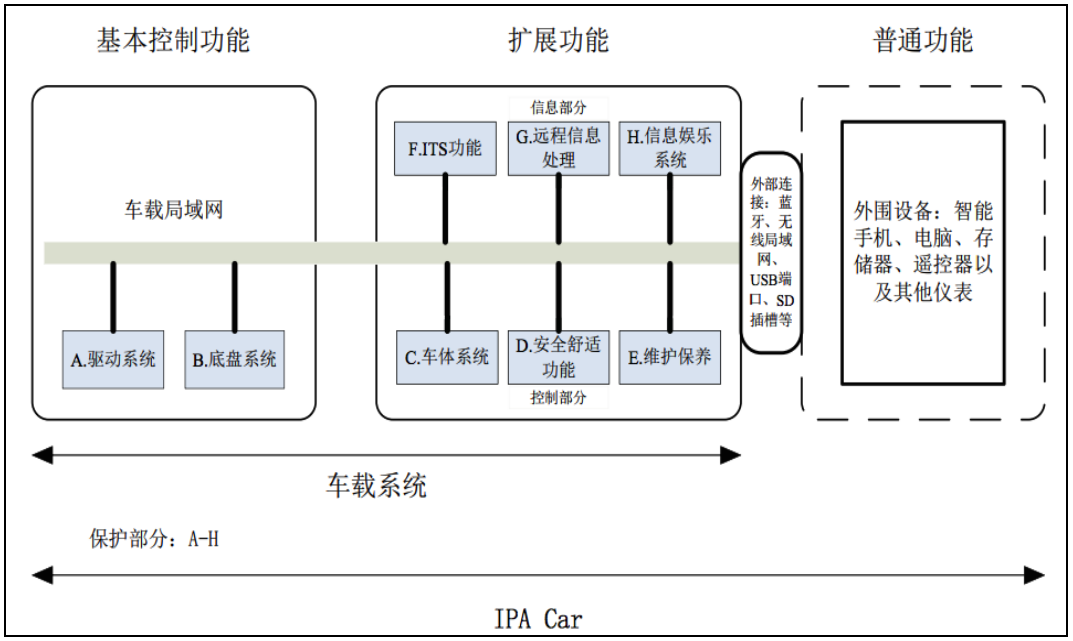
欧洲依托强大的汽车制造商和零部件厂商，自 2008 年开始分别开展了 EVITA、OVERSEE、PRESERVE 等项目，从汽车硬件安全、车辆通信系统架构、V2X 通信安全等方面，提出了解决方案和技术规范，部分技术成果已实现产业化应用。另外，欧洲电信标准协会（ETSI）针对智能网联汽车与智能交通系统制定了系列信息安全标准，具体涉及 ITS 安全服务架构、ITS 通信安全架构与安全管理、可信与隐私管理、访问控制和保密服务等方面。

（三）日本汽车生命周期信息安全保护措施

日本信息处理推进机构 IPA 推出的汽车信息安全指南，从汽车可靠性角度出发，通过对车辆功能群分类，定义了汽车信息安全模型 IPA Car，将信息安全产生威胁的原因分成用户偶然引发

的失误和攻击者恶意造成的威胁，提出了信息加密、判定用户程序的合法性、对使用者操作权限和通讯范围实施访问控制管理等应对之策。同时，IPA 按照汽车设计、开发、使用、废弃的全生命周期，整理出安全管理方针。在设计阶段结合各项功能安全性的重要程度进行预算分配，在开发阶段采用防漏洞的安全编码和编码标准，在使用阶段构筑信息安全迅速应对联络机制，废弃阶段提供信息删除功能等。

图 2　日本汽车信息安全模型 IPA Car



资料来源：中国科学院信息工程研究所

三、对策建议

（一）推进智能网联汽车信息安全技术研发与应用

智能网联汽车涉及多领域技术，是移动互联网、物联网、云计算等多种技术的应用平台，技术架构复杂，信息安全防护难度大。传统汽车信息安全技术无法满足更高的防护要求，亟需结合智能网联汽车的特点和使用场景，开展信息安全关键技术攻关。

