车载信息系统的安全测评体系及方法

陈秀真, 吴 越, 李建华

上海交通大学信息安全工程学院 上海 中国 200240

摘要 汽车信息系统的安全工作主要集中在分析、挖掘车载信息系统及其功能组件现存的安全漏洞及可行攻击方式的实验验证, 缺乏全面、系统的车载信息系统安全测评体系及评估方法。论文在分析车载信息系统安全现状的基础之上, 提出将车载信息系统的安全等级划分为: 家用车载信息系统和商用车载信息系统, 定义了两个等级车载信息系统的保护能力, 并借鉴通用信息系统的安全等级保护要求, 提出车载信息系统不同保护等级的基本安全要求, 首次建立车载信息系统的安全等级测评体系。进一步建立层次化安全评估模型及算法, 实现车载信息系统的定量安全评估。通过奥迪 C6 的安全测评案例证明, 提出的等级测评体系及评估方法是可行、合理的, 为分析车辆信息系统的安全状况提供支撑, 填补了国内车载信息系统安全测评体系及评估方法的空白。

关键词 车载网络; 安全评估; 层次分析法; 安全漏洞; 安全威胁
中图法分类号 TP309 DOI 号 10.19363/j.cnki.cn10-1380/tn.2017.04.002

System and Approach of Security Testing and Evaluation for In-Vehicle Information Systems

CHEN Xiuzhen, WU Yue, LI Jianhua

School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Abstract The study of in-vehicle information system security mainly focuses on discovering and analyzing security vulnerabilities hidden in a car's information system and its function components, and on exploring the experimental way of feasible attacking means. There is no comprehensive and systematic security evaluation system and method in the field of in-vehicle information systems. This paper firstly attempts to build classified security evaluation system for in-vehicle systems, including put forward to divide in-car information system security into two levels: family car and business car, define their protection abilities based on analysis of current security status of the car information system, and design baseline for classified protection of in-vehicle system security with reference to security requirements of classified general information systems. Further this paper builds a hierarchical security evaluation model with three levels: index, criterion and security goal for in-car systems and its corresponding algorithm. It well reaches quantitative security evaluation of in-vehicle systems. The evaluation test results on Audi C6 demonstrate that the proposed classified security evaluation system and method are feasible and effective for analyzing security status and discovering security gaps of in-car systems. It fills the gap of classified security evaluation systems in the field of in-vehicle systems.

Key words in-vehicle network; security evaluation; analytic hierarchy process; security vulnerabilities; security threats

1 引言

车载信息系统运用计算机、卫星定位、通讯、控制等技术, 向驾驶员及乘客提供安全、环保及舒适性功能和服务, 包括车身系统、动力传动系统、安全系统、信息系统, 实现包括车辆信息、车身控制、故障检测、实时路况、导航定位、辅助驾驶、多媒体娱乐、无线通信、移动办公等功能, 极大地提升了汽车信息化和智能化水平。

近年来, 汽车与互联网联动越来越普遍, 车载软件对于汽车控制功能的影响逐渐增大, 汽车与外部网络及外围设备交换车辆信息的必要性日益增加, 广泛的信息交换如下图所示。

由于车载信息系统趋向于使用通用系统与协议标准, 并以各种方式与互联网连接交互, 安全漏洞与威胁也随之而来。接入外部网络无疑会为攻击创

通讯作者: 吴越, 博士, 副教授, Email: wuyue@sjtu.edu.cn。

本课题得到国家自然科学基金(No.61562004, No.61431008, No.61271220)、上海市信息化发展专项资金(201601074)、中法国际合作与交流项目“徐光启 2016”项目(No.36492NA)的资助。
收稿日期: 2016-08-05; 修改日期: 2017-1-23; 定稿日期: 2017-03-07

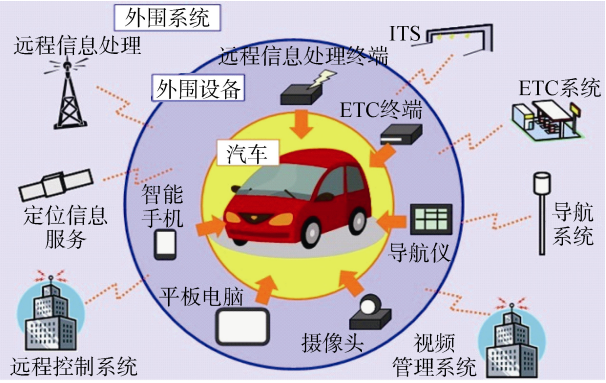

图 1　汽车与外部的信息交互

造入口, 通用系统普及致使攻击的难度下降, 服务的多样化意味着汽车拥有大量的信息, 只要窃取到有价值的信息就能直接获利。快速发展的车载信息系统为恶意攻击者提供了攻击便利, 包括直接攻击、从便携式产品入侵、从外部网络攻击等多重攻击方法[1]。从信息安全及行车安全的角度出发, 需要从设计、开发、使用、报废在内的每个阶段充分考虑汽车信息安全的问题。因此, 参照通用信息系统的安全测评体系及方法[2], 综合分析车载信息系统的安全现状, 研究车载信息系统的安全评估十分重要。

