全方位保护智能网联汽车信息安全研究

刘平一　王海均
中汽数据（天津）有限公司　天津　300393

[摘　要]随着我国科学技术的快速发展，智能网联汽车也为消费者提供了安全舒适的驾驶环境，其应用内容变得更加丰富，使用方式也更为便利。但同时智能化与网联化也会产生一些信息安全问题，进而使得智能网联汽车面临多重风险。当有信息安全问题产生后，一方面会对行车安全造成影响，另一方面还会泄露用户的重要数据，威胁到国家安全。对此，相关研究人员需要针对智能网联汽车的信息安全采取全方位保护，加大对安全问题的重视程度，采取有效的保护措施，以此来促进智能网联汽车行业的健康发展。本文针对全方位保护智能网联汽车信息安全进行分析，介绍了智能网联汽车面临的多重信息安全风险，并提出全方位保护措施，希望能够为相关研究人员起到一些参考和借鉴。

[关键词]全方位保护；智能网联汽车；信息安全
【DOI】10.12252/j.issn.2096-627X.2021.12.749

对于智能网联汽车而言，信息安全是其一项核心技术，需要涉及到国家战略安全。现如今，美国、欧洲以及日本等发达国家对汽车信息安全技术的研发工作不断推进，力求对此战略技术制高点进行抢占。而我国同样高度重视汽车信息安全，并在相关发展和规划当中明确提出，应将网络安全作为一项重点内容，合理建设智能网联汽车标准体系。我国的汽标委以及汽车工程协会，都在不断加快智能网联汽车信息安全标准体系的建设工作，并制定出具体的审核标准，这对汽车行业的发展具有重要促进作用。为了有效保证汽车信息安全，需要全方位的采取保护对策，有效识别信息安全风险，并采取针对性的预防对策，使智能网联汽车的信息安全水平得到有效提高。

一、智能网联汽车面临的多重信息安全风险

（一）车辆安全风险

在终端系统当中，将车辆作为系统当中的智能终端，而随着汽车智能化和网联化水平的不断提升，其自身所面临的相关信息安全问题也有所增多。对于车辆信息安全风险而言，具体需要涉及到以下几方面内容。首先，系统安全，具体包括软件系统和硬件系统两部分。目前，软件在汽车中的占比不断增加，这也使软件安全风险有所增大，例如主机厂在开放软件安装包下载后，容易受到相关黑客的攻击。而硬件系统安全则具体包括自动巡航系统以及自动驾驶，通过对障碍物进行伪造，可以使毫米波雷达的判断受到干扰，最终导致车辆前进被干扰或逼停。当汽车受到攻击后，可能会引发相关安全事故。其次，密钥安全。相关工作人员一般会采用数据加密方式对数据隐私加以保护，如果密钥遭到泄露，将会严重影响加密数据的安全性。例如，在远离汽车时对钥匙信号进行录制，可以有效实现一次性开门。而且在分析解码后，还可通过具体计算，使误差维持在合理范围内，以此来有效实现无限次开门。攻击者利用插桩调试可对控制信息进行获取，并进行逆向分析，以此来对控制流程加以获取，通过脚本的蓝牙钥匙对汽车加以控制。最后，架构安全。汽车内部的网络环境相对封闭，但也存在相应缺口，降低了其对外部攻击具有的防御能力，包括面向媒体的控制器、局域网络系统传输总线以及车载诊断系统接口等[1]。

（二）云平台安全风险

在智能网联汽车系统当中，云平台是十分重要的组成部分，具有丰富的功能，可以从娱乐服务提供监督管理和故障远程诊断等方面对车辆加以控制。而云平台安全具体需要涉及到数据库、设备主机、物理环境以及应用程序安全等。在云平台当中，往往需要面临许多恶意威胁，不仅包括病毒防护和访问控制防护，而且还需要涉及到数据安全防护，特别是对云端数据的窃取与丢失等问题进行预防。现如今，多数车联网数据主要采用分布式技术加以存储，其面临的安全威胁包括非法访问敏感数据、黑客恶意窃取与篡改数据。在未来还可通过云平台使多种形式的云服务得到有效实现，对车队车辆进行跟踪与管理。在智能网联汽车快速发展的背景下，数据安全以及访问控制等方面也有了更多的威胁，需要高度重视云平台安全风险。

（三）网络传输安全风险

V2X主要是指智能网联汽车的对外通信连接，主要为第5代移动通信网络和长期演进。现如今，我国对通信技术发展也在不断推动，而专用短程通信技术是十分成熟的一类技术，在车车通信方面有着明显优势。对于通信安全而言，需要有效保证通信的完整性，禁止非法篡改传输消息。同时还需要对伪装或中间人攻击进行有效预防，从而使消息能够由合法设备发送，提高通信过程的可用性与性能。在网络传输过程当中，其安全风险具体包括以下几个方面。首先，认证风险，主要通过动态劫持以及身份伪造等方式对验证者的身份信息加以冒充。其次，传输风险。在未加密车辆传输信息或缺乏强度时，往往容易受到相关攻击。最后，协议风险。通信流程通常将一种协议进行伪装，使其成为另一种协议。例如，由于未加密协议链路层通信，进而对链路层标识进行抓取，以此来定位车辆，并加以跟踪。在自动驾驶过程当中，汽车可结合V2X通信内容对行驶路线进行制定，而攻击者则利用伪消息对车辆进行诱导，使其发生误判，最终对车辆

