

面向智能汽车的信息安全漏洞评分模型

于海洋^{1,2}, 陈秀真^{1,2}, 马进^{1,2}, 周志洪^{1,2}, 侯书凝^{1,2}

(1. 上海交通大学网络安全技术研究院, 上海 200240;
2. 上海市信息安全综合管理技术重点实验室, 上海 200240)

摘要: 随着汽车智能化、网联化的发展, 汽车中集成了越来越多的电子器件, 数量庞大的硬件、固件和软件中隐藏着各种设计缺陷和漏洞, 这从根本上导致了智能汽车信息安全问题。大量汽车漏洞的披露, 严重影响了汽车安全, 制约了智能汽车的广泛应用。漏洞管理是降低漏洞危害、改善汽车安全的有效手段。在漏洞管理流程中, 漏洞评估是决定漏洞处置优先级的重要一环。但是, 现有的漏洞评分系统不能合理地评估智能汽车安全漏洞。为了解决智能汽车漏洞评估不合理的问题, 提出面向智能汽车的信息安全漏洞评分模型。基于通用漏洞评分系统(CVSS)漏洞评分原理, 根据智能汽车的特点, 优化了 CVSS 的攻击向量和攻击复杂度, 并添加了财产安全、隐私安全、功能安全和生命安全 4 个指标来刻画漏洞可能对智能汽车造成的影响; 结合机器学习的方法, 对 CVSS 评分公式参数进行了调整, 以使其更好地刻画智能汽车信息安全漏洞特点, 适应调整后的指标权重。通过实例评估和统计系统特征分布发现, 模型拥有更好的多样性和更稳定连续的特征分布, 表明模型可以更好地对不同漏洞进行评分; 并且基于模型评估得到的漏洞评分, 应用层次分析法给出整车脆弱性评估, 表征整车风险水平。所提模型相比现有模型可以更为合理地评价智能汽车中信息安全漏洞的严重程度, 科学地评估整车或者部分系统的安全风险, 为汽车漏洞的修复与加固提供依据。

关键词: 智能汽车; 通用漏洞评分系统; 漏洞评分; 风险评估; 非线性回归; 层次分析法

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2021096

Information security vulnerability scoring model for intelligent vehicles

YU Haiyang^{1,2}, CHEN Xiuzhen^{1,2}, MA Jin^{1,2}, ZHOU Zhihong^{1,2}, HOU Shuning^{1,2}

1. Institute of Cyber Science and Technology, Shanghai Jiao Tong University, Shanghai 200240, China
2. Shanghai Municipal Key Lab of Integrated Management Technology for Information Security, Shanghai 200240, China

Abstract: More and more electronic devices are integrated into the modern vehicles with the development of

收稿日期: 2021-06-11; 修回日期: 2021-08-12

通信作者: 陈秀真, chenxz@sjtu.edu.cn

基金项目: 国家自然科学基金联合基金(U2003206); 上海市工业强基专项(GYQJ-2018-3-03)

Foundation Items: The Joint Funds of the National Natural Science Foundation of China (U2003206), Shanghai industrial foundation project(GYQJ-2018-3-03)

引用格式: 于海洋, 陈秀真, 马进, 等. 面向智能汽车的信息安全漏洞评分模型[J]. 网络与信息安全学报, 2022, 8(1): 167-179.

Citation Format: YU H Y, CHEN X Z, MA J, et al. Information security vulnerability scoring model for intelligent vehicles[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 167-179.

