汽车信息安全攻防关键技术研究进展

冯志杰, 何 明, 李 彬, 邓 明

中国科学院信息工程研究所 北京 中国 100093

摘要 汽车技术的迅猛发展, 车载信息系统的智能化、电子化水平不断提高, 促使了车辆信息安全问题已经成为近年来最热门的研究领域之一。为提高车载信息系统抗攻击能力、实现汽车的安全平稳运行, 从信息安全的角度, 综述了汽车入侵式攻击与车辆信息安全防护保障措施理论与关键技术: 对现代汽车的车载信息系统概念、结构、软件标准化等进行了详细的论述; 对汽车的功能性安全、信息系统安全的区别进行了详细对比; 对现代汽车入侵式攻击的方法与种类, 及安全防护保障策略等进行了深入剖析; 对汽车信息安全领域的国内外研究进展情况作了概括性总结; 最后给出了汽车信息安全领域的发展趋势及展望。

关键词 汽车信息安全; 车载信息系统; 车载诊断系统; 电子控制单元; 汽车入侵式攻击; 防护保障策略
中图法分类号 TP309.2 DOI 号 10.19363/j.cnki.cn10-1380/tn.2017.04.001

Research on Car Information Security Attack and Protection Technology

FENG Zhijie, HE Ming, LI Bin, DENG Ming

Institute of Information Engineering, CAS, Beijing 100093, China

Abstract The rapid development of automotive technology, automotive information system of intelligent, electronic level has been improved continually, the vehicle information security problem has become one of the most popular research field in recent years. In order to improve the attack resistance ability of the vehicle information system and realize the automotive safety running smoothly, in the perspective of information security, car invasive attack and vehicle information were reviewed safety guarantee measures: theory and key technologies for modern automobile vehicle information system concept, structure, standardization of software and so on are described in detail; functional on car safety, makes a detailed contrast the difference between information system security; the modern car invasive attack methods and types, and guarantee of safety protection strategy etc. are carried on the thorough analysis; the car in the field of information security research progress at home and abroad made a general summary; the future development trend and prospects for car information security are also discussed.

Key words car information security; automotive information system; On-Board diagnostics; electronic control unit; car invasive attack; safety protection strategy

1 引言

互联网发展的大潮给汽车行业带了前所未有的冲击, 汽车通过网络与外界的信息互联愈加频繁。功能丰富的电子产品迅速在汽车上普及, 使汽车行业整体的电子化水平显著提升, 截止到 2016 年汽车电子化率已经快速提升到 30%~40%[1]。汽车中嵌入复杂的电子信息系统, 涵盖了大量的信息通信技术。另外, 汽车本身也是一个复杂的网络通信系统。车载信息系统承担了汽车内部电控单元之间的信息交互, 车内控制系统的电控单元通过不同的总线网络进行通信, 而各个总线网络通过网关相互连接, 构成了车载信息系统[2]。

车载信息系统并不是简单的汽车与网络之间的互联, 而是包含了汽车与互联网(V2I), 车与车(V2V), 车与智能交通基础设施(V2A), 车与云端(V2C)的互联, 以及车载网络通信的多网、跨网融合技术[3]。网联汽车、车载自组织网络和智能交通基础设施共同构成了全新的汽车控制系统[2-4]。

车载信息系统安全技术的概念是[5]: 利用系统

通讯作者: 何明, 博士, 助理研究员, Email:heming0405@163.com

本课题得到 National High Technology Research and Development Program of China (863 Program, No. 2013AA01A214). (国家高技术研究发展计划(863)项目)资助。

收稿日期: 2017-01-05; 修改日期: 2017-03-20; 定稿日期: 2017-03-24

化的车内电控设备信息采集, 通过综合分析与智能危机处理机制, 达到车内子系统和智能交通系统协调配合的目的, 从而最大程度保障汽车运行安全。车载信息系统中控系统是该系统的核心部分[6], 通过总线接口与各类车内总线相连, 实现与汽车的各总线及子系统的数据交换和控制功能。

诊断设备通过诊断总线与中控相连, 其作用包括[7]: 汽车行驶记录数据下载、实时数据检测、设置车载信息系统、在线故障分析与诊断等。车载信息系统中控系统通过三路总线与车内各分线及职能模块相互连接, 实现数据交换与信息共享功能。车载信息系统包含的子系统如图 1 所示。

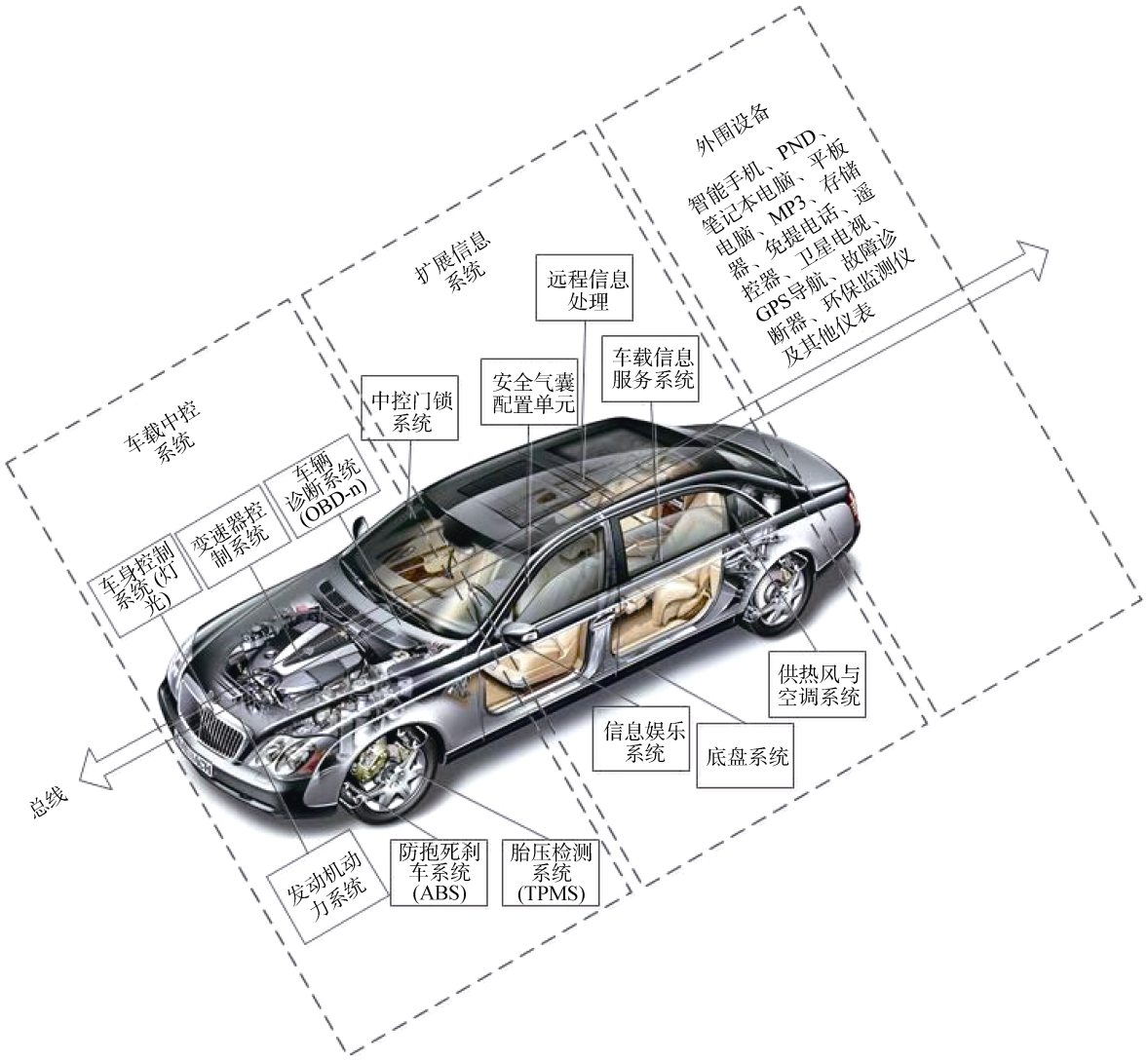


图 1　车载信息系统结构图

软件标准化[8]是车载信息系统的发展方向和必然趋势, 该系统的软件设计从多个层面进行了规范: 一是设计了兼容 OSEK 标准的嵌入式操作系统, 为许多底层操作, 如任务调度、网络管理等提供了标准的函数接口与规范, 应用软件的复杂度以及可靠性都有很大的提高; 二是几乎所有软件代码均采用 C 语言编写, 具有较好的可移植性及可维护性。

车载信息系统综合了多项汽车热点技术, 集成了行驶记录功能, 简化了车身电气线束, 实现了基于全车信息的实时故障分析, 为实现低成本、低功耗、易于实施的汽车安全系统开拓了一个新的思路。同时, 该系统构建了一个低成本的公共接入平台, 通过对现有技术的简单接入或改进, 实现全车信息共享、集中调度与最佳控制, 从系统性的高度实现汽车行驶安全。