2　相关工作

论文参照计算机信息系统的安全等级测评体系构建方法及过程, 首次探讨了车载信息系统的安全测评体系建立及量化评估方法, 为车载信息系统的安全测评提供一种可行的解决路径。下面给出车载信息系统安全评测的相关工作以及安全等级测评体系构建的关键过程。

2.1　车载信息系统安全评测

车载信息系统快速发展的同时, 也包含着潜在的安全隐患, 为黑客攻击车辆信息系统提供了多种途径。美国参议院、美国国家高速公路安全管理局(NHTSA)等多方专家及研究人员通过调研分析证实: 部分车载信息系统在认证、通信保密等方面存在安全漏洞及安全隐患, 易遭到入侵和干扰, 甚至可能造成驾车安全事故。Checkoway S 等人讨论了车载诊断系统、娱乐系统、蓝牙、遥控门禁系统、胎压监测系统等存在的安全漏洞, 并实验验证了以上多种情况下具体攻击的可行性, 证明了通过利用每一个漏洞, 恶意攻击者都能够完全控制汽车的系统[3]。Ishtiaq Roufa R M 等人详细研究了胎压监测系统存在的安全漏洞, 包括缺乏输入验证和软过滤等基本安全措施、通信范围广导致通信容易被窃听、数据包容易被伪造造成电子欺骗攻击和电池消耗攻击、轮胎传感器标识容易被记录导致汽车位置信息暴露等, 并提出了相对简单的设计变化和将减轻胎压监测系统安全风险的密码协议[4]。以 Koscher K 为首的科学小组在 2010 年开展的研究表明, 车载信息系统广泛采用的控制器局域网络(CAN)底层协议存在一些固有的弱点, 病毒能够侵入车载信息系统, 通过蓝牙等无线技术远程控制刹车、锁车、停车等各项功能, 进而制造驾车事故[5]。Ansaf A I 等人对遥控门禁系统的安全漏洞及脆弱性做了详细的研究, 具体说明了包括扫描攻击、重放攻击、两个小偷攻击、挑战向前预测攻击、字典攻击等多种攻击方式的实施过程, 并提出了相应的改进措施及解决方案[6][7]。

由此可见, 车载信息系统的安全测评工作主要集中在汽车信息安全问题的研究, 包括车载信息系统及其功能组件现存的安全漏洞、面临的威胁及可行的攻击方式等方面进行的实验验证, 缺少车载信息系统的安全测评体系及评估方法。

2.2　安全等级测评体系构建的关键过程

综合分析计算机信息系统安全等级保护相关标准文件, 包括《信息系统安全保护等级定级指南》[8]、《信息系统安全等级保护基本要求》[9]等, 总结出安全等级测评体系构建的关键过程有定级、确定安全保护能力要求和基本安全要求, 这为车辆信息系统的安全等级测评体系构建提供参考。具体的过程细节如下:

(1) 定级。在确定定级对象的前提下自主定级, 根据信息系统在国家安全、经济建设、社会生活中的重要程度, 遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。其定级由两个要素决定: 等级保护对象受到破坏时所侵害的个体和对客体造成侵害的程度, 其中客体为: 1)公民、法人和其他组织的合法权益; 2)社会秩序、公共利益; 3)国家安全。对客体造成侵害的程度有三种: 一般损害、严重损害和特别严重损害。

(2) 确定不同级别的安全保护能力要求。安全保护能力指系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度, 不同安全保护等级的信息系统要求具有不同的安全保护能力。比如第 3 级信息系统的安全保护能力为应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难, 以及其他相当危害程度的威胁所造成的主要资源损害, 能够发现安全漏洞和安全事件, 在系统遭到损害后, 能够较快恢复绝大

部分功能。

(3) 设计基本安全要求。为了确保不同安全保护等级信息系统应该具有的基本安全保护能力而提出的安全要求, 从各个层面提出系统的每个组件应该满足的安全要求。根据实现方式的不同, 基本安全要求分为基本技术要求和基本管理要求两大类。其中技术类安全要求与信息系统提供的技术安全机制有关, 主要通过在信息系统中部署软硬件并正确的配置其安全功能来实现; 管理类安全要求与信息系统中各种角色参与的活动有关, 主要通过控制各种角色的活动, 从政策、制度、规范、流程以及记录等方面做出规定来实现。基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出, 基本管理要求从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出。

3 车载网络系统的安全需求与现状

车载信息系统中的功能组件分为两大类: 基本控制功能和扩展功能[1], 其中基本控制功能包括驱动系统和底盘系统, 有发动机管理、变速器控制、防抱死制动系统等功能, 是实现行驶、停止、转弯等基本功能的必要组件。扩展功能由包括车体系统、安全舒适功能、维护保养的控制部分和包括智能交通系统(ITS)功能、远程信息处理、信息娱乐系统的信息部分组成。而且, 扩展功能和外围设备实现的普通功能之间通过蓝牙无线局域网、USB 端口、SD 插槽、车载诊断接口等方式连接。车载信息系统架构如下图所示。