intelligent vehicles. There are various design flaws and vulnerabilities hidden in a large number of hardware, firmware and software. Therefore, the vulnerabilities of intelligent vehicles have become the most important factor affecting the vehicle safety. The safety of vehicles is seriously affected by the disclosure of a large number of vulnerabilities, and the wide application of smart cars is also restricted. Vulnerability management is an effective method to reduce the risk of vulnerabilities and improve vehicle security. And vulnerability scoring is one the important step in vulnerability management procedure. However, current method have no capability assessing automotive vulnerabilities reasonably. In order to handle this problem, a vulnerability scoring model for intelligent vehicles was proposed, which was based on CVSS. The attack vector and attack complexity were optimized, and property security, privacy security, functional safety and life safety were added to characterize the possible impact of the vulnerabilities according to the characteristics of intelligent vehicles. With the machine learning method, the parameters in CVSS scoring formula were optimized to describe the characteristics of intelligent vehicle vulnerabilities and adapt to the adjusted and new added weights. It is found in case study and statistics that the diversity and distribution of the model are better than CVSS, which means the model can better score different vulnerabilities. And then AHP is used to evaluate the vulnerability of the whole vehicle based on the vulnerability score of the model, a score is given representing the risk level of whole vehicle. The proposed model can be used to evaluate the severity of information security vulnerabilities in intelligent vehicles and assess the security risks of the entire vehicle or part of the system reasonably, which can provide an evidence for fixing the vulnerabilities or reinforcing the entire vehicle.

Keywords: intelligent vehicle, CVSS, vulnerability scoring system, risk assessment, nonlinear regression, AHP

0 引言

智能汽车是国家近年来的重要战略发展布局之一^[1], 各大重点城市、互联网企业、安全公司均已经启动智能汽车行业的发展布局。对于智能汽车而言, 稳定性与安全性是至关重要的两个指标。然而, 由于汽车智能化、网联化程度的提高, 潜在信息安全问题急剧增多, 对稳定性和安全性造成了严重危害, 这成为影响智能汽车广泛应用的一个瓶颈。

智能汽车面临信息安全问题的根本原因在于汽车硬件、软件、协议的具体实现上或系统安全策略上存在缺陷, 智能汽车内部集成了数以万计的电子器件、运行了千万行以上的代码, 而且平均每千行代码就可能出现 15~50 个错误。在如此庞大的电子器件数量与代码量基数下, 智能汽车中必然存在众多严重的安全漏洞, 汽车漏洞已经成为影响汽车稳定性和安全性的关键因素。由于智能汽车的信息安全问题成为影响其广泛应用的瓶颈, 整车厂商、汽车零部件制造商等生产制造企业亟须了解生产的零部件或者整车产品存在的潜在安全风险与威胁, 需要将风险控制在合理的范围内, 提供更加安全可靠的产品。另外, 智能汽车的使用者需要对智能汽车的安全状况有一个

明确的认知, 特别是关系到生命安全的切身问题。无论是智能汽车生产方还是使用方, 都需要一种科学可信的方法来了解智能汽车安全状况, 这离不开智能汽车信息安全漏洞评估技术。

对于漏洞严重性的评估, 在传统信息安全领域中已经有被业界广泛接受的通用漏洞评分系统 (CVSS, common vulnerability scoring system)。但是由于智能汽车的特殊性, 汽车漏洞不仅影响智能汽车的正常驾驶功能, 还会对驾驶人员或乘客造成生命威胁, CVSS 不能够合理地评估汽车漏洞的严重性。因此, 在汽车信息安全领域亟须一种能够合理评价汽车漏洞严重性的评价系统。

本文基于主动防御的思想, 结合智能汽车信息安全漏洞的特殊性, 提出一种新型漏洞评分模型——面向智能汽车的信息安全漏洞评分模型 (VSMIV, information security vulnerability scoring model for intelligent vehicles)。系统采用与 CVSS 相同的使用方法, 通过权值确定和评分计算的方法进行汽车信息安全漏洞的评估, 具有较好的可用性, 并且添加的汽车信息安全相关指标能够较好地刻画漏洞对汽车安全的影响, 保证了模型的有效性, 使该系统可以对智能汽车中的信息安全漏洞严重性进行科学合理的评价, 为智能汽车信

息系统安全评估、漏洞修复与系统加固提供支撑。

如果没有特殊说明,本文提到的 CVSS 公式和评分方法均为 CVSS 3.0 版本的公式与评分方法。

1 相关工作

本文基于信息安全业界广泛接受的通用漏洞评分系统,研究面向智能汽车的信息安全漏洞评分模型,实现了智能汽车漏洞严重性的合理评价。下面给出与信息安全漏洞评估相关的一些研究工作。