2　国内外汽车攻击防御实例分析

任何设备只要连接互联网, 就有可能遭受黑客的恶性攻击。在享受网络带来便利的同时, 也必须面对网络的“黑暗面”——信息安全威胁, 这一点汽车

行业也不能幸免。从广义的角度而言, 国际上对汽车信息安全方向的攻击防御研究主要集中在三个方向: 车辆入侵式攻击、安全漏洞分析、车辆安全防御。如表 1 所示:

表 1 国内外车辆信息安全攻防实例分析

攻防实例类型和年份	车辆入侵攻击实例	安全漏洞分析实例	车辆安全防御实例
2010 年	攻击车胎胎压监测系统	Koscher 进行基准型、静车型、动车型实验和评估	Checkoway 提出单组件安全威胁模型
2011 年		发布 ECU 漏洞分析、威胁评估报告	
2013 年	①高速行驶下的汽车突然制动和转向; ②高速行驶下的车辆突然刹车失灵	360 团队为车厂做 Tbox 和 TSP 评测	Wolf 提出汽车总线防护建议
2014 年	①远程攻击 Tesla(特斯拉)事件; ②毫米波雷达, 超声波雷达遭受攻击	20 余款车型信息安全报告评估	华晨表示提出网络访问控制、关键数据加密、存储等进行安全维护与处理
2015 年	①雪佛兰 OBD 遭受攻击; ②车联网安吉星遭受攻击; ③Jeep Cherokee 遭受攻击	Ponemon 公布 60%~70%的汽车存在安全漏洞	

车载信息系统遭受最早的攻击案例发生在 2010 年[9], 南卡罗来纳州罗格斯大学的研究人员通过破解汽车内部信息系统, 伪造部分品牌型号汽车的胎压传感器信息, 干扰并毁坏距离 40 米以外汽车的轮胎压力监测系统(Tire Pressure Monitoring System, TPMS)。

加州大学圣地亚哥分校(UCSD)和华盛顿大学的两个研究团队, 于 2011 年就以“汽车安全攻击综合分析[10]”为题进行了实验和论证, 并从威胁类型、具体漏洞分析以及威胁评估三个方面进行了评估。其研究的主要对象是汽车内部的电子控制单元[10] (Electronic Control Unit, ECU)。

2013 年, 在拉斯维加斯黑客大会上, 著名白帽黑客 Miller 和 Valasek[11]博士对一辆处于高速行驶状态下的丰田普锐斯(Toyota Prius)发起攻击, 实现使其在高速行驶时刹车失灵或者突然制动等异常行为, 并发表了相关的“攻击白皮书”, 包括: 攻击过程使用的源代码、编译器及连接件原理图等。他们还可以让福特翼虎(Ford Escape)在慢速行驶时刹车失灵, 驾驶者无论用多大力气踩刹车, 都无济于事。

2014 年, 在黑帽子大会上(Black Hat USA2014)[11]上, Miller 和 Valasek 再次公布了一份针对市场上 20 余款车型的信息安全的研究报告, 对不同汽车厂商不同车型抵御恶意攻击的能力进行评估。

2015 年, 被世界公认为“汽车安全元年[11-13]”, 先后发生多起汽车攻击案例, 首先是雪佛兰科尔维特(Stingray)的车辆自诊断系统(OBD)漏洞导致黑客轻松获取该车型的最高权限, 通过手机短信的形式发送修改控制汽车指令。

2015 年, Samy Kamkar 用安吉星(On-Star)攻击了 4 家车企的车联网 APP, 轻而易举的获取到该车联网上的所有用户信息, 从此, 车联网也被列入了黑客攻击的“黑名单[14]”。

2015 年, Miller 和 Valasek 再次演示了“0day”漏洞, 攻击车载娱乐系统, 使用笔记本电脑远程控制一辆“Jeep Cherokee”汽车[11],这些公开的研究报告把车载信息系统的安全问题从边缘推到了前台, 以期望引起汽车制造商以及研究学者对汽车信息安全问题的关注。

2015 年, 美国独立研究机构 Ponemon[15-16]公布了一项关于汽车信息安全的调查报告, 其大胆预计了“未来将有 60%~70%的车辆将因为信息安全漏洞被召回”汽车正逐渐成为网络黑客入侵的热门目标, 汽车受到信息安全攻击的威胁正逐步攀升。而与之相反, 报告中接受调查的对象大部分是来自汽车制造商和其配套供应商的开发人员和管理者, 其中仅有 41%的人承认汽车信息安全的重要性。目前来讲, 汽车信息安全未引起汽车制造商的足够重视。

近年来, 国外品牌汽车制造商设计的车载配套软硬件所拥有的功能也不断延伸, 例如有汽车制造商使用手机 APP 或者蓝牙钥匙来提供门锁控制、手动泊车、调整发动机功率、更新软件等服务, 再加上辅助驾驶和紧急制动程序的出现, 使得此类应用能够通过互联网访问汽车的驱动、控制、底盘等核心系统。一旦这些应用被植入恶性病毒或远程木马被黑客入侵, 则会对行车安全造成致命的威胁。

现代汽车中的控制系统网络化程度对于恶性攻击基本处于不设防状态, 尤其总线(MOST, GigaStar 等)、无线接口(如 GSM、蓝牙)等通信网络的耦合性和公用性逐渐增强, 更引入了额外的安全风险。

Wolf[17]等人提出关于汽车总线安全防护的初步建议:

1) 控制器应对所收到的信息的来源进行验证

2) 数据通信方式引入加密通信技术

3) 网关应提供防火墙机制

基于控制器的数字签名或消息验证实现, 至少应避免低危网络(LIN, MOST)向高危网络(CAN, FlexRay)发送信息; 汽车正常使用时应禁止使用所有诊断接口。从信息安全与密码学的角度而言: 通过对总线上传递的数据进行加密和匿名化处理(Anonymization), 完成对每个 ECU 数据的传送; 通过数字签名校验方式检验故意伪造的数据信息; 底层采用 DOS 编码, 由于总线的广播式通信协议与分优先级处理特性, 通过 DOS 编码 ECU 系统功能对恶意攻击具有一定程度的免疫能力。

Koscher[18]等人在获取了对汽车内部的访问权限之后, 可以实现恶意的攻击效果。他们将实验环境冯特雷场地分为 3 种: 基准型, 即拆卸掉车内单独的硬件, 在实验室中进行测试; 静车型, 将法国品牌标志汽车固定后, 连接 OBD-Ⅱ诊断端口进行实验; 动车型, 即在一条封闭的路段驾驶该汽车, 开始测试杰出的性能, 对这三种实验进行了对比和评估: 尽管现代汽车已经是高度智能化产物, 但是, 机理仍是未被计算机安全界广泛了解和深入研究; 一些重要总线通信协议已经标准化, 可以通过自由桥接, “傻瓜式”的传输信息协议为车内提供大量的无线连接模块, 增强了远程控制能力; 有的车型存在一些弊端, 这为第三方的提供了丰富的开发接口。

Checkoway[19]等人研究的是如何获得对汽车内部网络获取控制权限的问题。他们从信息安全的角度再次刻画了现代机动车安全威胁模型及可能的外部攻击媒介; 并针对每种攻击行为, 发现了不止一种安全隐患, 针对该安全隐患, 提出了相应的机动车制造业的安全措施等。Checkoway 等人将安全威胁模型从宏观上分为: 单组件安全威胁模型、多组件安全威胁模型。单组件安全威胁模型包括的威胁种类有: 侦听数据包并定向探测攻击、模糊攻击、逆向工程攻击; 多组件安全模型包括恶意代码植入攻击、组合仪表显示失灵、CAN 总线。

加入 WTO 以后, 世界各国汽车电子零部件企业开始进入国内, 使得大部分市场份额被国外企业所占据, 我国汽车安全电子产品和国际先进水平相比, 竞争力明显落后, 国内自主品牌汽车行业存在对信息安全重视程度和理解深度还远远不够。相当一部分车企对信息化安全建设的投入长期采用紧缩的策略, 直至出现安全问题时才进行一定的补救措施; 造成上述状况的原因[19-20]: 一是汽车安全电子产品科技含量较高, 跨国汽车电子公司实力强大, 而国内汽车安全电子控制系统缺少相应的技术储备; 二是国内的汽车安全电子产品多由外方供应商提供, 国内自主研发的电子产品进入其配套系统时, 故障率和失误率较高。测试和分析手段较为复杂, 所需设备价格昂贵。目前国内汽车安全电子产业还没有形成完整的专业生产能力, 企业可以生产部分汽车安全电子产品, 但不具备大批量生产的能力, 且汽车信息安全技术的研发及产业化进程在我国尚属于起步阶段, 但国内的几家安全公司已经取得了突破性进展。