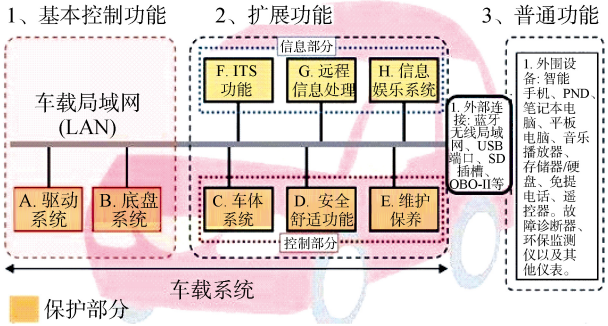

图 2 车载信息系统架构

车载信息系统最根本的目的是保证行驶安全, 在安全需求上更加注重实时性和可靠性, 因为这关系到汽车的基本行驶能力。一旦发生数据延迟等故障, 就可能导致驾车事故的发生。当某个或某几个控制单元发生故障时, 其他控制单元, 尤其是基本控制功能应仍可以正常工作。另外, 为了防止汽车位置和用户隐私等信息的泄露, 要对关键数据的存储、通信过程进行加密, 需要实现系统内组件间的身份鉴别。进行固件更新和诊断前, 需要严格认证更新及诊断来源, 防止恶意攻击者通过更新及诊断操作注入恶意代码, 以此确保车载系统的安全。

车载信息系统面临攻击者故意发起的攻击行为和用户偶然引发的失误, 比如非法设置系统数据、信息泄漏、窃听、DoS 攻击、虚假消息、记录丢失、病毒感染。通过访问方式, 将车载信息系统的安全漏洞与威胁进行分类, 如表 1 所示。

表 1 车载信息系统安全漏洞分类

访问方式	功能组件	漏洞
直接物理访问	车载诊断系统	外部诊断设备可以访问系统中所有 CAN 总线。
间接物理访问	车载诊断系统	缺少设备身份验证及输入验证措施。
	娱乐系统	基于 CD 的固件更新漏洞, 编码到 CD 或歌曲文件实现恶意输入。
	蓝牙	缓冲区溢出漏洞, 自动响应配对请求, 易被诱捕、劫持、窃听。
短距离无线访问	遥控门禁系统	易被窃听、受到重放攻击。
	胎压监测系统	没有身份验证、输入验证和软过滤, 易被窃听、假冒, 暴露汽车位置信息。
远程无线接入	远程信息处理系统	网关漏洞, 身份验证漏洞。
内部总线	CAN 总线	CAN 广播性质, 易受到拒绝服务(DoS)攻击; 没有身份字段; 弱访问控制; ECU 固件更新和开放的诊断控制。

车载诊断系统: 恶意攻击者直接通过诊断接口将恶意组件插入汽车的内部网络或者通过攻击连接诊断接口的外部设备, 进而攻击连接这个外部设备的汽车。由于车载信息系统与该外部设备之间的通信缺少身份验证或是输入验证措施, 攻击者能够很容易地控制它或是对其植入恶意代码。

遥控门禁系统: 无线电遥控钥匙和位于汽车上的无线电收发器之间的无线通信没有加密措施, 恶意攻击者可以使用廉价的无线扫描器接受汽车和遥控钥匙之间的无线电信号, 分析截获的无线电模式, 推断出某些破解遥控门禁系统的安全特征, 进而破解系统的安全防护, 直接盗取车辆。

胎压监测系统: 安装在轮胎内腔的多个无线传感器与位于汽车底盘的无线电接收机之间的通信基于标准的调制方案和简单协议, 协议未使用加密机制, 通信可以逆向工程实现, 信息容易被窃听及解析; 缺少数据包身份鉴别及过滤措施, 攻击者容易伪装压力报告信息, 造成电子欺骗攻击和电池消耗攻击。注入伪造信息干扰正常操作, 减弱驾驶员对系统的信任, 可能导致驾驶员完全忽略胎压监测系统相关的警告。如果此时汽车正在高速公路上行驶, 其直接后果将是严重的驾车事故。

娱乐系统: 几乎所有汽车提供一个能够播放各种格式音频的CD播放器及外部数字多媒体端口, 允许用户使用他们的个人音频播放器或电话控制汽车媒体系统。而且, 汽车媒体系统与CAN总线互联, 或直接与其他汽车系统连接, 支持一个共用的维护路径更新所有 ECU 固件。因此, 一个被危害的 CD 播放器可以提供一种有效矢量攻击其他汽车零部件。

蓝牙: 该技术有效解决了小型移动设备间的无线连接问题, 其通过个人识别密码(PIN 码)实现设备之间的连接认证, 但用户往往会使用一些很容易记忆的PIN码, 或者把PIN码存储在两个设备中, 这就会使得 PIN 码很容易遭到诱捕、劫持、窃听等攻击。通过车载蓝牙设备, 恶意攻击者可以采取间接短程无线攻击和直接短程无线攻击两种攻击方式, 即使在没有配对设备的情况下, 攻击者只要通过嗅探蓝牙通信等方式得到汽车的蓝牙 MAC 地址、并暗中对自己的设备与汽车进行配对, 就可以在配对的通道注入漏洞, 进而危害汽车。