控制产生影响[2]。

（四）外部链接设备安全风险

目前，智能网联汽车所承载的功能不断增多，对相关外部生态组件的频繁接入，会使车辆有新的安全风险产生，包括充电桩与操控APP等。消费者在对车辆外部链接产品进行购买与安装时，也为外部病毒的入侵与攻击提供机会。首先，在便携设备当中，往往有大量仿制恶意代码、应用程序或山寨产品等参杂，此类外联设备组件虽然成本相对较低，但其缺乏安全防护能力。其次，新能源汽车充电桩往往表现出相应的安全风险内容，将充电桩控制模块以管理系统和以太网进行连接，由于未防护网络内部进而其可运用互联网，在桩联网当中进行入侵，使充电电压被控制，并篡改了具体的充电金额。与此同时，充电APP关系到移动支付，通过将木马植入到手机当中，可以进行恶意吸费以及信息窃取等行为。最后，现有汽车的后装产品，往往面临相应的信息安全。从实际情况出发，相关车辆设计未充分考虑信息安全，如后装车机以及OBD盒子等，往往都存在一定的潜在风险。所以，在研发车辆时需要对外接设备的信息安全进行充分考虑[3]。

二、智能网联汽车信息安全的全方位保护策略

（一）推进智能网联汽车信息安全技术研发

为了促进智能网联汽车的健康发展，对信息安全技术也提出了更高要求。一方面需要满足安全功能需求，对网络攻击加以抵御，对软件漏洞进行检测扫描，避免数据遭到篡改，对异常行为进行实时检测，而另一方面对车辆功能也提出了相关特殊需求，具体包括保证隐私信息安全和车辆行驶安全，实现车辆信息交互。由于传统车辆处于相对封闭的状态，所以在设计车辆功能时，主要为功能安全与实时性，对信息安全未进行充分考虑。而随着车辆智能化的快速发展，在信息安全领域也有许多和车辆相关的风险衍生而出。所以，为了使智能网联汽车的信息安全得到保障，需要针对设计、研发以及生产等过程充分考虑信息安全元素，并对信息安全闭环进行建立，以此来使车辆的信息安全防护水平得到有效提高。

首先，加强顶层设计。通过合理制定政策以及发布指南，可以规范指导行业，并对智能网联汽车的信息安全防护体系进行建立，有效研发与应用信息安全技术。其次，需要从全生命周期维度出发，对智能网联汽车的信息安全防护进行强化，使关键芯片、通信协议、软件以及系统应用等得到有效创新，从而使安全可控水平得到提升。除此之外，还需要对芯片加密技术进行有效研发，合理运用软件、云平台数据加密以及安全隔离架构等安全防护技术。在远程监控平台当中，需要对信息安全监控模块进行导入，从而实时预警与监控外部链接设备和车辆等安全隐患，使恶意攻击的扩散与传播得到有效抑制。除此之外，还应对漏洞或者攻击及时进行上报，不仅要将安全漏洞第一时间弥补，而且还应对自身的安全性进行有效提升[4]。

（二）建立智能网联汽车信息安全标准法规

智能网联汽车信息安全是一项新兴领域，在监管主体、方法、内容以及手段等方面还未配备具体的法律法规。虽然目前已对相关网络安全法进行颁布，但由于未针对具体行业制定细则和解读，导致在开展监管工作时缺乏具体的法律依据和规章制度。对此，我国应对国外的汽车信息安全标准法规进行充分借鉴，并依据我国智能网联汽车的发展特点和信息安全问题，使汽车信息安全行业规范得到强化。首先，需要针对汽车信息安全强化立法工作，对信息安全框架下相关企业的要求进行明确，同时还应确定相关恶性事件的处罚以及责任判定。其次，需要对全球智能网联汽车的信息安全标准化动态加以跟踪，并与标准化机构相联合，使信息安全防护标准得到有效制定。最后，需要对智能网联汽车的数据安全技术标准进行制定，实现数据分级，对其保护级别加以确定。

（三）制定智能网联汽车信息安全测试规范

在智能网联汽车的发展过程当中，信息安全已成为相关企业的关注焦点。通过开展具体的安全测试工作，可对信息安全保护措施的有效性进行衡量判断，其是否与相关防护需求相符合，并通过测试对信息安全的薄弱环节以及隐患进行排查，使安全防护能力得到有效提高。首先，应对智能网联汽车的信息安全技术要求进行明确，并合理构建测评标准体系，对智能网联汽车的评估与检测平台进行合理搭建。其次，需要结合车辆的具体应用场景，对车辆信息安全威胁以及风险等级进行分析，构建智能化的车辆信息安全分析模型，从而有效检测相关产品可能存在的缺陷问题。

结束语

综上所述，在智能网联汽车行业的发展过程当中，需要对信息安全问题加大重视，并全方位的采取保护策略，以此来全面提高智能网联汽车的信息安全水平，从而更好的实现智能网联汽车发展战略。

参考文献

[1]安晖.全方位保护智能网联汽车信息安全[J].智能网联汽车，2020，14（2）：42-44.

[2]赵世佳，徐可，薛晓卿，等.智能网联汽车信息安全管理的实施对策[J].中国工程科学，2019，21（3）：108-113.

[3]刘伟莲.智能网联汽车信息安全关键技术探讨[J].电子测试，2020，12（8）：61-62.

[4]郭辉，罗勇.智能网联汽车信息安全关键技术[J].上海汽车，2019，34（10）：9-14.