专业安全公司奇虎 360[21]拥有很多汽车行业客户, 其中包含国产高端品牌和大众系列汽车。360 公司的安全团队认为的解决方案首先是 IT 技术难题, 包括防火墙(UTM 深度检测防火墙)、VPN 加密技术、防病毒、防间谍软件等等; 其次要确保网络通信系统的安全运行, 尤其是远程访问: 内部员工、合作伙伴、零配件供应商等, 每一个客户群, 应该有不同的访问权限。传统的解决方案是把远程网络和车辆之间传递的信息采用 IPSec 加密技术进行保密通信, 现在更为常用的方式通过 SSL 通道加密手段在部署简单的前提下, 做到深层次的访问控制, 支持更多用户群的接入。

华晨金杯汽车工程师表示[21]: 信息安全问题始终贯穿于汽车产业信息化中, 中国自主品牌汽车企业为保持自有产品和技术的专利知识产权的安全性, 在网络访问控制(NAC)、关键数据加密和防泄露(图档加密和防拷贝、防打印)、关键数据存储备份(如存储备份、异地灾备中心)等方面逐步加强管理力度。

此外, 国内的安全专家在发现车载信息系统漏洞方面, 取得了突破性进展。2014 年, 奇虎 360 车联网安全评估小组[21]首次公开了特斯拉(Tesla Model S)汽车应用程序存在设计漏洞, 该漏洞可以使得黑客远程控制汽车, 包括执行车辆解锁、鸣笛、闪光以及车辆行驶中开启天窗等操作。最近该公司取得了对汽车自动驾驶技术破解方面的突破性进展, 成功的实现了毫米波雷达和超声波雷达的欺骗。因为现在的自动驾驶技术依赖于各种传感器、其中包括毫米波雷达、超声波雷达。自动驾驶汽车是通过雷达来探测障碍物的, 要欺骗雷达可以使障碍物消失, 或者突然造出一个障碍物[22-26]。这样就会造成汽车向障碍物方向行驶。此外, 该团队还与长安汽车合作, 进行车联网的安全评估, 打造了长安汽车电商安全顾问咨询平台, 提供安全顾问咨询服务, 从安全防

护这个角度而言, 传统的车辆体系结构大多是面向功能安全的, 欠缺汽车的信息安全层面的防护, 该安全团队为车企提供相应的咨询建议, 安全设计指导, 包括软件、硬件、固件的升级。设计出安全模型后, 做黑盒、白盒测试, 最典型的就是给车厂做 Tbox、Tsp 的评估, 从整个系统的角度而言, 不仅仅是各个部件的评估, 以及做系统级别的安全评估, 而且还可以为客户制订安全运营的规划。

目前, 车载信息系统的嵌入式系统没有十分成熟的产品, 在软硬件方面的专门的标准还没有出台; 同时, 车载嵌入式计算机系统也必须根据具体硬件资源和现实应用, 选择合适的嵌入式操作系统。操作系统是车载信息系统的灵魂, 现在比较理想的车载嵌入式系统有 WinCE、LINUX 等[27-29], 为此, 国内在车载嵌入式操作系统领域也展开了多项研究工作, 部分汽车企业和科研机构也在推动相关技术发展, 中国第一汽车集团公司、东方汽车公司, 以及清华大学、吉林大学、交通部公路科学研究所等多家科院院所对车载嵌入式操作系统性能要求的不断提高, 汽车企业及配套企业观念的转变, 车载信息系统技术领域也取得快速发展, 越来越多的汽车智能化信息安全系统必将成为车辆的标准配置, 具有较好的市场前景。

3 汽车攻击关键技术分类

汽车行业进入信息化时代后, 汽车产品逐步向智能化、网络化方向发展。已经由集中式的手工控制向分布式的电子自动控制转变, 车内上百个电子控制单元(ECU)通过总线传递信息的方式相互连接, 经由千万行的程序代码进行驱动, 构成了高效复杂的网络化系统。另外, 无线通信模块的普及, 尤其是车载信息系统的引入, 对汽车信息安全提出了全新的挑战。黑客有可能通过远程无线入侵的方式, 攻击车载信息系统的现有漏洞, 进而利用现代汽车丰富电气化、网络化功能, 达到车内信息窃取、驱动系统失灵、制动系统远程操控等目的[30-31]。

由此可见, 汽车已经成为了一个装有大规模软硬件的高度集成化的信息系统。车载信息系统在提高信息化水平同时, 信息安全问题也日益突出。车辆遭受黑客攻击的途径也日益翻新, ECU 木马和病毒变体数量不断攀升, 威胁驾驶人员生命财产的行车安全隐患刻不容缓。

3.1 车载信息系统遭受攻击的途径

车载信息系统中存在信息安全脆弱的一面, 车载软件系统受到黑客攻击的可能性越来越大。原因是汽车的外部接口数量和类型不断增多, 除了车载诊断系统OBD接口和USB充电接口外, 现在汽车上还可以通过 GPS、WIFI、蓝牙接口与卫星、智能手机、平板电脑等外接设备相互连接[32]。而在接入上述外接设备时, 黑客植入在该设备的恶性病毒和远程木马也随之侵入到了车载信息系统内部, 为黑客攻击该车辆提供了便捷的途径。

3.1.1 智能手机攻击途径

智能手机是汽车用户经常使用的网络通信工具, 与传统手机最大的差别是, 智能手机上的应用程序可以自由发布、下载并安装, 而且种类繁多, 其中包含大量面向汽车的应用软件, 而这些软件可能存在可靠性低、安全性差等特点, 黑客通过其中的漏洞、通过智能手机, 使得车载信息系统、导航系统出现异常, 或是窃听用户的谈话记录及驾驶员个人隐私信息等[32]。用户在使用智能手机同时, 就意味着整部汽车与外界网络相连。因此, 黑客通过外界网络破解智能手机, 目的是干扰车载信息系统, 对正在高速行驶下的车辆发起恶性攻击。

3.1.2 车联网远程攻击

车联网等外围通用系统针对汽车基本控制功能在逐渐增加。例如, 汽车制造商使用通用的信息终端来控制中控门锁系统、调整发动机功率、更新应用程序等服务。而这些功能也成为攻击的目标, 信息终端一旦被成功入侵, 对车辆和驾驶人员造成严重的人身安全威胁。为了确保通用性, 大多数车载信息系统都采用同种类型的底层操作系统, 用户通过该底层操作系统, 使用各项服务也越加方便, 但攻击操作系统的难度变得越来越低。除了底层操作系统外, 车联网等外围通用系统的通信协议也在逐渐提高, 德国政府支持的“基于 IP 协议的安全嵌入式系统(SEIS)”项目[33], 该项目计划让车联网采用 Ethernet 网络协议, 并在 TCP/IP 协议基础上开发新的通信通用模块。2008 年, 德国宝马汽车有限公司首先采用 Ethernet 网络接口, 作为 OBD 协议接口, 用于安装车载应用软件[34]。车联网的通信方式虽然在电路层实现了标准化, 但请求指令、响应机制上存在差异, 造成了实际应用中的“门槛”。但从车辆信息安全的角度而言, 该“门槛”其实是一道“防火墙”[13]。目前, 已经出现了采用无线通信协议 WIFI、蓝牙等车联网通信协议适配器。随着车联网采用的互联标准越来越多, 车内外的众多设备和车载信息系统与汽车紧密相连[35]。车联网接入变得越来越简单, 黑客突破这道“防火墙”也相对变得容易。

3.1.3 移动互联网远程攻击

移动互联网远程攻击汽车成为最新黑客和安全

专家共同研究的目标, 攻击者为实现远程跨网攻击, 利用逆向工程技术, 通过解析移动互联网通信及信息终端, 开发出了针对特定品牌、车型的入侵代码和可执行代码[36-38]。在这种情况下, 倘若有人开发出了攻击移动互联网通信及信息服务代码, 并将其散布, 有可能造成更严重的危害[38]。

3.2 车载信息系统遭受攻击的种类

汽车信息安全产生威胁的原因分为两类: 驾驶者偶然发生的失误; 攻击者故意引发的失误。按照不同发生原因, 相应的威胁种类如表 2 和表 3[39]:

表 2 驾驶者偶然发生的失误

威胁类型	说明
设置错误	驾驶者通过车内应用接口, 执行错误的驾驶操作指令
感染病毒	驾驶者通过从外部带入的存储设备, 车载系统感染病毒和恶意软件

表 3 攻击者故意引发的失误

威胁类型	说明
非法利用	黑客通过伪装身份、篡改标识等, 攻击车内软件产品漏洞, 达到完成某种汽车系统功能
非法设置	攻击者通过权限升级、指令破解等, 非法变更汽车系统设置数据
信息泄露	车载信息系统, 应当受保护的信息落入非法人员手中
窃听	车载设备之间的通信、汽车与周边系统通信、车内人员的谈话记录遭到窃听
窃照	车内放置的文件、私人物品遭到监视器或针孔相机窃拍
Dos 攻击	由于车载信息系统底层操作系统采用 Dos 版本, 通过非法连接请求, 造成系统瘫痪、服务受阻
虚假消息	攻击者通过 GPS 导航系统, 发送伪造的 GPS 导航信号, 诱导驾驶者行驶线路发生偏移
记录丢失	删除和篡改操作记录等, 使驾驶者无法查看
非法传播	通过破解通信信道, 劫获常规数据, 夹杂非法信息

