Engineering Technology and Development, 工程技术与发展 (9)2021,3
ISSN:2661-3506 (Online) 2661-3492(Print)

智能网联汽车信息安全关键技术探究

施维振
烟台职业学院 山东 烟台 264670

摘 要：近年来，在互联网以及电子科技快速发展背景下，汽车产业逐渐与电子信息安全技术进行融合，推动汽车电子信息技术发展，对汽车的功能进一步完善，为人们的出行提供更大的便利。然而，人们在享受智能网联汽车便捷高效服务的同时，还需要面对一些信息安全问题。因此，智能网联汽车相关研究人员还需要结合存在的信息安全问题进行进一步探究，完善信息安全技术，保证智能网联汽车用户的信息安全。本文对智能网联汽车信息安全关键技术进行探讨。

关键词：智能网联汽车；信息安全；关键技术

一、智能网联汽车概述

智能汽车是现代化科学技术发展的重要产物，也是汽车产业优化升级的先进产品之一。在汽车上增设传感器、控制器和执行器等装置，比如雷达、摄像头等，以此通过车载环境感知系统、信息终端尽可能实现车、路、人的信息交换，保证车辆具有一定的智能环境感知能力，有利于自动分析车辆行驶安全和危险状态，有效替代人去实现驾驶决策和操作。而将智能汽车与网络相连接，则构成了智能网联汽车，是当前智能交通系统的核心部分，利用自主的环境感知能力和车联网体系，保证车载信息终端与业务平台实现无线通信和各类信息交换。所以，智能网联汽车是一种跨技术、跨产业域的新兴汽车体系。对于其定义有广义和狭义两种。广义的智能网联汽是指以车辆为主体和节点，运用现代通信和网络技术，促使车辆与外部网络进行信息共享和协同化控制，保证车辆的行驶安全。从狭义上讲，智能网联汽车是搭载先进的传感器、控制器以及执行器，基于现代通信与网络技术，实现 V2X 智能信息交换和共享，具有对复杂环境感知、智能决策以及协同控制和运行执行等功能，替代人来驾驶操作的新一代汽车产品 [1]。

二、我国智能网联汽车存在的信息安全问题

1. 车辆安全问题

目前，我国的智能网联汽车技术还不够成熟，并且也无法保证我们在使用汽车的过程中的人身安全以及信息安全，信息安全问题更是容易被黑客破解，比如车内的应用系统以及秘钥安全。车辆系统安全以及秘钥安全都可以分为两个方面，首先是系统安全，分别是软件系统安全以及硬件系统安全这两个组成部分，近些年来我国汽车智能软件不断的发展，各种类型的应用软件相继上线并且应用，不断地方便用户的体验，但是使用智能网联汽车使我们的信息更容易被盗取，现在大多数车辆软件的制造都还比较粗糙，还是使用传统形式的下载安装方法，将自己的软件做成一个安装包，让用户下载。这样虽然方便了各大用户的下载，但也极其容易受到不法分子以及黑客入侵，这样的方式极其容易泄露使用者的信息，严重情况下会导致整个车辆系统的瘫痪。硬件是车辆当中一些必需品，比如说雷达和自动驾驶系统等等，如果汽车硬件受到了入侵，就极其容易对我们的人身安全造成影响，比如汽车在行驶的过程中，黑客会影响雷达对于周围环境的判断情况，通过制造假的障碍物来干扰汽车的正常行驶。秘钥分为对称秘钥以及非对称秘钥，其主要内容就是通过各种加密的手段来保护信息安全。所以说，黑客一旦入侵破解秘钥系统，我们的所有信息都会被泄露，就没有任何的秘密可言 [2]。

2. 路侧单元安全问题

如今，随着社会中车辆的增加，我国提出了交通强国的战略路线，为了确保车辆日常行驶的安全，我国对于各地政府也下达了相应的政策，从而改善现在的路况，并且设置了更多的科技化的路段基础设施，例如监控摄像，微波探测仪，气象站，智能化交通指示灯，电子路牌等方便汽车智能化行驶的设施。智能网联汽车通过物联网系统对道路中各项设施做出智能的判断，并且感知到道路的环境以及交通运行状态，物联网系统对于这些路段基础设施做出了更好更优秀的路面判断，可以帮助行驶的车辆告知行驶的道路中其他的对于行驶安全的的障碍，并做出智能的判断。但是，如果这些路侧单元被不法分组入侵，将会对整个社会造成极其恶劣的影响。

3. 云平台安全问题

智能网联汽车的云平台主要是通过远程操控，分析用户的驾驶行为，对车辆健康做出判断，并且定位汽车等等，是智能网联汽车中必不可少的内容，如果汽车云平台被入侵将会对汽车造成非常巨大的影响，因此，我们要做好对汽车的防护措施，做好对于病毒的防控，以及设置除用户之外的访问权限等等。

