车载娱乐系统网络安全与隐私保护策略

张　云
扬州航盛科技有限公司　江苏　扬州　225100

摘　要：本文围绕车载娱乐系统的网络安全与隐私保护策略展开深入探讨。通过分析车载娱乐系统面临的网络安全漏洞和隐私合规性挑战，提出了相应的数据加密、身份验证等隐私保护技术和措施。同时本文还就车载娱乐系统安全策略的设计与实施提出了防御层级与策略架构，以及安全性测试与评估方法等建议，为提升车载娱乐系统的网络安全水平提供参考。

关键词：车载娱乐系统；网络安全；隐私保护

引言

随着汽车智能化和网联化的发展，车载娱乐系统已成为现代汽车不可或缺的重要组成部分[1]。然而，车载娱乐系统的广泛应用也带来了网络安全和隐私保护方面的诸多挑战。黑客攻击、数据泄露等安全事件频发，不仅威胁着车内乘员的信息安全，更可能对行车安全造成严重影响。因此如何构建完善的车载娱乐系统网络安全与隐私保护策略，成为汽车制造商和相关企业亟待解决的重要课题。

1 车载娱乐系统的网络安全现状与挑战

1.1 车载娱乐系统的网络安全漏洞分析，车载网络攻击的主要方式

由于车载娱乐系统与车辆的其他电子控制单元（ECU）紧密连接，一旦遭到恶意攻击，不仅会导致娱乐系统本身的功能失常，更可能危及整车的行驶安全。目前，车载娱乐系统存在的主要网络安全漏洞包括：操作系统层面的漏洞，如缓冲区溢出、权限提升等；应用程序层面的漏洞，如SQL注入、跨站脚本攻击等。

通信协议层面的漏洞，如CAN总线注入、TPMS欺骗等[2]。攻击者可以利用这些漏洞，通过USB接口、蓝牙、Wi-Fi等多种方式对车载娱乐系统发起攻击，实现远程控制、数据窃取、恶意代码植入等目的。同时车载娱乐系统与互联网的连接也为攻击者提供了可乘之机，使得车辆面临更大的网络安全风险。

1.2 信息安全与隐私保护的法规要求，车载娱乐系统的安全合规性问题

随着各国对信息安全和隐私保护的日益重视，车载娱乐系统也面临着日益严格的法规要求，这些法规对车载娱乐系统的数据收集、存储和使用提出了更高的合规性要求。然而，由于车载娱乐系统涉及的数据类型广泛，包括定位信息、驾驶行为数据、娱乐偏好等，如何在功能实现与隐私保护之间取得平衡，成为车企面临的重大挑战。车载娱乐系统作为汽车的一个子系统，其安全性也受到整车安全法规的约束。

2 车载娱乐系统的隐私保护技术与措施

2.1 数据加密技术在车载娱乐系统中的应用，隐私保护的技术手段

目前，车载娱乐系统常用的加密技术包括对称加密和非对称加密两大类。对称加密算法，如高级加密标准，具有计算速度快、资源消耗低等优点，特别适用于对海量数据进行加密保护。在对称加密的使用过程中，加密和解密双方共享相同的密钥，通过将明文数据与密钥进行复杂的数学运算，生成密文数据，从而实现数据的机密性保护[3]。而非对称加密算法，如RSA算法，则使用一对公私钥来实现加密和解密过程。公钥可以公开发布，用于对数据进行加密；私钥则由密钥持有者秘密保存，用于对数据进行解密。非对称加密虽然在计算效率上不如对称加密，但其独特的密钥管理方式，可以有效地解决密钥分发和管理的问题，提供更高的安全性。通过在车载娱乐系统的关键数据传输和存储环节，合理地应用对称加密和非对称加密技术，能够从根本上防止敏感数据被非法窃取和滥用为用户的隐私安全提供坚实保障。

除了数据加密技术外，车载娱乐系统还可以采用一系列其他技术手段来实现隐私保护。比如数据脱敏技术通过对原始数据进行转换和处理，在保留数据基本特征的同时，去除其中的敏感信息，使得脱敏后的数据即使被非法获取，也难以对用户隐私造成损害。具体的脱敏方法包括数据掩码、数据置换、数据加噪等，通过对敏感数据字段进行部分替换、重新组合或添加随机噪声，来实现数据的隐私保护。差分隐私技术也在车载娱乐系统的隐私保护中得到广泛应用。差分隐私通过在原始数据中引入随机噪声，使得任何一个数据记录的存在与

