基于车载信息交互系统信息安全性研究

沈林强
杭州鸿泉物联网技术股份有限公司

摘要：随着城市化的推进，越来越多的人涌入城市，加之私家汽车数量的持续增长，导致现代城市交通承担的压力与日俱增。在互联网时代下，车联网逐渐成为缓解交通压力的重要举措，但网络环境的开放性却会对用户的信息安全带来威胁。基于此，本文将对车载信息交互系统信息安全的保障策略进行深入研究，以期为该领域的发展扫清障碍。

关键词：车载信息交互系统；信息安全；问题；对策

随着互联网技术的持续发展，其与社会许多行业的融合也在持续推进。在交通领域，基于互联网技术而构建的车联网在交通事故防控、行车导航等方面均发挥着十分重要的作用。但由于车联网需要通过各类通信互联网技术实现远程控制，在此过程中就可能会出现信息安全问题。对此，必须尽快构建一套适应车载信息交互系统的安全防护体系，为用户的信息安全提供保障。

一、车载信息交互系统结构功能以及存在的安全问题分析

（一）车载信息交互系统的结构级功能

车载信息交互系统（T-BOX）是安装在汽车上用于控制、跟踪汽车的嵌入式系统，其一般结构主要包括移动通信模块、存储模块、GPS模块、微控制器模块、OBD模块等五个部分。车载信息交互系统可以支持汽车内网和外网的信息交流沟通。一方面，T-BOX通过CAN总线和汽车内部主机建立连接，对车辆状态信息、控制信息等进行采集整合，另一方面T-BOX通过云平台和用户的平板、智能手机等进行信息交互。

T-BOX的功能主要包括数据采集、数据上报、安防服务、远程控制、远程诊断、远程升级以及与中控屏的数据交换等功能。其中远程控制功能可以帮助车主通过在远端完成汽车发动的启动关闭、车门的上锁开锁，此外灯光、空调等也可以通过该功能进行调控。通过数据采集上报功能可实现车辆定位、驾驶行为记录查询等，可以使车主对车况进行实时了解。安防服务主要包括紧急救援求助、碰撞自动报警、车门入侵自动报警等方面。远程诊断功能可远程诊断车辆，了解车辆的故障信息以及驾驶人未察觉的潜在故障信息，可以用于指导车辆的维修。远程升级功能可实现对T-BOX本身的升级功能，还可以对与T-BOX相连的仪表、ECU、BMS等主机的升级功能。T-BOX与中控屏的数据交换功能可实现将T-BOX产生的报警信息、故障信息以及其它信息在中控屏上展示，完成人机交互的功能。

（二）车载信息交互系统中涉及到的安全问题分析

通过上文分析可知，车载信息交互系统的安装可以为用户带来多领域的便利，但是由于该系统在运行的过程中会通过云平台和外部网络建立连接，并进行信息的传输，而在这一过程中则存在巨大的安全隐患。结合实践来看，车载信息系统所涉及到的安全问题主要包括以下四个方面：

其一，硬件安全问题。车载信息交互系统的硬件结构十分复杂，其中芯片、PCB板、启动模块、硬中断等多个方面都存在一定的安全隐患。在硬件设计的过程中，若是不能以专业的工具对其各部件安全进行全面分析，很可能会在今后的使用中出现安全问题。

其二，软件安全问题。在车载信息交互系统中，软件是最容易出现恶意攻击的部分，如何保障软件在恶意攻击下仍旧能够安全正确运行是现阶段该领域研究的热点项目。软件安全问题主要源自于操作系统、通信协议、应用软件等方面，当前阶段，敏感信息保护、应用安全等受到了消费者越来越多的关注。

其三，通信安全问题。车载信息交互系统的通信主要由车内通信和车外通信两部分构成，相较而言，车内通信存在的安全隐患较小，因为其只涉及到了车内主机和交互系统的通信，车辆状态信息和控制信息始终在车内流转。而车外通信则涉及到了车载信息交互系统和云平台的数据传输，这需要通过互联网来实现，这就需要面临加密、认证、协议等方面的安全问题。如车辆信息加密强度不够的情况下容易出现信息泄露、丢失的问题。而在认证环节则存在身份信息伪造的问题。

其四，数据安全。在进行信息录入、处理、统计以及打印等工作的过程中，操作不当、程序缺陷、黑客攻击、断电、设备故障等问题都有可能会导致数据库的损坏或是丢失。此外，权限设置不合理可能会导致一些资质不足的人员接触到敏感信息，使数据泄露的风险大幅度增加。

二、车载信息交互系统信息安全问题的有效对策研究

（一）优化硬件设计

在硬件设计过程中，对芯片、标识以及启动模块等部件进行重点防护，在芯片中添加智能加密单元，并在其接口部位设置鉴权机制，防止信息从此泄露。对于标识，应对其改写权限进行严格的设置，保障其具有唯一可识别性。在启动模块方面，则需要加强对启动过程的安全监督，同时严格校验系统硬件配置和内核是否匹配。

（二）加强软件安全防护

为了保障车载信息交互系统的软件安全，应构建多层次的安全防护体系。首先，对车密匙采取高强度的加密手段予以保护。其次，设置访问权限，禁止一些未授权的访问行为。再次，完善安全审计，做好审计日志存储管理。最后，选择经签名认证后的应用软件，并对资源、数据等进行安全隔离。

（三）通信安全防护措施

基于通信安全问题的具体情况，其信息安全防护应从网络连接、通信应用以及外置存储等方面入手。其中网络连接安全涉及到WIFI、蓝牙、蜂窝网等方面。对通信应用采取用认证机制，同时对通信数据进行严格的加密处理。此外，在外置存储中同样需要对数据进行加密，在此基础上设置访问权限。

（四）数据安全

数据安全防护应该着重关注数据采集、传输、存储、访问等工作环节。在数据采集阶段，建立严格规范的采集规则。在进行数据传输时必须进行加密处理，通过校验保障数据的完整性。在数据存储中，应采用加密存储技术，并做好备份，降低数据损坏、丢失可能造成的负面影响。数据访问应设置权限，禁止未授权访问行为。

结束语

综上所述，车载信息交互系统目前在我国已经得到了广泛的普及，为人们的车辆管理以及日常出行带来了极大的便利，同时也有效的缓解了我国交通压力。但为了保障其健康发展，必须尽快解决其存在的信息安全问题，为广大车主提供更加优质的信息功能服务。

参考文献

[1]刘子龙.多通道交互在车载信息娱乐系统中的应用研究[D].北京理工大学，2016.

[2]李晓峰，朱倩，张平.浅析车载信息娱乐系统界面设计[J].机械，2015年06期.

[3]路璐，田丰，戴国忠，王宏安.融合触、听、视觉的多通道认知和交互模型[J].计算机辅助设计与图形学学报，2014年04期.