CAN 总线: 其是国际上应用最广泛的现场总线之一, 在汽车各电子控制装置 ECU 之间交换信息, 形成汽车电子控制网络。在总线的数据传输与访问控制部分, 存在许多容易被攻击者利用的安全漏洞。比如CAN数据包物理上和逻辑上都是广播到所有节点, 网络上的恶意组件可以很容易地窥探所有通信或发送给网络上其他节点的数据包。CAN 数据包不包含身份验证字段或任何源标识符字段, 任何组件可以无差别地发送一个数据包到任何其他组件。这意味着如果组件本身不具有防御机制, 任何一个被危害的组件可用于控制总线上的所有其他组件。

远程信息处理系统: 其通过蜂窝语音和数据网络提供持续连接, 提供包括远程诊断、故障救援、防盗追踪、车载导航在内的多种功能。汽车制造商使用的 aqLink 软件调制解调器存在基于堆栈的缓冲区溢出漏洞, 同时“挑战-应答”的通信方式中随机数发生器每次都使用相同的常数进行随机计算, 这意味着多次调用系统会导致相同的预期响应, 攻击者能够观察到响应数据包后重放应答。

4 安全等级划分体系

4.1 信息资产

车载信息系统不同于传统信息系统, 其应当保护的信息资产存在特殊性, 具体包括基本控制功能的运行、汽车固有信息、汽车状态信息、用户信息、软件、内容及设置信息, 详细说明见表 2 所示。

表 2 汽车内部信息资产说明

信息资产类别	说明
基本控制功能的运行	基本控制功能的连贯性和可用性, 基本控制功能的执行环境和使其运行的通信。
汽车固有信息	包括汽车车体中固有的信息(车辆 ID、设备 ID 等)、认证信息码、行驶及运行记录等积累的信息。
汽车状态信息	表示汽车状态的数据、位置、车速、目的地等。
用户信息	用户(驾驶员和乘员)的个人信息、认证信息、缴费信息、使用记录和操作记录等。
软件	ECU 的固件等关系到汽车基本控制功能和扩展功能的软件。
内容	视频、音乐、地图之类的应用数据。
设置信息	硬件和软件的运行设置数据。

4.2 安全等级划分及保护能力定义

参照传统信息系统的等级划分方法[8], 确定车载信息系统的受侵害客体、保护级别定义及不同级别的保护能力要求, 具体如下:

受侵害的客体: 汽车内部的信息资产, 包括两类: 1)基本控制功能和其他功能的正常使用; 2)汽车信息及用户信息。

等级划分: 将车载信息系统划分为两级: 第一级车载信息系统命名为“家用车载信息系统”, 即从普通家庭的使用角度出发, 关键在于汽车的正常行驶和各附加功能的正常使用, 具体要求保障汽车基本的运行及视频、音乐、地图导航等应用软件的正常使用; 将第二级车载信息系统命名为“商用车载信息系统”, 即从商用办公的使用角度出发, 在家用车的基础上增加对汽车固有信息、汽车状态信息及用户信息等可能关系到商业信息的隐私信息的保护。

保护能力要求: 对于家用车载信息系统, 应能够确保系统基本控制功能、软件、内容、设置信息的正常运行, 防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的关键资源损害, 能够发现重要的安全漏洞和安全事件, 在系统遭到

损害后, 能够恢复部分功能; 对于商用车载信息系统, 应能够确保系统基本控制功能、软件、内容、设置信息的正常运行, 确保汽车固有信息、汽车状态信息及用户信息的数据安全, 在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难、以及其他相当危害程度的威胁所造成的主要资源损害, 能够发现安全漏洞和安全事件, 在系统遭到损害后, 能够较快恢复绝大部分功能。

4.3 安全等级保护基本要求

参照传统信息系统的安全等级保护基本要求[9], 针对家用和商用两个级别的车载信息系统, 结合其安全漏洞、面临的威胁及不同等级对信息资产的保护要求, 尤其是车载信息系统特定功能组件的安全要求, 从系统安全、网络安全、应用安全、数据安全及备份恢复四个方面给出基本要求。家用车载信息系统的系统安全、网络安全、应用安全、数据安全和备份恢复的具体要求分别如表 3、表 4、表 5、和表 6 所示。

商用车载信息系统在家用车的基础上提出了更高的安全要求, 增加了剩余信息保护、抗抵赖性等要求。下面给出商用车载信息系统比家用系统增加及修改的主要安全需求:

表 3 家用车载信息系统的系统安全要求

安全要求	细则说明
身份鉴别	身份鉴别、口令复杂度要求、认证失败处理功能、设备名唯一性, 应特别关注通过诊断接口连接的设备。
访问控制	资源控制、限制默认账户访问权限。
安全审计	审计范围、审计内容、审计记录、审计保护, 应特别关注接入设备、进程调用等行为。
入侵防范	最小安全原则。
恶意代码防范	防恶意代码软件, 应特别关注通过诊断接口注入的恶意代码。
资源控制	设备接入限制、操作超时锁定、资源使用限度。

表 4 家用车载信息系统的网络安全要求

安全要求	细则说明
结构安全	冗余度要求、带宽要求、网络拓扑图、子网/网段划分。
访问控制	访问控制设备、会话控制、资源控制。
安全审计	审计内容、审计记录, 应特别关注蓝牙、遥控门禁系统及远程信息处理系统等网络设备。
边界完整性检查	非法外联。
入侵防范	监视攻击行为, 应特别关注经蓝牙、胎压监测、远程信息处理系统发起的攻击。
网络设备防护	身份鉴别、地址限制、身份标识唯一、口令复杂度要求、认证失败处理功能、蓝牙连接。