否，都不会对最终的统计分析结果产生显著影响，从而在保证数据可用性的同时，最大限度地保护了个体隐私。差分隐私技术不仅能够抵御常见的隐私攻击，如链接攻击和推理攻击，还能够提供严格的数学隐私保证，使得车载娱乐系统的隐私保护达到更高的安全标准。

2.2 用户身份验证与权限管理，防止未经授权的访问与数据泄露

为确保系统资源和敏感数据的访问安全，必须对每个试图接入系统的用户进行可靠且全面的身份认证。传统的身份验证方法如用户名和密码，虽然简单易行，但在安全性和便捷性方面存在诸多不足。密码等静态身份凭证容易被窃取、猜测或破解，一旦泄露，就会为非法访问和数据窃取敞开大门。因此车载娱乐系统应积极引入多因素身份认证机制，综合利用多种独立的认证要素，如生物特征（指纹、人脸、虹膜等）、物理令牌（智能卡、USB Key等）、行为特征（击键节奏、鼠标轨迹等）等，构建起更为可靠和安全的身份验证防线。通过要求用户提供他知道的（如密码）、他拥有的（如智能卡）和他自身的（如指纹）多重身份凭证，大大提高了身份假冒和非法访问的难度。同时车载娱乐系统还应支持灵活的认证策略，根据访问请求的安全等级、环境条件等因素，动态调整认证的强度和方式[4]。比如，对于一般性的娱乐功能访问，可采用相对简便的单因素认证；而对于涉及隐私数据和敏感操作的请求，则应启用更为严格的多因素认证。车载娱乐系统还需妥善处理身份凭证的生命周期管理，如何安全地生成、分发、存储、更新和注销用户的身份凭证，避免凭证被盗用、伪造或泄露也是身份验证机制设计中需要重点考虑的环节。

车载娱乐系统应该遵循权限最小化和职责分离原则，根据用户的角色、职责和需求，合理定义和分配系统资源、应用功能以及数据访问的权限。通过细粒度的权限控制，确保用户只能访问其工作所需的资源，而无法触及与其无关的敏感数据和关键功能，最大限度地减少内部误操作和权限滥用所造成的安全风险。同时系统还应该支持动态的权限管理，根据用户的行为、环境变化等因素，实时调整用户权限，比如当用户长时间未操作、离开车辆或进入可疑区域时，自动收回相关权限，待其重新通过身份验证后再恢复相应权限。针对不同层次的隐私数据，还需建立分级的数据访问控制体系[5]。将隐私数据划分为公开、内部、机密、绝密等不同安全级别，明确规定每一级别数据的访问权限分配、使用授权流程、访问行为审计等管理要求，并采取相应的技术措施，如数据加密、访问监控、数字水印等，有效控制隐私数据的可见性和可用性。权限管理还应与系统的运行监控和安全审计机制紧密结合，对用户的访问请求和操作行为进行全程记录和分析，及时发现可疑行为和非法操作，为事后追责和事件调查提供可靠的审计证据。

3 车载娱乐系统安全策略的设计与实施

3.1 安全防护策略的制定，车载娱乐系统的防御层级与策略架构

在硬件层面要选择安全可靠的芯片和元器件，采用安全启动、硬件加密等技术，确保系统从源头上防范恶意篡改和非法访问。在操作系统层面要采用安全增强型操作系统，并进行必要的安全加固，如关闭不必要的服务和端口，及时打补丁修复漏洞，严格控制系统权限和资源访问。在应用层面要遵循安全编码规范，采用安全的开发框架和工具，对关键代码进行安全审计并对应用程序进行全面的安全测试，及时修复发现的安全漏洞。同时还要重视数据安全，采用加密、脱敏等技术保护敏感数据，防止数据泄露和非法访问。在网络层面要采用安全通信协议，并部署必要的网络安全设备，如防火墙、入侵检测系统等，对网络通信进行监控和防护，抵御网络攻击和入侵行为。综合多个层面的安全防护措施，构建一个全方位、立体化的安全防御体系，从而最大限度地保障车载娱乐系统的安全。