Zhao 等^[2]提出了一种针对动态攻击的脆弱性评价方法,该方法包括两个层次的评价:漏洞级别的评估和系统级别的安全评估。漏洞级别的评估是基于 CVSS 的拓展评估方法,系统评估是基于自适应攻击图的评价方法。最后通过实验证明了方法的有效性,并且验证了在动态网络场景下具有更好的效果。

Keramati 等^[3]提出一种新型的漏洞评分系统,并考虑了时间等动态因素。该系统从漏洞可行性与漏洞影响两方面评价漏洞严重性,可用于安全的动态评估。与 CVSS 不同的是,该系统使用概率估计计算漏洞可行性,并考虑到了漏洞本身和时间的因素。最后,验证了该系统在评分的多样性和准确性两个方面比 CVSS 表现更好。

Li 等^[4]提出一种新型的安全框架来对云服务漏洞进行评分,并且开发了评分系统的原型,可以通过该系统原型获得漏洞排名,云服务提供商可以根据漏洞排名修复最关键的漏洞,并通过实例证明该系统在云服务漏洞评分方面比 CVSS 更为出色。

Liu 等^[5]提出一种新型的定量、定性漏洞评分系统,采用基于 CVSS 的漏洞评分方法,对漏洞影响度的生成与计算做了修改,使用基于规则的漏洞影响度评价方法,给出基于规则的漏洞影响度的评级表,并进一步根据评级表确定漏洞影响度。定量的方法将漏洞评级作为评分数值,与漏洞可行性分值代入评分公式运算得到。漏洞可行性分值与 CVSS 的可行性分值计算方式相同,并且该模型在 1999 年到 2008 年的漏洞数据集上取得了较好的检验效果。

Spanos 等^[6]提出一种基于 CVSS 的新型定量

评分系统 WIVSS,其影响度计算基于 CVSS 影响度的计算方法并对权值做了改进。使用基于规则的影响度指标权值生成方法,分析指标关系获得对应规则,根据规则进行数学近似得到评分指标的权值,通过各个影响度指标相加得到影响度分值,再将漏洞可行性分值代入 CVSS 2.0 版本的公式中进行最终漏洞评分的计算。

Ur-Rehman 等^[7-8]提出了一种基于 CVSS 的复杂信息系统拓展漏洞评分模型,该改进模型根据物联网与传统网络之间的差异,修改了攻击向量与攻击复杂度指标,并且添加了人身安全指标,该指标体现了物联网特点,能够更好地评价物联网漏洞。添加的各个指标权值的确定依据是实验室分析和过去的经验,通过对 CVSS 公式简单扩展实现了漏洞的评分。在此基础上,他们又提出了一种基于 CVSS 的复杂工业控制系统拓展漏洞评分系统,在物联网指标的基础上添加了过程可视性、过程控制和过程监控等过程安全相关的指标。进一步使用贝叶斯信念网络确定对应的指标权值,并对 CVSS 公式做了修改扩展得到漏洞评分计算公式。

总体来说,一方面,目前的安全漏洞评分模型主要是针对特定应用领域,包括云服务、工控网络等,现有的漏洞评价方案不能直接应用于汽车漏洞严重性的评估,通用的漏洞评价系统在汽车安全领域无法合理地对汽车漏洞进行评价。另一方面,现有的漏洞评价系统指标仅为安全相关属性,漏洞修复和安全加固涉及多个方面,仅有体现安全影响的漏洞评分是不够的。

在此背景下,针对汽车信息安全领域缺乏一种有效评估汽车漏洞方法的现状,本文提出一种面向智能汽车的信息安全漏洞评分模型,用于合理评价汽车信息安全漏洞的严重性。

2 VSMIV 评分模型

智能汽车的信息安全威胁不仅会影响信息的保密性、完整性和可用性,还会带来隐私泄露,如地理位置信息、用户行驶记录等,因此,本文结合通用漏洞评分系统的工作原理^[9],参考《道路车辆功能安全》国际标准 ISO 26262^[10]、车辆电子安全入侵防护应用(EVITA, E-safety vehicle

intrusion protected applications)^[11]和 Den-Hartog 等^[12]对汽车安全与隐私应用研究,提出智能汽车漏洞评分模型(VSMIV)。