表 5 家用车载信息系统的应用安全要求

安全要求	细则说明
身份鉴别	认证控制模块、身份标识唯一性、认证失败处理、安全策略, 应特别关注胎压监测系统中传感器 ID 的身份验证、CAN 数据总线中通信双方的设备标识验证。
访问控制	安全策略、覆盖范围、默认账户权限限制、设备权限限制。
安全审计	审计范围、审计内容、审计保护。
通信完整性	校验码技术, 应特别关注胎压监测系统等通信过程中信息的完整性。
通信保密性	会话初始化验证、敏感信息字段加密。
软件容错	有效性校验功能、故障处理。
资源控制	自动结束会话、系统最大并发会话数限制、设备多重并发会话数限制、对总线控制时间限制、远程信息处理系统连接请求数量、ECU 组件访问次数和拉动车门把手次数限制。

表 6 家用车载信息系统的数据安全和备份恢复要求

安全要求	细则说明
数据完整性	传输完整性破坏检测。
数据保密性	存储保密性。
备份和恢复	重要信息备份恢复、硬件冗余。

表 7 商用车增加及修改的安全要求

安全要求	细则说明
安全审计	增加“分析审计数据并生成审计报表”。
入侵防范	增加“记录攻击行为并提供警报”。
身份鉴别	增加“使用两种或两种以上组合的鉴别技术”。
剩余信息保护	增加“完全清除设备鉴别信息”、“完全释放文件目录等资源所在存储空间”。
抗抵赖性	增加“为数据源发者或接受者提供数据原发证据、接收证据”。
资源限制	增加“对系统服务水平降低到预先规定的最小值进行检测和报警”。

5 基于 AHP 的定量评估方法

层次分析法(Analytic Hierarchy Process, 简称 AHP)是一种定性与定量相结合的决策分析方法, 将复杂问题分解为若干层次和若干因素, 构建多层次的分析结构模型[10]。其将决策者对复杂系统的决策思维过程模型化、数量化, 适用于多准则、多目标的复杂问题决策分析, 已经成功应用于网络安全风险评估中[11][12]。论文以车载信息系统在系统安全、网络安全、应用安全、数据安全及备份恢复四个方面的安全要求为基础, 建立层次化结构模型, 采用 AHP 方法实现车载信息系统安全的定量评价。

5.1 层次化结构模型

以家用车载信息系统为例, 将车载信息系统进行

层次分解。目标层对应车载信息系统的安全, 准则层分别为网络安全、系统安全、应用安全、数据安全及备份恢复四项。网络安全包括结构安全、访问控制、安全审计、边界完整性检查、入侵防范和网络设备防护六项指标; 系统安全包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范和资源控制六项指标; 应用安全包括身份鉴别、访问控制、安全审计、通信完整性、通信保密性、软件容错和资源控制七项指标; 数据安全及备份恢复包括数据完整性、数据保密性、备份和恢复三项指标。具体层次结构模型如图 3 所示。

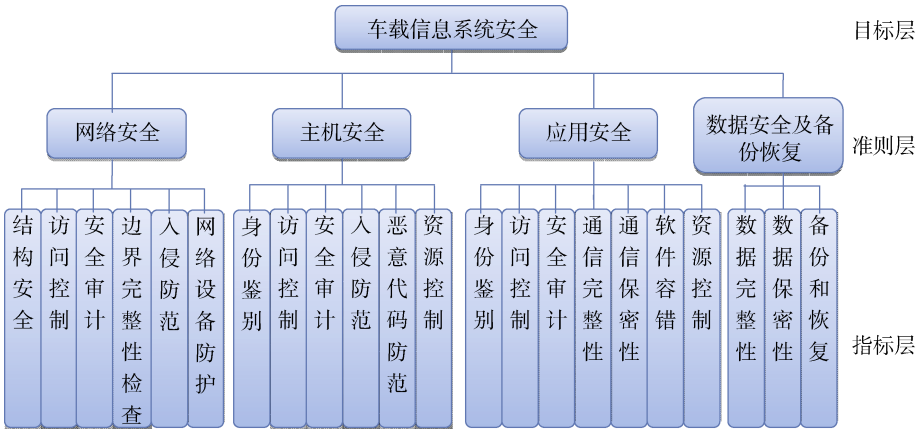

图 3　车载信息系统安全层次结构模型

5.2　判断矩阵的构造

使用九分位的相对重要比例标度确定评估准则层对目标层、指标层对准则层的相对重要程度, 以此构造判断矩阵:

$$A=(a_{ij})_{n\times n}$$

而且, 判断矩阵 A 有以下 4 个性质:

① $a_{ij}>0$;

② 当 $i\neq j$ 时, $a_{ji}=1/a_{ij}$;

③ 当 $i=j$ 时, $a_{ij}=1$。a_{ij} 为 i 与 j 两个指标相对权值的比值;

④ a_{ij} 的取值范围为 1、2、3、4、5、6、7、8、9, 其中取值为 1、3、5、7、9 分别表示对上一级而言, 指标 a_i 与指标 a_j 相比同样重要、稍微重要、明显重要、重要得多、极端重要, 取值为 2、4、6、8 分别表示与之相邻取值对应的判断级的中间值。