具体有以下几种实施手段：第一，要保证云平台的系统稳定，技术人员随时监控和升级系统，搭建最新防御体系，主动防御黑客的入侵和破坏；第二，汽车生产厂家和相关系统开发团队要针对黑客入侵、病毒爆发等事件做好充分准

备，建立起一套完整的应急体系、应对策略和数据保护系统，完善相关的标准化工作、通信协议，随时保护和备份客户资料数据；第三，厂家在维护和升级系统软件的同时，也要在硬件层面加大研发投入，升级老旧造车平台，确保整车从系统到硬件各个方面的安全性。

4. 网络传输安全问题

使用智能网联汽车时要注意网络传输的安全，可以采取下面的几种方法来预防：一是注意其他用户的来访，现在很多黑客通过对于身份的改变对网络进行入侵；二是和其他车辆进行信息传输的时一定要注意对其过程进行加密，确保与我们接触的应用程序、连接等是的安全；三是进行协议签订的过程中，会受到其他不法分子对协议进行更换，所以我们需要在签订协议时进行加密[3]。

5. 连接设备安全问题

现在人们对智能网联汽车的认可度越来越高，智能网联汽车的社会普及度也在增高，在这种环境出现了针对于智能网联汽车的各种形式的 APP 和路边的充电站，但是这些产品对智能网联汽车的外部环境造成了巨大的隐患，因为人们在使用这些 APP 或者充电桩时就有可能被病毒入侵。现在对于这些产品的管控不足，导致这些产品的质量参差不齐，一些山寨产品以及恶意产品也会混入其中，车辆对于这些产品的防护能力还十分的薄弱，在使用过程中有可能受到病毒的入侵。路边的一些充电桩看似安全，其实也暗藏玄机，黑客可以通过对充电桩的入侵，在车辆充电的时候侵入到车辆系统从中获利。甚至通过修改充电桩的收费设置，在支付环节进行恶意扣费，还会获取用户的支付信息等等。

三、智能网联汽车信息安全关键技术

1. 进一步加强安全技术研发工作

当前，智能网联汽车的安全问题尚未达到远期的要求，需要对智能网联汽车的安全技术进行整体性的升级。首先，需要升级防病毒侵袭系统，让用户在驾驶的过程中更加放心，进而对智能网联汽车的使用过程中有着更好的体验，并确保汽车信息交换安全、汽车行驶安全以及隐私信息安全等。

相较于传统汽车，智能网联汽车有着明显的开放性，有更加多样化的功能。现在人们对于智能网联汽车的接受度越来越高，使得信息安全领域延伸出各种信息问题，为了避免在驾驶智能网联汽车所遇到安全问题，必须将信息安全防护意识体现到各个环节。需要从研发环节到整个生产过程构建出系统的信息安全闭环，提高车辆信息的安全性。另一方面，从生命周期的角度来强化该项防护研究工作，将其中的芯片、APP、通讯协议以及内核系统应用的创新作为主要工作内容，全面提高汽车云平台以及应用软件的安全防护水平。我们还需要不断学习国外的先进技术，研究国外的先进的防护系统。最后，国家需要下达对智能网联汽车的相关法律条规，从而整治当前的不良情况，对其进行统一管理，从而确保监管和服务的稳定与可靠。

2. 构建完善的信息安全标准体系

智能网联汽车对于我国来说还处于创新阶段，其安全问题尚未形成较为完整的标准体系，针对该问题我国虽然发布了的相关的条规，但仍有一定欠缺，导致未知的安全隐患出现。因此，我国目前阶段还需要根据国内的具体情况对法规进行完善。需要做的内容：首先，强化专项法律工作，在智能网联汽车信息安全细节工作上给予明确的规定。其次，不断的学习其他国家先进的安全防护技术，联合标准化机构制定信息安全防护的标准。此外，智能网联汽车数据安全技术标准，必须要对数据进行分级制定，确定其保护级别，建立云端外部连接数据安全的标准制度[4]。

总结语

综上所述，智能网联汽车作为我国的新兴行业，在信息安全技术方面还需要加强研究，做好技术的完善与升级，为广大用户提供优质且安全的智能网联汽车服务。

参考文献

[1] 赵光辉，许美星 . 智能网联汽车信息安全关键技术探讨 [J]. 时代汽车，2019（21）：76-77.

[2] 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（08）：61-62.

[3] 王建，陈晓光，朱研，任翔 . 基于车载以太网的智能网联汽车网信安全防护技术研究 [J]. 智能网联汽车，2020（01）：92-95.

[4] 重视智能网联汽车产业发展与安全共振 [J]. 自动化博览，2020（11）：56-59.

作者简介：施维振（1984-）男，汉族，山东郯城人，硕士研究生，中级讲师，烟台职业学院，研究方向为智能网联汽车技术。