面向智能汽车的信息安全漏洞评分模型如图 1 所示,评分模型由两部分构成,可行性评分部分和影响评分部分:可行性评分部分评估漏洞被利用的难度,包含攻击向量、攻击复杂度、权限要求和用户交互 4 个方面的指标,可以通过可行性计算公式得出;影响评分部分评估漏洞被利用后可能造成的影响,由机密性、完整性、可用性和隐私安全、财产安全、功能安全、生命安全指标通过影响计算公式得出漏洞影响分值。漏洞影响严重度的最终评分 S_{ICV} 由可行性分值和影响分值联合得出,具体的计算如式(1)所示。

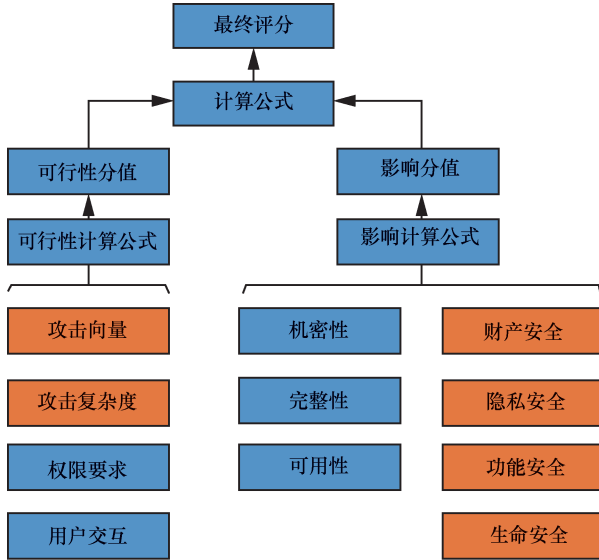


图 1 面向智能汽车的信息安全漏洞评分模型
Figure 1 Information security vulnerability scoring model for intelligent vehicle

$$S_{ICV} = \begin{cases} 0, S_i \leq 0 \\ \text{Roundup}(\text{Min}[(S_i + S_e) + 0.2, 10]), S_i > 0, \\ \text{scope} = \text{Unchanged} \\ \text{Roundup}(\text{Min}[1.08 \cdot (S_i + S_e) + 0.2, 10]), S_i > 0, \\ \text{scope} = \text{Changed} \end{cases} \quad (1)$$

其中, S_i 和 S_e 分别表示漏洞影响分值和漏洞可行性分值, scope 表示漏洞的影响范围,用来评价某个易受攻击组件中的漏洞是否影响其安全范围以

外组件中的资源,如位于车载娱乐系统的漏洞,被利用后可以影响到车内 CAN 总线控制车辆行为,这就是发生了影响范围的变化。如式(1)所示,漏洞的影响分值 S_i 小于等于 0 时,代表在当前评价指标下该漏洞不会产生危害,故最终评分为 0。当漏洞的影响分值 S_i 大于 0 且影响范围不发生改变,漏洞影响严重度的最终评分 S_{ICV} 取 10 与 S_i 、 S_e 之和加上偏差常量 0.2 的最小值;当漏洞的影响分值大于 0 且影响范围发生改变时,此时漏洞可能造成的危害比范围不发生改变时大,参照 CVSS 影响范围改变对漏洞评分的影响,漏洞影响严重度的最终评分 S_{ICV} 取 10 和 $1.08 \cdot (S_i + S_e) + 0.2$ 的最小值,因为漏洞评分的最高值为 10。当漏洞影响范围改变时,造成的危害会更为严重,借鉴 CVSS 对于漏洞影响范围的调整权值,此处使用 1.08 作为权值对漏洞影响分值进行调整。