由于篇幅关系, 下面给出层次化结构模型中准则层对目标层、指标层对准则层中网络安全的判断矩阵, 分别如表 8、表 9 所示。

表 8　准则层对目标层 G 的判断矩阵 A_{zg}

	网络安全	主机安全	应用安全	数据安全及备份恢复
网络安全	1	2	1/3	3
主机安全	1/2	1	1/3	3
应用安全	3	3	1	5
数据安全及备份恢复	1/3	1/3	1/5	1

表 9　指标层对准则层中网络安全的判断矩阵 A_{zn}

	结构安全	访问控制	安全审计	边界完整性检查	入侵防范	网络设备防护
结构安全	1	1/2	2	3	1/3	1/5
访问控制	2	1	3	3	1/3	1/5
安全审计	1/2	1/3	1	2	1/5	1/7
边界完整性检查	1/3	1/3	1/2	1	1/5	1/7
入侵防范	3	3	5	5	1	1/3
网络设备防护	5	5	7	7	3	1

5.3　指标权重计算

为了计算指标层中各个指标对车载系统信息安全总目标的影响, 先计算准则层中 4 个准则对系统安全影响的相对重要性, 再逐次计算同一准则下对应指标的相对重要性, 最后计算出所有指标对信息安全总目标的权重。

5.3.1　准则层权重计算

论文提出的车载信息系统安全层次结构模型中准则层共有准则数 4 个, 即 n=4, 其权重向量 $W^{zg}=(W_1^{zg}, W_z^{zg}, W_3^{zg}, W_4^{zg})$具体的计算步骤如下:

(1) 将判断矩阵 A_{zg} 的每一列向量归一化。

$$\overline{a}_{ij}=\frac{a_{ij}}{\sum_{k=1}^{n}a_{kj}}(i=1,2,\cdots,n) \quad (1)$$

(2) 对按列归一化的判断矩阵 A_{zg}, 再按行求和。

$$\overline{W}_i=\sum_{j=1}^{n}\overline{a}_{ij}(i=1,2,\cdots,n) \quad (2)$$

(3) 将向量 $\bar{W}=\left[\bar{W}_1,\bar{W}_2,\cdots,\bar{W}_n\right]^T$ 归一化, 得到权重向量 W^{zg} 的第 i 个元素:

$$W_i^{zg}=\frac{\bar{W}_i}{\sum_{i=1}^{n}\bar{W}_i}\quad(i=1,2,\cdots,n) \tag{3}$$

5.3.2 指标层权重计算

利用公式(1)、(2)、(3), 依次处理指标层的 22 个指标对准则层中网络安全的判断矩阵 A_{zn}、主机安全的判断矩阵 A_{zh}、应用安全的判断矩阵 A_{za} 和数据安全的判断矩阵 A_{zd}, 得到以下权重向量:

$$W^{zn}=\left(W_1^{zn},W_2^{zn},\cdots,W_6^{zn},\underbrace{0\cdots0}_{16\text{ 个}}\right)$$

$$W^{zh}=\left(\underbrace{0\cdots0}_{6\text{ 个}},W_1^{zn},W_2^{zn},\cdots,W_6^{zn},\underbrace{0\cdots0}_{10\text{ 个}}\right)$$

$$W^{za}=\left(\underbrace{0\cdots0}_{6\text{ 个}},W_1^{za},W_2^{za},\cdots,W_7^{za},\underbrace{0\cdots0}_{9\text{ 个}}\right)$$

$$W^{zd}=\left(\underbrace{0\cdots0}_{19\text{ 个}},W_1^{zd},W_2^{zd},W_3^{zd}\right)$$

进一步形成指标层对准则层的权重矩阵 $W^{zz}=\left(W^{zn},W^{zh},W^{za},W^{zd}\right)^T$, 最后将准则层权重向量 W^{zg} 与权重矩阵相乘 W^{zz}, 得到 22 个指标的综合权重:

$$W=W^{zg}\times W^{zz} \tag{4}$$

5.4 系统安全定量评估

给定 22 个指标的取值向量 Z=(Z_1, Z_2,…, Z_{22})时, 车载信息系统的安全指数 S_c 的计算公式为:

$$S_c=Z\times W^T \tag{5}$$

其中, S_c 量化了车载信息系统的安全状况, 取值越大, 说明系统的安全性越高。

6 测评实施案例

针对奥迪 C6 进行安全测评, 这款车型使用了最先进的网络技术, 如 CAN、LIN、MOST 以及蓝牙等, 整车网络拓扑如图 4 所示。CAN 总线控制组合仪表、