一是加强智能网联汽车关键芯片、基础软件、核心算法、通信协议和系统应用等创新，提升自主可控水平，重点研发芯片加密技术、应用软件安全防护技术，以及安全隔离架构技术、云平台数据加密安全防护技术等，降低外部设备风险。二是运用大数据、云计算、人工智能等高新技术，加强对个人信用记录、违法失信行为等数据的收集与分析，通过事前感知、事中防御、事后分析，降低攻击发生的可能性。三是在国家科技专项中支持智能网联汽车信息安全技术的研发和推广应用，设立课题，强调部门协作进行关键技术公关。四是构建智能网联汽车基础数据交互管理平台，推动各车企平台、服务提供商平台信息数据的实时接入，统一监管，以保证监管和服务的时效性、精准性和前瞻性。

（二）建立智能网联汽车信息安全法规标准

智能网联汽车的计算、控制和传感单元以及连接路径，都存在被黑客攻击和控制的风险。提前预研并出台相应的法规标准，明确汽车生产商、零部件企业责权非常必要。近年来，美国、日本、欧洲等国家和地区积极推进智能网联汽车信息安全标准的研究制定，我国 2017 年 6 月发布了《国家车联网产业标准体系建设指南》（征求意见稿），也首次提出要制定 30 项以上智能网联汽车重点标准。

一是加强智能网联汽车信息安全立法工作，明晰信息安全框架下对汽车企业、零部件企业的要求，明确由于信息安全系统被破坏引发恶性事件的责任判定和处罚。二是跟踪全球智能网联汽车信息安全标准化动态，加快制定智能网联汽车信息安全防护标准，包括《汽车信息安全防护通用技术条件》、《汽车网关信息安全技术要求》、《汽车信息安全通用技术规范》、《车载 T-BOX 信息安全技术要求》、《电动汽车充电信息安全防护规范》等。三是制定智能网联汽车数据安全技术标准，通过对数据进行分级，确定保护级别，建立云安全、管安全、端安全的数据安全标准框架。

（三）制定智能网联汽车信息安全测试规范

搭建智能网联汽车检测和评估平台，衡量信息安全保护管理措施和技术措施是否符合信息安全保护需求，通过测试排查信息安全隐患和薄弱环节，明确整改要求，提升安全防护能力。

一是对智能网联汽车信息安全技术应用进行分类汇总，研究制定《汽车信息安全通用测试与评价方法》，保障信息安全的可控性。二是搭建智能网联汽车操作系统、通信系统、信息服务系统等产品信息安全的测试平台，依托第三方评测机构开展检测服务与评估，对产品可能存在的缺陷和弱点进行安全检测。三是推动DA、PA级智能网联汽车通过国家信息认证体系实现自愿认证。对CA、HA、FA级智能网联汽车要求实施强制安全认证。

本文作者：工业和信息化部赛迪研究院　　徐可　赵世佳
联系方式：18600457809
电子邮件：xuke @ccidthinktank.com

赛迪智库
面向政府 服务决策

研究，还是研究
才使我们见微知著

信息化研究中心	工业化研究中心	规划研究所
电子信息产业研究所	工业经济研究所	产业政策研究所
软件产业研究所	工业科技研究所	军民结合研究所
网络空间研究所	装备工业研究所	中小企业研究所
无线电管理研究所	消费品工业研究所	政策法规研究所
互联网研究所	原材料工业研究所	世界工业研究所
集成电路研究所	工业节能与环保研究所	安全产业研究所

编 辑 部：赛迪工业和信息化研究院
通讯地址：北京市海淀区万寿路27号院8号楼12层
邮政编码：100846
联 系 人：刘 颖 董 凯
联系电话：010-68200552 13701304215
010-68207922 13910685050
传 真：0086-10-68209616
网 址：www.ccidwise.com
电子邮件：liuying@ccidthinktank.com

报：部领导

送：部机关各司局，各地方工业和信息化主管部门及相关部门

编 辑 部：工业和信息化部赛迪研究院
通讯地址：北京市海淀区万寿路27号院南门8号楼12层
邮政编码：100846
联 系 人：刘颖　董凯
联系电话：010-68200552　13701304215
010-68207922　13910685050
传　　真：010-68200534
网　　址：www.ccidwise.com
电子邮件：liuying@ccidthinktank.com