在式(1)得出最终的漏洞评分之前,式(1)中的小数计算依赖具体实现算法的小数精度,式(1)中的 Roundup 函数实现小数向上取整,该函数保留的数据精度是小数点后 5 位。如 Roundup(1.200 03)的结果是 1.3,最小评分单位为 0.1,所以最后结果会保留到 1 位小数。在此处没有采用常用的四舍五入取整的方式,因为四舍五入会舍弃不大于 5 的部分。这会导致部分漏洞的最终评分低于其未取整评分,在安全领域这是要尽量避免的;向上取整得到的评分总是会大于等于其未取整评分,而高估漏洞评分相对而言是比较安全的,所以在此处的小数处理选择了向上取整的方式。

2.1 可行性分值

可行性分值 S_e 用于刻画漏洞被利用的可行性程度,评价指标由攻击向量 E_{av} 、攻击复杂度 E_{ac} 、权限要求 E_{pr} 和用户交互 E_{ui} 组成。可行性分值 S_e 具体的计算式为

$$S_e = 7.57 \cdot E_{av} \cdot E_{ac} \cdot E_{pr} \cdot E_{ui} \quad (2)$$

其中,攻击向量 $E_{av} = \{\text{网络 } N, \text{远程访问 } R_v, \text{相邻网络 } A, \text{近程访问 } L_v, \text{本地网络 } L, \text{物理接触 } P, \text{物理访问 } P_v\}$ 描述了漏洞被利用的路径或手段,7.57 是可行性的权值。此处,新的汽车攻击向量为远程访问、近程访问和物理访问值(R_v 、 L_v 、 P_v)。与传统设备相比,智能汽车远程访问比网络访问困难,但比邻接网络简单,故其权值 $A < R_v < N$ 。

汽车近程访问主要是指蓝牙、射频等近场通信技术，与 CVSS 攻击向量中相邻网络的定义较为相似，故近程访问值取 $S_i=A$ 。物理访问汽车比物理访问计算机更为容易，汽车通常停放在室外或者停车场，而计算机通常存放在机房，故 $P_v>P$ 。智能汽车相关的漏洞可能涉及远程服务器漏洞、通信协议漏洞等方面，所以此处保留与 CVSS 相同的攻击向量，与智能汽车攻击向量组成最终的攻击向量集。并且，规定在描述智能汽车漏洞的攻击向量时，应该优先考虑智能汽车专用的攻击向量。

攻击复杂度描述了漏洞被利用的复杂程度。其取值可为低、中、高、极高 4 种复杂程度，分别对应 L 、 M 、 H 、 H_v 。其中，复杂程度中等和极高是智能汽车专用的攻击复杂程度。具体分级标准如表 1 所示。

权限要求 E_{pr} 描述了漏洞被利用时的权限要求，分为高、低、无 3 种情形，在漏洞影响范围改变时该指标的高、低两种类型取值会发生改变。无权限要求指攻击者在攻击前是未授权状态，不需要任何文件访问权限或系统设置权限即可发起攻击。低权限要求指攻击者需要基本用户权限来访问用户文件或者配置，从而达成攻击。高权限要求指攻击者需要对受攻击目标或组件拥有管理或控制权限。

用户交互 E_{ui} 描述了在漏洞被利用时是否需要用户交互操作，该指标包含需要和不需要两种类型。

2.2 影响分值

影响分值 S_i 用于描述漏洞被利用后对系统造成的影响与损失，评价指标从两个不同的视角出发，一个是对信息安全三要素造成的危害，具体包括机密性 I_c 、完整性 I_i 和可用性 I_a ；另一个是

对智能汽车安全要素造成的危害，智能汽车安全要素包含生命安全 I_{hsi} 、财产安全 I_{pl} 、功能安全 I_f 和隐私安全 I_{ps} 。影响分值的具体计算公式如式(3)所示。

$$S_i = \begin{cases} 7.08 \cdot ISS_{scope=Unchanged} \\ 7.53 \cdot (ISS - 0.029) - 3.24 \cdot (ISS - 0.02)^{15}, & (3) \\ scope=Changed \end{cases}$$