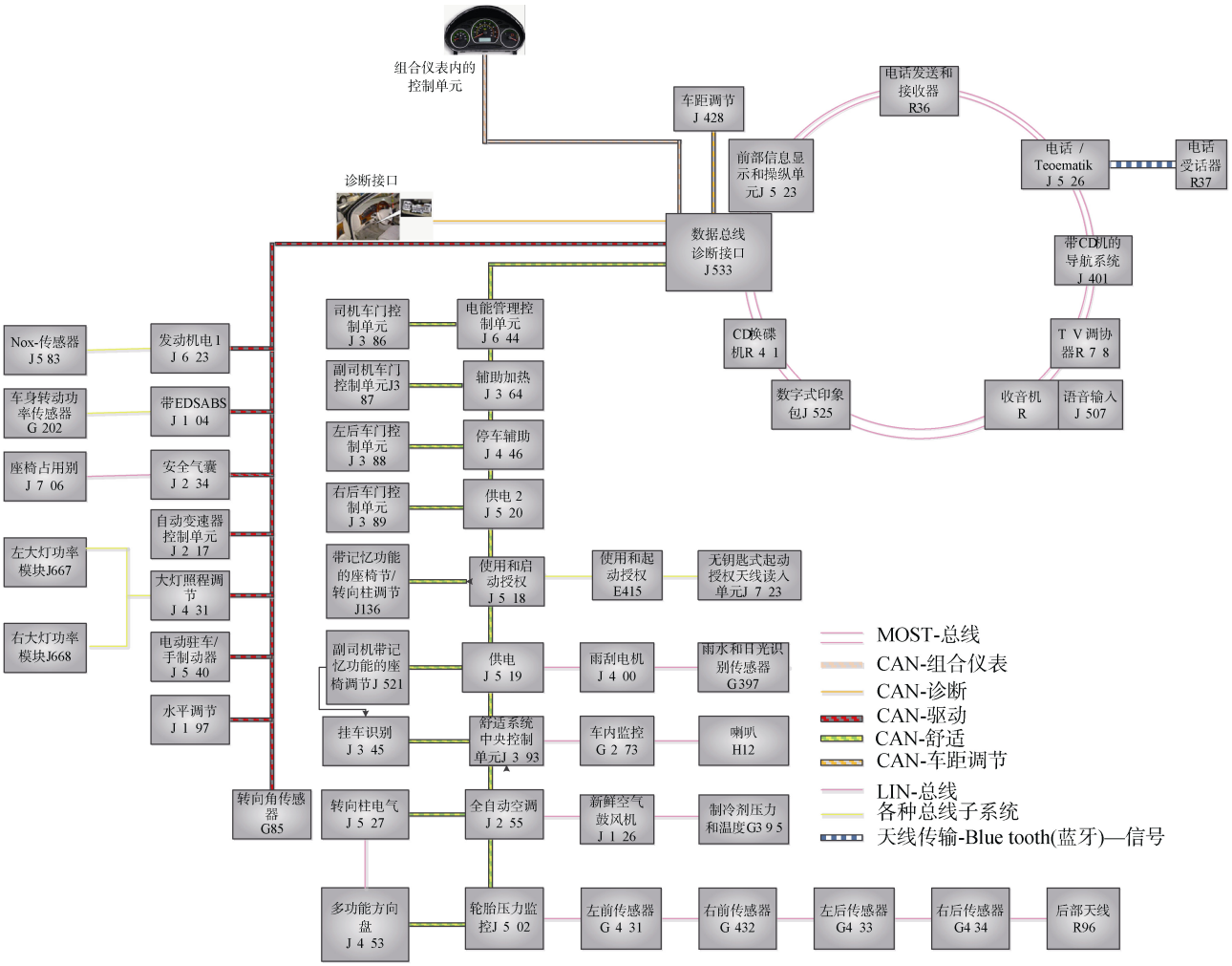

图 4 奥迪 C6 整车网络拓扑

表 10 奥迪 C6 各项指标得分表

准则层	指标层	得分 (满分 10 分)	指标层	得分 (满分 10 分)
网络安全	结构安全	10	访问控制	6
	安全审计	7	入侵防范	5
	边界完整性检查	4	网络设备防护	8
主机安全	身份鉴别	9	访问控制	7
	安全审计	7	入侵防范	6
	恶意代码防范	5	资源控制	8
应用安全	身份鉴别	9	访问控制	7
	安全审计	7	软件容错	10
	通信完整性	8	通信保密性	7
	资源控制	7		
数据安全	数据完整性	6	数据保密性	6
	备份和恢复	7		

诊断、驱动、舒适、车距调节等功能。LIN 总线控制部分 CAN 子功能, 包括轮胎压力监控、全自动空调、多功能方向盘等。MOST 总线控制信息娱乐系统, 包括带 CD 机的导航系统、收音机、蓝牙电话、Telematics 等。整个系统通过数据总线诊断接口联系起来。根据现场测评, 得到奥迪 C6 各部分的得分, 如表 10 所示。结合各指标的综合权重, 可计算得到奥迪 C6 车载信息系统的安全得分为 7.487, 测评对象的总体安全水平良好。

总的来说, 测评结论与奥迪 C6 车载信息系统的实际安全机制相符。在网络安全中, 该系统通过划分不同功能子网等措施保证了网络结构的安全。在网络设备防护部分, 蓝牙系统只有在将手机放入手机座内时才会工作, 保证了蓝牙连接的信息安全。在主机安全中, 有基本的身份鉴别及访问控制措施, 而且出于安全考虑, 使用和起动授权控制单元及使用和起动授权开关都要使用固定按钮位置信号; 出于资源控制考虑, 使 CAN 舒适系统在不工作时休眠。在应用安全中, 通过控制遥控门禁系统的工作频率和发射脉冲, 在避免各种如袖珍手机、无线耳机等持续的无线电发射干扰的同时, 为通信完整性和保密性提供了一定保障。对于软件容错, 供电控制单元等软件可以实现应急功能, 并记录下相应的故障。对于资源控制, 系统也有采用车上锁后约 80 小时, 或无授权钥匙操纵 20 次后, 关闭遥控门禁系统传感器等措施。