3.2.1 物理接触攻击

汽车由于自身的可移动性, 有别于计算机, 驾驶者很难始终监视车辆, 而黑客及其容易接触到汽车。而且, 在进行日常维护保养时, 汽车必须交由厂家和车主以外的第三方维修人员管理, 有可能受到装扮成第三方维修人员黑客的攻击[40]。另外, 用户在自行改装车辆时, 有可能将汽车本身自带的安全装置无意识地拆除掉[41]。

3.2.2 便携式设备攻击

除了汽车本身具有的功能之外, 汽配市场等途径购买并安装在车上的产品也种类繁多。驾驶者在购买和安装该产品时, 有可能带来外部病毒入侵式的攻击。尤其是智能手机、平板电脑、PDA、GPS 卫星导航系统[41-43], 一方面, 这些便携式设备很容易获得面向汽车接口的通用应用市场, 受到广大用户的好评; 另一方面, 该便携设备也掺杂着大量仿制、山寨产品和恶意代码应用程序等[44]。汽车制造商在车辆开发设计时, 必须考虑到用户带入车内的任何便携式设备所带来的恶性攻击威胁。

3.2.3 无线网络攻击

为了防止物理攻击, 汽车有很多通过无线网络完成的功能, 例如智能钥匙、轮胎压力检测系统、路车间通信等装置都使用短距离无线通信方式, 这为黑客空口截取信息内容, 打开了方便之门[45]。此外, 智能手机与车载信息系统之间的交互应用也越来越普及, 如今车联网“井喷式”的发展, 加上汽车连接外部网络的环境日益完善。车载信息服务也开始普及, 利用车联网对汽车发起木马和病毒的入侵攻击和情报窃取已成为现实[46]。

3.2.4 总线 CAN、MOST、LIN 攻击

汽车中大量控制器的网络化程度飞速发展, 使得外部网络可以访问汽车关键部件(如引擎、刹车、气囊等), 而控制信息通过总线系统进行各部件之间的信息传递, 而总线系统对于恶意攻击基本处于不设防状态, 尤其是负责多媒体通信的 MOST 总线、负责传递控制信息的 CAN 总线, 以及负责中控门锁系统的 LIN 总线[47-49], 它们与无线网络接口的耦合性逐渐增强, 加上所有控制器间的通信都是明文传送(非加密状态); 大部分总线传递消息的编码方式和通信协议都是公开的, 控制器也没有相应的检测程序, 来验证抵达的信息是否是合法的控制信息[50]。

理论上讲, 任何 CAN、MOST、LIN 总线上的控制器都可以向其他任何控制器发送指令[51-54], 因此, 任何遭受到总线攻击的控制器, 都会对整车通信网络构成实质性的威胁。例如, 多媒体总线 MOST,D2B 等与外部接口和互联网相连使得恶意软件(远程木马、恶性病毒)可能通过光盘、MP3、电子邮件等方式侵入车内核心系统。虽然车内部分网关提供了简单的防火墙机制, 但与此同时, MOST 和 D2B 总线也提供了强大的, 不设防诊断接口, 从而使得攻击者轻而易举的攻破整车网络。表 4 列出了车内所有总线及其遭受攻击时的风险指数[55]。

对于汽车总线系统破解的防护, 目前仍然停留在对控制器所接收到信息的源地址、目的地址验证, 传递信息所用信道加密, 网关防火墙加密措施阶段, 上述措施无法避免低危网络向高危网络发送信息, 只能采取汽车正常启动时, 关闭所有接口等防护措施, 迫使驾驶者体验度大打折扣。

表 4 总线遭受攻击风险度分析

总线名称	风险评估	隐患
LIN 总线	风险低	①利用从节点对主节点依赖关系, 制造单节点失效; ②由于 LIN 总线具有同步功能, 造成 LIN 总线无法正常工作
CAN 总线	风险高	①阻断高优先级正常帧的传输; ②伪造错误信号帧, 使控制器与 CAN 总线终端通信
FlexRay 总线	风险极高	①隐与 CAN 相同; ②另外, 攻击者可以通过制造休眠信号帧使控制器休眠
MOST 总线	风险低	①通过 MOST 时间源特性, 干扰信号同步; ②伪造信道请求信息, 消耗带宽
蓝牙	风险可变	①无线通信网络传输的风险隐患, 蓝牙接口都存在; ②所有消息都以广播、易侦听方式进行

3.3 ECU 电控系统攻击

ECU 电子控制单元(Electronic Control Unit,ECU)又称行车电脑[56], 其早期的作用是获取汽车上各种传感器数据, 进行运算处理, 从而做出判断性指令, 向发动机、喷油器、刹车制动系统及时发出调整指令, 使得行驶中的车辆保持良好的运行状态, ECU 和普通计算机一样, 也是由微处理器、存储器、输入输出接口、模数转换器, 以及驱动设备等大型集成电路组成。图 2 为 ECU 电子控制单元组成架构[35]:

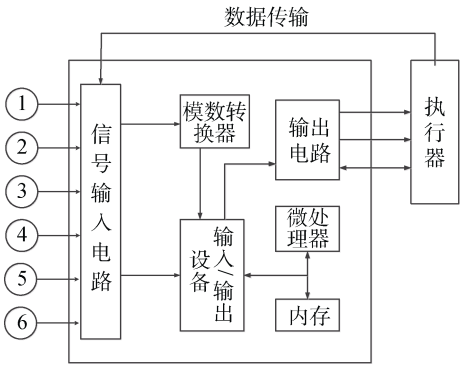


图 2 ECU 组成架构

在汽车 ECU 设计之初, 首先追求的是工控系统的反应速度以及处理能力, 在 ECU 的内部设计者并没有划分任何层次和权限, 尤其是汽车内部, 每一个 ECU 通过 CAN 总线采用多级互联的方式相互通信, 显著地提升了处理效率和稳定性, 但也意味着从任何一个接口都可以获得整部汽车的控制权[58]。如今, 市场上高端车型的 ECU 都具备学习功能, 会记录汽车行驶过程中的数据, 除了在发动机上得以广泛应用之外, ABS 防抱死系统、四轮驱动系统、变速器系统、主动悬挂系统、液压控制系统等, 都通过 ECU 进行控制, 这就使得 ECU 掌握的信息越来越多, 攻击者通过分布式 ECU 来控制汽车的多个系统, 正是因为每一个 ECU 与 CAN 总线相连, 在 CAN 网络里, 从发动机 ECU 到安全气囊 ECU, 这些 ECU 控制系统是同级别关系, 攻击者破解了 CAN 总线系统, 所有的控制系统的 ECU 都面临较大的安全风险。针对 ECU 攻击的手段有[59]:

1) ECU 数据包侵入式攻击

不同的 ECU 通过 CAN 标准连接成一个总线型结构网络, 在该网络环境下, ECU 采用组播的方式发送数据包, 由于 CAN 网络是个高度可信的网络, 在汽车设计之初就没有考虑到 CAN 网络数据包标识的问题, 每个数据包只有简单的 ECU 发出标识, 攻击者通过 CAN 上发送特定内容的数据包使得整个网络产生动作, 相应的 ECU 传感器和执行器会响应该动作指令, 达到攻击者控制汽车的目的[60]。

2) ECU 数据包篡改式攻击

CAN 网络发包时, 具有组播特性, 攻击者可以修改其数据包内容, 再重新发送, 用以欺骗汽车工控系统使其做出错误的指令动作。每个数据包都有自己的 ID, 数据包 ID 代表它是由某个具体的 ECU 发出来的, ISO14229 电气工业标准中规定了数据包 ID 和 ECU 对应关系[61], 通过修改数据包 ID, 将错误的指令发送到指定的 ECU 上, 可以达到汽车刹车、抱死、猛打方向等操作, 还可以通过篡改数据包内容, 使得汽车转速表上对应的参数信息显示有误, 更有甚者, 通过修改中控解锁 ECU 发出的数据包信息, 使得行驶中的车辆强行解锁[62]。

3) ECU 数据包重放式攻击

通过 OBD 接口可以访问 CAN 网络中的所有总线结构, 理论上可以将 OBD 转接头, 直接连接到汽车 OBD 接口处, 实时进行攻击[63]。国外研究机构已经可以通过无线网络直接启动 OBD 盒子的驱动程序, 通过非物理接触的方式, 对发动机 ECU 进行持续性攻击, 如图 3 所示, OBD 无线网络连接终端:

图 3 OBD 无线网络连接终端

4) ECU 恶意代码植入

国内外多大数的 4S 店都支持 ECU 升级服务, 其目的是为了提高发动机涡轮增压、提升扭矩以降低油耗。原理是[63-64]: 通过重写 ECU 程序中的相关代码, 实现供油点火曲线精细调整, 优化 ECU 中相关参数信息。这其实是对 ECU 源代码进行重新烧录, 攻击者可以利用这一点, 伪装成为 4S 店的工作人员, 对目标车辆 ECU 重写包含恶意代码的程序, 这种方式可以有效的将恶意代码隐藏在常规代码中, 使得车检人员和驾驶者很难发现。等到时机成熟时, 自动触发[65]。例如, 安全气囊无法正常打开, 车辆超过某个时速时, 刹车/制动系统失灵等, 这也被称作汽车“病毒”的植入。

5) ECU 虚假信息干扰

大多数汽车都安装 GPS 导航系统, 尤其是高档汽车出厂时, 在行车电脑中嵌入 GPS 芯片, 方便汽车厂商为驾驶者提供定位服务, 黑客可以利用“伪基站”的方式, 跟踪目标车辆, 当目标车辆开启智能导航模式后, 黑客通过干扰目标车辆 GPS 芯片所在的 ECU 发起攻击[66]: 向 GPS 芯片发送一条伪造的路线信息, 系统提示该路线为到达目的地最优路线(时间最短, 路途最近, 避堵等), 驾驶员按照系统提示信息, 进入预先设置好的路线, 攻击者对目标车辆伺机进行破坏活动。

3.4 车辆行车信息感知系统攻击

车辆行车信息感知与处理系统是自动驾驶、自动巡航技术的核心组成部分, 实时地对车辆运行数据进行采集、检测, 并通过必要的信号处理获得准确、可靠的行车记录信息。其中, 车间距离及相对车速测量传感器是该系统特有功能[67]。国外行车信息感知及处理系统的研究集中于车间距离测量传感器的研制和信号测量处理方面。而它们也是自动驾驶技术和自动巡航系统的理论依据。因此, 车辆信息感知系统探测技术主要包括[68]: 探测距离范围要求、探测角度范围要求、探测精度要求及温度适用范围、抗震、抗干扰等方面。参数分析依据是[69]: 道路交通规则、道路交通实际情况、车辆设计规范及实际使用环境等特点。

按照探测介质不同, 车辆信息感知系统探测技术分为微波雷达探测和激光雷达探测两种[69]: 微波雷达探测的优点是运行可靠, 测量性不受天气等外界因素的影响, 缺点是结构复杂, 成本较高; 激光雷达探测技术主要优点在于结构简单, 测量精度较高, 价格便宜, 缺点是测量性能易受环境因素干扰, 在雨、雪、雾霾等天气情况下测量性能会有所下降。

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, 首先雷达发出电磁波被前方物体遮挡, 产生反射现象, 车内雷达接收装置接收到反射波, 车载中控系统根据光速和电磁波传输时间的一半, 计算出汽车与障碍物之间的距离, 车载中控系统根据自身的车速, 调整行驶路线。

此外, 攻击者通过吸收雷达电磁波形式对自动驾驶和自动导航系统发起攻击, 针对车载雷达探测系统能探测到的物体进行隐藏, 使得雷达电磁波“有来无回”, 被攻击车辆通过车载中控系统综合参数判定, 车辆行驶路线前方并无障碍物, 继续按照原先设定的路线行驶, 直到与障碍物发生碰撞为止。

自动驾驶和自动巡航系统主要依赖于行车信息采集系统将获得的车辆状态及行车环境信息传递给车载中控系统。车载中控系统综合利用各种信息, 对车辆安全状态做出评估。只要攻击者修改其中一个环节的数据, 使得在中控系统对前方的行车路线的安全性做出错误的判断, 从而制造车毁人亡的事故。

4 汽车防护关键技术措施

汽车防护技术主要分为三大类:汽车主动防护技术、汽车被动防护技术、车辆及零部件信息安全防护技术:

1) 汽车主动防护技术包括: 汽车电子稳定性控制技术、智能安全辅助技术以及人车安全状态监控与感知技术等。

2) 汽车被动防护技术包括: 车载防护自动通知技术、成员安全保护技术、中央门锁检测技术等。

3) 车辆及零部件信息安全防护技术包括: 动力学控制传感器数据识别技术、零部件程序代码信息校验技术、零部件安全“写保护”机制、数据信息传送校验机制、数据信息容错防护机制、重要数据和程序设有“加密”功能等。

4.1 汽车主动防护技术

1) EyeCar 技术

EyeCar[70]技术可以使得每一位驾驶员的眼睛处于同一相对高度水平面上, 确保提供一个完整的路面和周围车道无阻碍视野, 眼位传感器可以测试出驾驶员的位置, 然后据此确定、调节座椅的位置, 为驾驶员提供能够掌握路面情况的最佳视线, EyeCar 技术还可以重新布置 B 立柱, 可以减少驾驶员视野中的“盲区”。EyeCar 技术通过使用电动座椅自动将不同身材驾驶员的眼睛调整到统一高度来解决视见度的问题, 同时对方向盘、制动与加速踏板、中央控制台进行调整, 以构造自适应的驾驶环境, 从而避

免了黑客利用驾驶员“盲区”对车辆进行物理攻击的企图。

2) CamCar 技术

CamCar[71]技术可以帮助驾驶者提高对周围环境的认知能力, 多台摄像机和可切换视角显示器扩展了驾驶员的视野, 可以使得驾驶者能够绕过大型车辆同时观察到隐蔽处的行人和车辆, 提前做出预判。侧置后视摄像头弥补了后视镜反射面的不足, 特别是临近车道。扇形排布的 4 台微型摄像机可以有效的增加后视视角, 图像经过电子合成后传回可切换显示器, 并且摄像机可在低照明环境下提供红外线摄像功能, 彻底消除前照灯及其他光源所带来的眩目问题。这些技术相互结合为驾驶者提供一个全车及周围环境的鸟瞰图, 有效的对接近车辆的人和物体进行实时监控。

3) SensorCar 技术

SensorCar[72]技术是专门为汽车碰撞事故研发的碰撞预警系统, 其目的是减少追撞和伤害行人风险。首先, 安装在后保险杠中监测后面车流情况的传感器和计算机通过无线通信模块相连, 从传感器采集上来的数据经过计算机程序分析确定有无撞车的可能; 其次, 激光雷达装置监测车前是否有行人经过, 如监测到有物体进入两个激光雷达组成的扇形区域, 仪表盘上的警示灯和扬声器同时发出报警信号, 提醒驾驶员, 注意减速和避让。再次, 马上发生碰撞后, 安全带电子预紧器, 自动拉紧安全带, 最大限度地保障了乘客生命安全。

4.2 汽车被动安全技术

1) RescueCar 技术

车辆被攻击后, 能够及时通知有关部门, 将 RescueCar[73]技术可以防止黑客对车辆进行恶意攻击造成的碰撞或侧翻事故, 该技术可以在遭受攻击后 1 分钟之内, 由车载防护自动通知系统向有关部门发出报告, 报告汽车基于全球卫星定位(GPS)数据的准确位置。车辆救援人员在抵达事故现场之前就可以充分了解有关车辆的实时状况: 乘员数量、乘座位置、安全带使用情况和气囊展开情况、汽车的姿态, 是侧翻还是倾覆等信息, 从而制定出相应的救援措施。RescueCar 的事故分析和通信机制可以帮助设计师设计出更符合现代安全理念的汽车, 它是从多种受攻击车辆中自动收集重要信息, 因此也能帮助研究人员迅速建立一个车辆攻击信息数据库。

2) SecurCar 技术

SecurCar[74]技术能够保证: 即使车辆在静止状态, 也新增了很多安全防护措施。它可以防止驾驶者疏忽大意将重要物品, 例如, 文件、手机、枪械等锁在车内, 并为锁在行李箱中的成人或儿童提供逃离安全设施, 还能检测出车内是有潜在的非法入侵者, 原因是: SecurCar 技术通过一个可以测出车内是否有无线电磁波外泄的传感器, 如果中控门锁系统锁定后, 仍有车内仍能发射电磁波, 报警装置发出声音。如果有入侵者藏在汽车行李箱中, SecurCar 技术的心跳传感器, 可以敏锐的发现该入侵者的心率, 组合仪表中的入侵检测提醒装置发出报警。

3) SeccuriLock 技术

SeccuriLock[75]是一种可以阻止黑客破解中央门锁系统的防盗钥匙系统。钥匙芯片上嵌入一套电子通信系统, 如果这套电子通信系统检测出该钥匙不是该车专门授权钥匙, 将禁止该车发动机启动。