与 CVSS 直接使用安全三要素 I_c 、 I_i 、 I_a 计算得到影响分值 ISS 不同，式(4)、式(5)首先使用信息安全三要素 I_c 、 I_i 、 I_a 和智能汽车安全要素 I_{hsi} 、 I_{pl} 、 I_f 、 I_{ps} 计算得出信息安全影响值 ISS_{SEC} 和智能汽车安全影响值 ISS_{ICV} 。然后，式(6)通过信息安全影响值 ISS_{SEC} 和智能汽车安全影响值 ISS_{ICV} 加权计算得到影响分值 ISS。其中 0.6 和 0.4 是分别赋予智能汽车安全影响值 ISS_{ICV} 和信息安全影响值 ISS_{SEC} 的权值，代表在评估漏洞影响时智能汽车安全影响和信息安全影响两部分所占的权重大小。

$$ISS_{ICV} = 1 - [(1 - I_{hsi}) \cdot (1 - I_{pl}) \cdot (1 - I_f) \cdot (1 - I_{ps})] \quad (4)$$

$$ISS_{SEC} = 1 - [(1 - I_c) \cdot (1 - I_i) \cdot (1 - I_a)] \quad (5)$$

$$ISS = 0.6 \cdot ISS_{ICV} + 0.4 \cdot ISS_{SEC} \quad (6)$$

从这两类指标评估一个智能汽车漏洞的影响，一方面，从后果严重性上来说，智能汽车安全指标包含漏洞对生命安全的损害，此类指标相比信息安全指标更重要，应该分配更高的权值；另一方面，本模型主要评估智能汽车信息安全漏洞，在权值分配时应该更加偏向智能汽车安全，所以最终给智能汽车安全指标分配了 0.6 的权值，而信息安全指标分配了 0.4 的权值。

在 CVSS 中，只考虑信息安全三要素，直接将信息安全影响值 ISS_{SEC} 作为影响分值 ISS 进行

表 1 攻击复杂度分级标准
Table 1 Attack complexity scoring standard

攻击复杂度等级	攻击复杂度分级说明
极高	攻击难度极大或要求苛刻的攻击，需要达成突破防护措施、试验获得目标环境中竞态条件等多种条件后才有可能成功，几乎很难成功
高	需要满足一定条件才可以达成攻击，且限制条件较为严格，如搭建目标环境、中间人攻击、准备特定脚本或工具等条件中的一条或多条
中	需要满足一定条件才可以达成攻击，但限制条件较为简单，如获取目标环境信息等
低	不需要满足特定条件，攻击能够重复获得可预期的成果

后续计算, 而此处加权计算综合考虑到了信息安全要素和智能汽车因素, 其权值分配根据实验分析和过往经验得出。

信息安全影响分值具体评价指标是机密性、完整性和可用性, 每个指标对应应有高、低、无 3 个等级。每个等级分别表征该漏洞对相应信息安全要素的损害程度, 具体分级标准如表 2 所示。

智能汽车影响分值具体评价指标由生命安全、财产安全、功能安全和隐私安全 4 个指标组成。每个指标对应应有高、低、无 3 个等级, 每个等级分别表征该漏洞对相应指标的威胁程度, 具体分级标准如表 3 所示。漏洞可行性指标和影响指标对应的不同评级取值如表 4 所示, 该取值参考 Ur-Rehman 等^[7-8]的取值结合实验分析和过往的经验得出。其中, 影响范围的取值为改变 C 和未改变 U, 该项指标会影响式(1)和式(3), 也就是漏洞影响分值计算公式和最终评分公式的计算。如式(3)中, 如果影响范围未改变影响分值, 则 S_i 计算取 7.08-ISS, 如果影响范围改变, 则 S_i 计算取 $7.53 \cdot (ISS - 0.029) - 3.24 \cdot (ISS - 0.02)$ ¹⁵。