除了技术层面的安全防护外，车载娱乐系统的安全策略还需要与汽车整体的安全策略相协调，形成一个统一、完善的安全防护框架。这就要求在安全策略的制定过程中要充分考虑车载娱乐系统在整车中的角色和地位，兼顾功能性、安全性、可用性等多个方面的平衡。同时还要建立健全的安全管理制度和流程，明确各部门和人员的安全职责，规范开发、测试、运维等各个环节的安全工作并定期开展安全培训和教育，提高全员的安全意识和技能。还需要与产业链上下游的合作伙伴建立良好的沟通协调机制，共享安全威胁情报，协同应对安全事件，构建汽车行业的综合安全生态。

3.2 安全性测试与评估方法，车载娱乐系统的漏洞扫描与修复机制

常用的安全性测试方法包括渗透测试、模糊测试、代码审计等，渗透测试是一种主动式的安全测试方法，通过模拟恶意攻击者的思维和行为，利用各种工具和技术，对系统进行全面的攻击测试，以发现系统在真实环境中可能存在的安全漏洞和薄弱环节。渗透测试通常分为外部测试和内部测试两种形式，外部测试主要针对系统的外部接口和服务进行测试，如网络通信接口、蓝牙接口、USB接口等；内部测试则主要针对系统内部的软

件模块和组件进行测试，如操作系统、中间件、应用程序等[6]。通过渗透测试可以全面评估系统抵御外部攻击和内部威胁的能力并根据测试结果制定针对性的安全加固措施。模糊测试是一种基于异常输入的安全测试方法，通过向系统发送大量的随机或半随机生成的异常数据，观察系统的响应和行为，以发现系统在处理非预期输入时可能出现的异常和崩溃。模糊测试可以有效地发现系统在边界条件和极端情况下的安全缺陷，如内存溢出、空指针引用、格式化字符串漏洞等。代码审计则是一种基于源代码分析的安全测试方法，通过人工或自动化工具对系统的源代码进行静态分析，检查代码中是否存在安全漏洞和编程错误，如注入漏洞、权限控制缺陷、加密算法使用不当等。

车载娱乐系统漏洞的有效修复是一项持续性的工作，需要建立完善的漏洞管理流程和机制，从漏洞的发现、报告、分析、验证到最终修复的全过程进行规范化管理。要建立畅通的漏洞报告渠道，鼓励安全探究人员、白帽黑客、用户等及时报告发现的系统漏洞，并建立漏洞奖励机制，激励社会各界共同参与到系统安全建设中来。对报告的漏洞进行严格的分析和验证，确定漏洞的真实性、影响范围、危害程度等并根据漏洞的风险等级，制定相应的修复策略和计划。漏洞修复需要遵循严格的变更管理流程，对修复方案进行可行性分析和安全性评估，并经过充分的测试验证，确保修复措施的有效性和系统的稳定性。随着社会发展步伐的不断加快，创新型人才逐步成为推动社会发展的重要动力。所以，教育教学要注重学生创造性思维的培养，为社会培育出更多实用型创新人才。漏洞修复过程中还需要与相关业务部门充分沟通和协调，最大限度地减少对系统正常运行和用户体验的影响。建立漏洞知识库和安全事件响应机制，对已知漏洞进行统一管理和跟踪并总结漏洞修复的经验教训，不断完善系统的安全防护能力。

结束语

车载娱乐系统的网络安全与隐私保护已经成为汽车产业的重要课题。汽车制造商需要与产业链上下游企业密切合作，遵循相关法律法规要求，采用先进的安全防护技术和策略，提升车载娱乐系统的安全防护能力。同时还要加强与白帽黑客等安全探究团体的合作，通过持续的安全性测试与评估，及时发现和修复系统漏洞，构建全面、动态、持续的安全防护体系。

参考文献

[1]三星携手高通助力高级车载信息娱乐与高级驾驶员辅助系统[J].汽车与配件,2024(17):20.

[2]孙德强,张俊仪,时瑞浩.车载信息娱乐系统发展及趋势研究[J].汽车电器,2024(6):39-41.

[3]赵文棣,黄红蓝,李豪,等.车载信息娱乐系统框架介绍及发展概述[J].汽车电器,2021(6):7-9.

[4]刘文滔,陈以.一种通用的车载信息娱乐系统防窜货系统方案设计与实现[J].桂林理工大学学报,2015(2):418-421.

[5]吴剑斌,张竞元,张凌浩.基于情境感知的车载信息娱乐系统交互设计研究[J].包装工程,2018,39(16):189-196.

[6]郝赓,毕腾飞.车载娱乐总成的静态电流分析[J].汽车电器,2020(1):42-44.