4.3 车辆及零部件信息安全防护技术

1) 数据识别技术

当用汽车钥匙、电子遥控钥匙或其它手段开启汽车时, 是把本车型和该辆汽车的关键参数[76]: 汽车发动机型号、汽车车架号、汽车的批次、出厂日期等, 通过无线信息发送给车载信息系统, 车载信息系统接收到这些关键参数时, 要自动识别这些关键参数是否正确, 如识别不是本车型的汽车钥匙、电子遥控钥匙或其他手段开启本汽车时, 汽车内的信息控制系统就会自动识别或者自动关闭这些数据参数, 汽车信息控制系统就停止相应功能。

2) 程序代码信息校验技术

汽车中的电子控制系统和零部件系统, 在汽车启动时, 都要进行相应的数据信息或程序代码校验工作, 以防止被黑客或不法分子恶意篡改。校验的方法包括[77]: 奇偶校验法、按位与校验法、CRC(循环冗余码校验)等校验法。如果检测出重要程序或数据被恶意篡改或破坏, 组合仪表中的报警装置, 发出警示信息, 引起驾驶者高度重视, 并采取紧急措施。

3) 安全“写保护”机制

汽车是机械与电气信息系统的相互融合产业, 控制指令、程序代码、数据流、信息流等彼此在工作时, 受到机械部件的点火(发动)、震动、噪声、磁场等因素的干扰, 信号容易发生故障、失效等情况。电子信息系统之间在传递信息时, 应采取“写保护”机制[78]: “防擦”、“防写”、“防飞”等信息安全防护措施, 避免由于其他信号干扰而造成的数据信息传输错误。

4) 数据信息传送校验机制

电子信息系统在传送控制命令、数据内容、重要参数时, 可以采用多数表决法、向前纠错法、

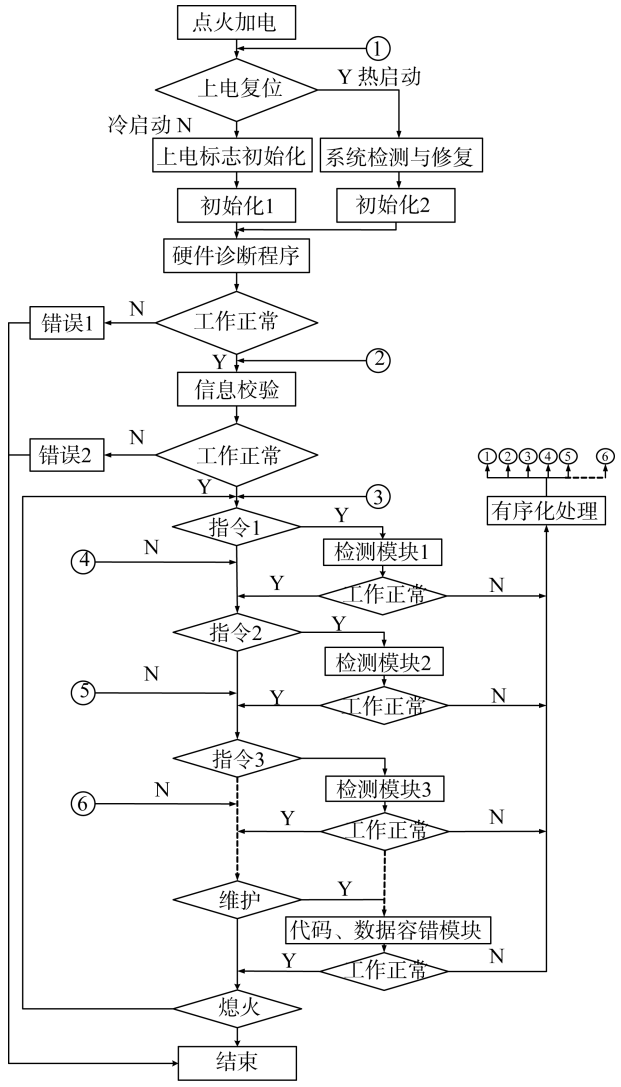


图 4　信息系统及零部件安全检测主要流程图

ARQ(自动请求重发)方法, 接收数据时, 一旦发生错误, 通知发送方重新发送, 直到正确为止。车企和主机厂根据数据格式和网络通信协议选择校验的方法和机制。

5) 数据信息容错防护机制

未来汽车是电子产业和机械产业高度融合的产物, 设计和编辑控制系统和电子信息系统时, 应该充分考虑到容错防护机制和异常处理措施。防止数据内容和程序代码在运行时, 出现的“死机”和“假死机”等现象。

6) 重要数据和程序设有“加密”功能

当汽车发动时, 电子信息系统将加密后的控制指令通过总线发送到各个电子零部件系统和可执行单元中, 各零部件系统和电子控制单元接收到该指令后, 根据各系统之前分配好的秘钥, 进行相应的解密操作, 自动解开本系统的数据内容和程序代码。因此, 可以防止部分指令信息在传递过程中, 被黑客截获, 并进行相应的破解, 嵌入恶性木马和病毒[79]。当然加密算法和加密函数、解密算法和解密函数, 可以通过汽车制造、车联网或其他无线手段等, 来装入、更新、修改和传输。

该六项防护措施可以单独独立操作, 彼此之间高耦合, 低内聚。汽车制造商可以根据实际情况, 进行任意三个以上的组合, 保证数据传输时的安全性和准确性。图 4 为电子信息系统和汽车零部件之间信息安全检测的主要流程。

5　现代汽车功能安全与信息安全的关系

安全是未来汽车面向人性化设计的重要内容和关键问题, 不仅在汽车辅助和动力驱动领域, 新添加的功能也在逐渐触及汽车安全领域的技术。这些功能的开发和集成, 将强化对安全相关系统的开发需求, 并且要求车企和汽车销售代理商提供满足所有合理的系统安全目标认证。与此同时, 将大幅度提高汽车零部件现有技术标准和功能安全等级。即便如此, 也不代表汽车是绝对信息安全的。功能安全是适用于道路车辆上特定的由电子、电气和软件组成的安全相关系统在安全生命周期内的所有活动[78]。信息安全是指汽车无论在静态和动态的环境下, 存储在汽车电子/电气系统或控制器内的数据参数、命令格式、通讯协议、程序代码等信息要有安全防护措施。重要数据信息要防止被篡改、被窃取、拷贝、解剖、仿制等[79]; 在车辆上电或下电、数据信息传输和传递时, 要有防干扰和防差错等方法和措施[80]。汽车功能安全与信息安全是两个科研范畴和研究领域, 但它们可以相互衬托、相互依赖、相互弥补各自不足。

6　汽车信息安全展望

汽车信息安全技术是当前国际汽车高新技术发展的主题之一, 它集成了计算机、现代传感器、信息融合、通信、人工智能及自动控制等技术, 是今后汽车安全领域发展的一个主流研究方向。研制先进车载信息安全系统是高效安全交通运输的基础和保障, 同时也是人民生命财产保证的必要选择。随着汽车保有量的迅速增加、交通运输系统日趋复杂、国际恐怖活动逐渐加剧, 在国家安全、社会经济安全方面对汽车安全提出了更高的现实要求, 现代汽车的安全电子控制技术已明显向集成化、智能化和网络化三个方向发展, 通过采用分布式控制系统为基础的汽车车载电子网络系统、嵌入式系统、局域网控制和数据总线技术, 可实现汽车信息安全电子控制系

统的综合协调控制。

本文概述了汽车功能安全与信息安全的定义和研究现状, 对车辆攻击技术和防护技术进行了详细的归纳与分类, 分析了针对汽车常见的攻击手段和潜在安全威胁, 并针对每一种安全威胁总结了相应的汽车防护措施。综述了汽车信息安全领域的国内外最新进展情况。汽车信息安全电子研究及产业化正处于起步阶段, 与国际汽车安全电子行业还存在较大差距。可以通过制定相关的行业标准、鼓励自主研发、加强企业合作、搭建信息共享平台和培养专业人才等方面入手, 加快我国汽车信息安全电子产业的快速发展, 逐步积累研究成果和研究经验, 形成自身的竞争优势, 从而提高我国汽车工业的国际竞争力和安全保障性, 同时具有广阔的商业前景和发展潜力。

参考文献

[1] “2017-2021 年中国汽车电子行业投资规划及前景分析报告,” 百度文库, http://wenku.baidu.com. 2016.

[2] Y. Wang, W. Zhang and S. Wu, “In-Vehicle Information System and Driving Safety”, *Review Science & Technology*, 2012.27（13）: 105-110.
(王颖, 张伟, 吴甦, “车载信息系统与驾驶安全研究综述”, *科技导报*, 2012, 49(11): 2450-2463。)

[3] Y. Lien, “Study of theoretical and practical aspects of transition systems [Ph.D.dissertation],” University of California, Berkley, 1972.

[4] H. Gao, “The Research and Implementation of In-Vehicle Information System Sharing Platform and Safety Mechanism [Ph.D.dissertation]”, Zhe Jiang University, Hangzhou, 2015.