表 4 评分指标权值
Table 4 Weight of scoring index

指标名称	指标分级	可能取值
攻击向量	[N,R _v ,A,L _v ,L,P _v ,P]	[0.85,0.77,0.62,0.62,0.55,0.44,0.2]
攻击复杂度	[L,M _v ,H,H _v]	[0.77,0.44,0.44,0.2]
权限要求	[N,L,H]	[0.85,0.62(0.68),0.27(0.5)]
用户交互	[N,R]	[0.85,0.62]
影响范围	[U,C]	[U,C]
机密性	[H,L,N]	[0.56,0.22,0]
完整性	[H,L,N]	[0.56,0.22,0]
可用性	[H,L,N]	[0.56,0.22,0]
生命安全	[H,L,N]	[0.97,0.44,0]
财产安全	[H,L,N]	[0.56,0.22,0]
隐私安全	[H,L,N]	[0.56,0.22,0]
功能安全	[H,L,N]	[0.56,0.22,0]

评价指标的各项要素根据其关键点进行区分和评定, 如完整性和可用性的区分, 完整性侧重于数据未被篡改, 数据是可靠且正确的; 可用性侧重于评价合法用户能否对系统或者资源正常访

表 2 机密性、完整性、可用性指标分级标准
Table 2 Confidentiality, Integrity and Availability scoring standard

等级	机密性	完整性	可用性
无	不会对机密性造成危害	不会对完整性造成危害	不会对可用性造成危害
低	通过漏洞会获得某些受限信息的访问, 但攻击者无法控制获取的信息, 或者获取信息的数量或种类受到限制, 不会对部件造成直接的严重的影响	通过漏洞可以修改数据, 但是攻击者无法控制修改的结果, 或者修改的数量有限, 不会对部件造成直接的严重的影响	漏洞会造成性能降低或资源可用性暂时中断, 但是即使重复利用该漏洞, 攻击者也不能完全使该服务不可用。要么资源始终部分可用, 要么部分时间完全可用, 不会对部件造成直接的严重后果
高	完全丧失机密性, 受影响部件中的所有资源都泄露给攻击者, 或者只泄露部分受限信息, 但是所公开的信息会对部件机密性有直接的严重的后果	完全丧失完整性, 攻击者能够修改部件任何文件, 或者只能修改部分文件, 但会对部件造成直接的严重的后果	攻击者能够使受影响组件拒绝服务, 导致可用性完全丧失

表 3 生命安全、财产安全、功能安全和隐私安全指标分级标准
Table 3 Human safety index, Property security, Functional safety and Privacy security scoring standard

等级	生命安全	财产安全	功能安全	隐私安全
无	不会对生命安全造成危害	不会对财产安全造成危害	不会对功能安全造成危害	不会对隐私安全造成危害
低	漏洞会对关键部件、关键系统造成影响, 或者影响安全装置正常工作, 对生命安全有间接影响, 但是不会对生命安全造成直接的严重的影响	漏洞会导致间接、相对较小财产损失, 不会对财产安全造成直接的严重的影响	漏洞会使部分功能受损或者暂时不可用, 但是不会对车辆关键功能造成直接的严重的影响	通过漏洞会获得某些隐私信息的访问, 但攻击者无法控制获取的信息, 或者获取信息的数量或种类受到限制, 不会对隐私安全造成直接的严重的影响
高	漏洞对关键部件或关键系统造成严重影响, 对安全装置有严重危害, 或对生命安全造成直接的严重的影响	漏洞会导致重大财产损失, 对财产安全造成直接的严重的影响	漏洞会使功能不可用, 或者关键功能受损并对车辆关键功能造成直接的严重的影响	通过漏洞会获得全部隐私信息, 或者获得部分隐私, 但是泄露的隐私信息对隐私安全有直接的严重的后果

问。例如，CVE-2019-9493 使用固定管理员凭证后可以获得汽车的控制权限，远程进行车辆锁定，损害了可用性，但并未对完整性造成损害。

2.3 基于层次分析法的整车脆弱性评估

层次分析法(AHP, analytic hierarchy process)是将复杂问题分解为若干层次的准则和指标，定性与定量结合的决策分析方法^[13]。现有研究已经成功将层次分析法应用于网络安全风险评估^[14-15]和车载系统安全评估方面^[16]。本节参考现有研究成果，基于层次分析法提出一种整车脆弱性评估方法，以攻击面、系统安全和数据安全为准则建立层次化结构模型，如图2所示。