该系统比起传统信息系统更关注汽车特定功能的正常运行, 包括在故障处理方面都能采取及时的处理措施。除此之外, 该系统也实现了很多先进的功能, 包括丰富的娱乐功能等。但对于信息安全的保障还是有所欠缺, 缺少从全局的角度对系统信息资产进行全面的安全防护。

7 结论

论文首次提出面向车载信息系统的安全等级测评体系及基于 AHP 的量化评估方法, 包括等级划分、安全保护能力的定义、安全保护要求的设计及层次化定量评估模型, 有效填补了国内车载信息系统安全测评指标体系的空白, 有助于推动车载信息系统安全测评工作的开展, 为车载信息系统的安全防御提供有力支撑。

参考文献

[1] X.W. Wang, “Automotive information security issues can’t be ignored”, *Auto Industry Research*, 2013, No.11, pp. 34-39 (in Chinese), 2013.
王喜文, “汽车信息安全问题不容忽视”, *汽车工业研究*, 2013 (11): 34-39.

[2] L. Yang, Z.B. Guo, “Testing and evaluation for classified security protection of information system”, *Journal of Peoples’ Public Security University of China (Science and Technology)*, 2007, Vol.13, No.1, pp. 50-53.
杨磊, 郭志博, “信息安全等级保护的等级测评”, *中国人民公安大学学报*(自然科学版), 2007, 13(1): 50-53.

[3] S. Checkoway, D. McCoy, B. Kantor, et al, “Comprehensive Experimental Analyses of Automotive Attack Surfaces” in *Proc. USENIX Security Symposium*, pp.1-16, 2011.

[4] R.M. Ishtiaq, H. Mustafaa, S.O. Travis, et al. “Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study”, in *Proc. 19th USENIX Security Symposium*, pp.11-13, 2010.

[5] K. Koscher, A. Czeskis, F. Roesner, et al, “Experimental security analysis of a modern automobile”, in *Proc. Security and Privacy (SP)*, pp. 447-462, 2010.

[6] I.A. Ansaf, M.M. Syed, “Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs”, *IEEE Transactions on Vehicular Technology*, 2005, Vol. 54, No. 1, pp. 41-50.

[7] I.A. Ansaf, M.M. Syed, “Some Attacks Against Vehicles’ Passive Entry Security Systems and Their Solutions”, *IEEE Transactions on Vehicular Technology*, 2003, Vol. 52, No. 2, pp.431-439.

[8] GB/T 22240-2008, Information security technology – classification guide for classified protection of information system security, 2008.
GB/T 22240-200, 信息安全技术 信息系统安全等级保护定级指南, 2008.

[9] GB/T 22239-2008, Information security technology – Baseline for classified protection of information system security, 2008.
GB/T 22239-2008, 信息安全技术 信息系统安全等级保护基本要求, 2008.

[10] Yajun GUO, Theory and method of comprehensive evaluation, *Science press*, July 2002 (in Chinese).

郭亚军著, 综合评价理论与方法, 科学出版社, 2002 年 7 月.

[11] Qiong LIU, Study and design of the risk assessment system based on analytic hierarchical process, *Xidian University*, Master thesis, 2009.
刘琼, 基于层次分析法的风险评估系统的研究与设计, *西安电子科技大学*, 硕士学位论文, 2009.

[12] Yajuan Zhang, Xinyang Deng, Daijun Wei, Yong Deng, Assessment of E-commerce security using AHP and evidential reasoning, *Expert systems with applications*, 2012, Vol.19, No.3, pp. 3611-3623.

陈秀真 于 2005 年在西安交通大学控制科学与工程专业获得博士学位。现任上海交通大学电子信息与电气工程学院副教授。研究领域为计算机网络安全检测、评估与管理。研究兴趣包括: 信息系统安全检测与评估、网络安全综合监控与管理、工业控制系统安全。Email: chenxz@sjtu.edu.cn

李建华 于 1998 年在上海交通大学通信与信息系统专业获得博士学位。现任上海交通大学电子信息与电气工程学院教授、博导, 上海交通大学信息安全工程学院院长, 信息内容分析技术国家工程实验室主任, 国家教育部信息安全工程研究中心主任, 上海市信息安全综合管理技术研究重点实验室主任。研究领域为信息安全、计算机通信网。研究兴趣包括: 网络信息安全管理理论及应用、内容安全管理理论及应用、电子政务理论及应用、网络攻防和信息系统安全评测理论及应用。Email: lijh888@sjtu.edu.cn

吴越 于 2004 年在东南大学通信与信息系统专业获得博士学位。现为上海交通大学信息内容分析技术国家工程实验室副教授。研究领域为移动无线网络安全。研究兴趣包括: 无线网络安全, 车载网络安全与信任。Email: wuyue@sjtu.edu.cn