[5] L. Yin, L. Wu, Q.Z. Lu and T. Zhu, “Research on relationship between in-vehicle information system and driving safety based on scanning features ”, *China Safety Science Journal*, 25(6): 124-128, 2015.
(殷莉, 吴玲, 路巧珍, 朱彤, “基于扫视特征的车载信息系统与驾驶安全关系研究”, *中国安全科学学报*, 2015, 25(6): 124-128, 2015.)

[6] S. Benedetto, M. Pedrotti and L. Minin, “Driver workload and eye blink duration”, Transportation Research Part F: Traffic Psychology and Behaviou,14(03): 199-208, 2011.

[7] N.G. Masao, “The Perspectives of Reserach for Enhancing Active Safety Based on Advanced Control Technology”, Automotive Safety and Energy, 1(1): 14-20, 2010.

[8] A.I. King, “A Suggestion for making rapid advances in automotive safety in China”, Automotive Safety and Energy, 1(1): 14-20, 2010.

[9] L.W. Chen, K.Z. Syue and Y.C. Tseng, “A vehicular surveillance and sensing system for car security and tracking applications”, in Proc. *the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks(IPSN, 2010)*, pp. 426-427, 2010.

[10] W.B. Li and X.N. Wang, “Designing of detecting and measurement system for car security based on supersonic principle”, *Advanced Materials Research*, 2011, vol. 179-180, pp.1346-1349.

[11] A. Bouard, M. Graf and B. Burgkhardt, “Middleware-based security and privacy for in-car integration of third-party applications”, 401:17-32,2013.

[12] I. Symeonidis, M. Mustafa and B. Preneel, “Keyless car sharing system: A security and privacy analysis”, *in Proc. IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life* (ISC2 2016), 2016.

[13] T. Becsi, S. Aradi and P. Gaspar, “Security issues and vulnerabilities in connected car systems”, in Proc. *2015 International Conference on Models and Technologies for Intelligent Transportation Systems(MT-ITS 2015)*, pp. 477-482, 2015.

[14] J. Pacheco, S. Satam, S. Hariri, C. Grijalva and H. Berkenbrock, “IoT Security Development Framework for building trustworthy Smart car services”, *in Proc. IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data(ISI 2016)*, pp.237-242, 2016.

[15] H. Stubing and A. Jaeger, “Secure beamforming for weather hazard warning application in Car-to-X communication”, *Lecture Notes in Electrical Engineering*, 78: 187-206,2010.

[16] S. Hameed, O. Khalifa and M. Ershad, “Car Monitoring, alerting and tracking model, enhancement with mobility and database facilities”, in Proc. *International Conference on Computer and Communication Engineering (ICCCE'10)*, 2010.

[17] F. Wolf, “Will vehicles go the mobile way?: Merits and challenges arising by car-apps”, i*n Proc. the 10th International Conference on Informatics in Control, Automation and Robotics(ICINCO 2013)*, pp.425-428, 2013.

[18] K. Koscher, A. Czeskis, F. Roesner, and S. Patel., “Experimental security analysis of a modern automobile”, *in Proc. IEEE Symposium on Security and Privacy(SP 2010)*, pp. 447-462, 2010.

[19] L. Li, J. Song and X.L. Qin, “Investigation and development of vehicle dynamics stability control system”, *Trans Chinese Soc for Agricultural Machinery*, 37(2): 141-144,2006.
(李亮, 宋健, 祁雪乐, “汽车动力学稳定性控制系统研究现状及发展趋势”, *农业机械学报*, 2006, 37(2), pp.141-144.)

[20] A. Mutter, “Robustness of a CAN FD Bus System- bout Oscillator Tolerance and Edge Deviations”, *in Proc.the 14th international CAN Conference(ICAN 2013)*,2013.

[21] “360 安全响应中心,” 奇虎 360, http://security.360.cn/.

[22] T.P. Chang, K.L. Hung, H.T. Chou, “A K-band FMCW radar with the receiving antenna diversity in the car detection applications”, in Proc. *2015 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC 2015)*, pp.169-172, 2015.

[23] J. Dickmann, J. Klappstein, M. Hahn and M. Mutziger at el., “Present research activities and future requirements on automotive radar from a car manufacturer's point of view”, *2015 IEEE MTT-S International Conference on Microwaves for Intelligent Mobility (ICMIM 2015)*, 2015.

[24] S. Zhao, L. Chen, “Research on the single target recognition of car collision avoidance radar based on the FMCW technology”, *Advanced Materials Research*, 2014.

[25] S. Zhao, L, Chen, “Research on target recognition of the millimeter

wave car collision avoidance radar based on the LFMCW", *Advanced Materials Research*, 2014, 1056(2014):244-247, 2014.

[26] J. Dickmann, N. Appenrodt, C. Brenk, "Making Bertha: Radar is the key to Mercedes-Benz's robotic car", *IEEE Spectrum*, 2014, 51(8): 44-49, 2014.

[27] M. Sonneberg, K. Kuhne, M. Breitner. "A decison support system for the optimization of electric car sharing stations", *2015 International Conference on Information Systems: Exploring the Information Frontier(ICIS 2015)*, 2015.

[28] A. Vagner, "Intelligent route planning system for car drivers in a city", *6th IEEE Conference on Cognitive Infocommunications (CogInfoCom 2015)*, pp.551-555, 2015.

[29] T. Sawada, "Car navigation system with enhanced connecting funciton", *Fujitsu Scientific and Technical Journal*, 2015, 51(4), 2015.

[30] K. Daniel, L. Erich, P. Thomas and L. Marus, "Replacement of the Controller Area Network (CAN) protocol for future automotive bus system solutions by substitution via optical networks", *in Proc. International Conference on Transparent Optical Networks (ICTON 2016)*, pp.7550335, 2016.

[31] M. Wolf, A. Weimerskirch and C. Paar, "Security in automotive bus systems", in Proc. *The Workshop on Embedded Security in Cars (ESC 2004)*, pp.1-13, 2004.

[32] M. Wolf, A. Weimerskirch and T. Wollinger, "State of the art: Embedding security in vehicles", *EURSIP Journal on Embedded Systems*, 16(1), 2007.

[33] "Open Thyself!-Security vulnerablilities in BMW's Connected Drive", S.D.Beemer, *http://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html. Feb*. 2015.

[34] T. Hopper, S. Kiltz and A. Lang, "Exemplary Automotive Attack Scenarios: Trojan horses for Electronic Throttle Control System (ETC) and replay attacks on the power window system", *VDI BERICHTE 2016*, pp. 165-183, 2007.

[35] K. Koscher, A. Czeskis and F. Roesner, "Experimental Security Analysis of a Modern Automobile", *in Proc. of the 31st IEEE Symposium on Security and Privacy (IESSP)*, pp.447-462, 2010

[36] S. Checkoway, D. McCoy and B.Kantor, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", *in Proc. The 20th USENLX conferece on Security*, pp.6-6, 2011.

[37] R.M.1. Roufa, H. Mustafaa and T. Taylora, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study" *in Proc. the 19th USENIX Security Symposim (USENXSS 2010)*, pp.11-13, 2010.

[38] R. Wang and S.Y. Yang, "The design of a rapid prototype platform from ARM based embeded system", *Consumer Electronics, IEEE Transaction* on, 50(2):746-751, 2004.

[39] K. Koscher, A. Czeskis and F. Roesner, "Experimental security analysis of a modern automobile", *in Proc. Security and privacy 2010 IEEE Symposium (SPS2010)*, pp.447-462, 2010.

[40] S. Woo, H.J. Jo and D.H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN", *Intelligent Transportation Systems, IEEE Transactions* on, 16(2): 993-1006, 2015.

[41] N.O. Tippenhauer, C. Popper and K.B. Rasmussen, "On the requirements for successful GPS spoofing attacks", *in Proc. Of the 18th ACM conference on Computer and communications security (CCS 2011)*, pp. 75-86, 2011.

[42] P. Kleberger, T. Olovsson and E. Jonsson, "Security aspects of the in-vehicle network in the connected car", *in Proc. Intelligent Vehicles Symposium (IVS 2011)*, pp.528-533, 2011.

[43] K. Han, S.P. Divya and K.G. Shin, "On authentication in a connected vehicle: secure integration of mobile devices with vehicular networks", *Cyber-Physical Systems 2013 ACM/IEEE International Conference on(ICCPS 2013)*, pp. 160-169, 2013.

[44] T. Yang, L. Kong and W. Xin, "Resisting relay attacks on vehicular passive keyless entry and start systems", *in Proc. Fuzzy Systems and Knowledge Discovery 2012 9th International Conference on(FSKD 2012)*, pp. 2232-2236, 2012.

[45] J. Freudiger, M. Raya and M. Felegyhazi, "Mix-zones for location privacy in vehicular networks", *in Proc. the First International Workshop on Wireless Networking for Intelligent Transportation Systems(Win-ITS 2007)*.

[46] T. Hoppe, S. Kiltz and J. Dittmann, "Security Threats to Automotive CAN Networks-Pracitcal Examples and Selected Short-Term Countermeasures", *in Proc. The 27th International Conference on Computer Safety, Reliablity and Security (SAFECOMP 2008)*, pp.235-248, 2008.

[47] B. Groza, S. Murvay and A.V. Herrewege, "Libra-can: a lightweight broadcast authentication protocol for controller area networks", *in Proc. Cryptology and Network Security (CNS 2012)*, pp. 185-200, 2012.

[48] B. Groza and S. Murvay, "Efficient protocols for secure broadcast in controller area networks", *Industrial Informatics, IEEE Transactions* on, 9(4):2034-2042, 2013.

[49] M. Muter, A. Groll and F.C. Freiling, "A structured approach to anomaly detection for in-vehicle networks", *in Proc. Information Assurance and Security (IAS 2010)*, pp. 92-98, 2010.

[50] P.S. Murvay and B. Groza. "Source identification using signal characteristics in controller area networks", *in Proc. Signal Processing Letters (SPL 2014)*, 21(4):395-399, 2014.

[51] L. Yu, J. Deng and R.R. Brooks, "Autombile ECU Design to Avoid Data Tampering", *in Proc. the 10th Annual Cyber and Information Security Research Conference(CISRC 2015)*, pp.10-18, 2015.

[52] H. Schweppe and Y. Roudier, "Security and privacy for in-vehicle networks", *in Proc.Vehicular Communications, Sensing, and Computing (VCSC 2012)*, pp.12-17, 2012.

[53] H. Schweppe, Y. Roudier and B. Weyl, "Car2x communication: securing the last meter-a cost-effective approach for ensuring trust in car2x applications using in-vehicle symmetric cryptography", *Vehicular Technology Conference (VTC Fall 2011)*, pp.1-5, 2011.

何磊. 基于 FlexRay 总线的转向系统双电机控制方法研究[博士学位论文]. 长春: 吉林大学, 2011.

[54] J. Petit and S.E. Shladover, "Potential cyberattacks on automated vehicles", *Intelligent Transportation Systems, IEEE Transaction* on, 16(2): 546-556, 2015.

[55] M. Raya and J.P. Hubaux, "Securing vehicular ad hoc networks", *Journal of Computer Security*, 15(1):39-68, 2007.

[56] S. Checkoway, D. McCoy and B. Kantor, “Comprehensive Experimental Analyses of Automotive Attack Surfaces”, *in Proc. USENIX Security Symposium(USENIXSS 2011)*, pp. 23-31, 2011.

[57] D.K. Nilsson and U.E.Larson, “Conducting forensic investigations of cyber attacks on automobile in-vehicle networks”, *in Proc. of the 1st international conference on Forensic applications and techniques in telecommunications,* information, and multimedia and workshop (ICST 2008), pp. 8-16, 2008.

[58] T. Hoppe, S. Kiltz and J. Dittmann, “Applying instrusion detection on automotive it-early insights and remaining challenges”, *Jounal of Information Assurance and Security*,4(6):226-235, 2009.

[59] J.H. Liu, C.P. Ji and M. Gao, “Research on intelligent ECU for engine based on CAN”, *in Proc. 2010 WASE Global Congress on Science Engineerin(GCSE 2010)*, pp.40-41, 2010.

[60] K.J. Lee, Y.H.Ki, H.S.Ahn, G. Hwang and J.S.Cheon, “Functional Safety Compliant ECU Design for Electro-Mechanical Brake (EMB) System”, *SAE International Journal of Passenger Cars - Mechanical Systems*,6(3), 2013.

[61] A.X.A. Sim and B. Sitohang, “OBD-II standard car engine diagnostic software development”, *in Proc. 2014 International Conference on Data and Software Engineering(ICODSE 2014)*, 2014.

[62] R. Ech, P. Tomik and J. Kuhanek, “Setting of combustion engine ECU parameters with use of knocking detection”, *in Proc. the 2015 16th International Carpathian Control Conference(ICCC 2015)*, pp.69-72, 2015.

[63] T. H. Nguyen, B.M.Cheon and J.W. Jeon, “CAN FD performance analysis for ECU re-programming using the CANoe”, *in Proc. Consumer Electronics (ISCE 2014)*, pp.1-4, 2014.

[64] J. S. Park, I.H. Suh, C.Y. Choe, M. Ro and S.P. Brewerton, “Intelligent ECU end of line testing to support ISO26262 functional safety requirements”, *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, 6(1):162-168, 2013.

[65] C. Sun and X.F. Pei, “Development of ABS ECU with Hardware-in-the-Loop Simulation Based on Labcar System”, *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, 8(1): 14-21, 2014

[66] T. Nighswander, B.Ledvina and J.Diamond, “GPS software attacks”, in Proc. *the 2012 ACM conference on Computer and communications security(CCS 2012)*, pp.450-461, 2012.

[67] G.C.Ma, Z.D.Liu, X.F. Pei, B.F. Wang and Z.Q. Qi, “Study on multi-object identification and compensation for on car radar”, *Transaction of Beijing Institute of Technology*, 33(11): 1135-1139, 2013.
(马国成, 刘昭度, 裴晓飞, 王宝锋, 齐志权, “车载雷达多车道目标识别及补偿方法”, *北京理工大学学报*, 2013, 33(11): 1135-1139)

[68] “EyeCar,”baiduwenku,http://wenku.baidu.com/link?url=EoeZeC6Wy5__7pa33QGQ5_cpUIk5IaCAmwty3iXd4lt4fZKlYbTioQc0wInLOg0RUYIUBX8HZJgdGoFeBZa4NKAd6BqiMqYSchJ19FVgvyK,Sept, 2012.

[69] “CamCar,”baiduwenku,http://wenku.baidu.com/link?url=JD5HzjX2EUz0hrYo2KPSDuwMJ-NaF_2P9VD-voDSd8B_wExI2cOcjJ3TbcNb3Sq4yduSYw5_aCyUKHZzFoJUvI80Dj5IvMOkLhDvE6PpZ8q, May 2013.

[70] “SensorCar,”baiduwenku,http://wenku.baidu.com/link?url=_qRiVE23EaeZJWyErJR9MfmOtNf4j81AiPKAENF-sBr7fLcQhTB4TIWytby1wn3V-r0E0E5y5e5FDAP0GX142_IEgaB8VIoqLtxM-FJMH1W, Sept. 2010.

[71] “RescueCar,”baiduwenku,http://wenku.baidu.com/view/0c55051de97101f69e3143323968011ca300f77a.html?from=search, Nov. 2016.

[72] “SecurCar,”baiduwenku,http://wenku.baidu.com/view/09cf66ff04a1b0717fd5dd20.html?from=search, Dec. 2012.

[73] “SeccuriLock,”baiduwenku,http://wenku.baidu.com/view/09cf66ff04a1b0717fd5dd20.html?from=search, Dec.2012.

[74] Y. You, J. Hu and G.Y. Li, “Primary models of passenger car information integrated control system”, in Proc. *2010 IEEE International Conference on Automation and Logistics(ICAL 2010)*, pp. 618-623, 2010.

[75] W. Hogpracha and S. Wongpradhip, “Recognition system for QR code on moving car”, in Proc. *10th International Conference on Computer Science and Education(ICCSE 2015)*, pp.14-18, 2015.

[76] B. Martin, K. Yves, S. Christian and J. Friedrich. “Signal design and coding for high-bandwidth OFDM in car-to-car communications”, in Proc. *IEEE Vehicular Technology Conference (VTC 2010)*, 2010.

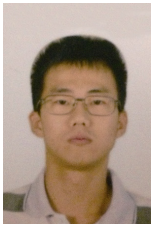
[77] Y. Shibahata, K. Shimada and T. Tomari, “Improvement of vehicle maneuverability by direct yaw moment control”, *Vehicle System Dynamics*, vol.22, pp. 465-481, 1993.

[78] D.W. Xu, “Study on Motor Vehicle Safety Technical Regulations and Standards of the World [Ph.D.dissertation]”, *Wuhan University of Technology*, Wuhan, 2007.

[79] B. Groza, S. Murvay, “Efficient protocols for secure broadcast in controller area networks”, *Industrial Informatics IEEE Transaction on*,9(4): 2034-2042, 2013.

冯志杰, 男, 博士生, 1982 年生, 现在中国科学院信息工程研究所担任工程师。研究领域: 移动通信安全、网络信息安全。Email: fengzhijie@iie.ac.cn

何明, 男, 博士, 1982 年生, 现在中科学院信息工程研究所担任助理研究员。研究领域: 数据挖掘, 车载信息系统攻防、计算机网络。Email: heming0405@163.com



李彬, 男, 硕士, 1983 年生, 现在中国科学院信息工程研究所担任工程师。研究领域移动通信安全、物联网信息安全。Email: libin@iie.ac.cn

邓明, 男, 硕士, 1986 年生, 现在中国科学院信息工程研究所担任工程师。研究领域通信安全、隐蔽信道、信道通信等。
Email: dengming@iie.ac.cn