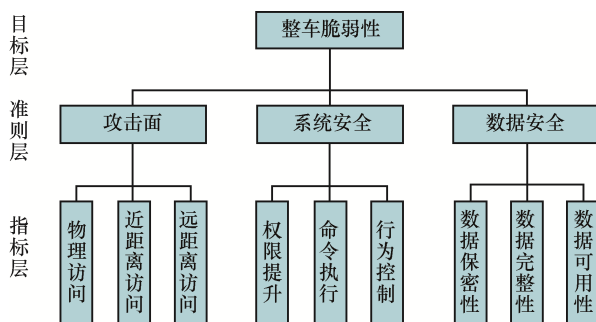


图2 整车脆弱性评估层次结构模型
Figure 2 Hierarchical model of vehicle vulnerability evaluation

以准则层中的攻击面、系统安全和数据安全为基础，建立指标层。攻击面包括物理访问、近距离访问和远距离访问；系统安全包括权限提升、命令执行和行为控制；数据安全包括数据保密性、数据完整性和数据可用性。

攻击面、系统安全和数据安全构成整车脆弱性评估的准则层。其中，攻击面描述整车通过不同途径被攻击的可能性，系统安全和数据安全描述整车遭受攻击后受到影响的方面。例如，CVE-2019-13582 通过 Wi-Fi 连接可以向 Wi-Fi 模块植入恶意代码或者造成该模块拒绝服务。该漏洞通过 Wi-Fi 发起攻击，Wi-Fi 属于攻击面的近距离访问，植入的恶意代码属于系统安全的命令执行，拒绝服务属于系统安全的行为控制，故该漏洞可以对攻击面的近距离访问指标、系统安全的命令执行指标和行为控制指标造成影响。

参考文献[16]中层次分析法的九分位的相对重要比例标度和公式计算得到判断矩阵和指标综合权重 W ，具体如图3~图6所示。

	攻击面	系统安全	数据安全
攻击面	1	1/3	5
系统安全	3	1	3
数据安全	1/5	1/3	1

图3 准则层对目标层的判断矩阵
Figure 3 Judgment matrix of criterion layer to target layer

	物理访问	近距离访问	远距离访问
物理访问	1	3	5
近距离访问	1/3	1	5
远距离访问	1/5	1/5	1

图4 指标层对准则层中攻击面的判断矩阵
Figure 4 Judgment matrix of attack surface in index layer to criterion layer

	权限提升	命令执行	行为控制
权限提升	1	1/2	1/5
命令执行	2	1	1/5
行为控制	5	5	1

图5 指标层对准则层中系统安全的判断矩阵
Figure 5 Judgment matrix of system security in index layer to criterion layer

	保密性	完整性	可用性
保密性	1	2	3
完整性	1/2	1	2
可用性	1/3	1/2	1

图6 指标层对准则层中数据安全的判断矩阵
Figure 6 Judgment matrix of data security in index layer to criterion layer

通过判断矩阵可以计算得出各项指标的综合权重，首先需要获得各个判断矩阵的权重矩阵。以准则层对目标层的判断矩阵 W_c 为例，获得权重矩阵的步骤为：

- 1) 判断矩阵列归一化；
- 2) 列归一化后的矩阵行求和；
- 3) 将得到的行求和再次归一化。

可以通过相同的方法得到指标层的权重矩阵：指标层对于攻击面的权重矩阵 W_{as} ，指标层对于系统安全的权重矩阵 W_{ss} ，指标层对于数据安全的权重矩阵 W_{ds} 。将权重矩阵扩充为 1×9 的权重向量，具体扩充方式如下。

$$\begin{cases} W_{as} = (W_1^{as}, W_2^{as}, W_3^{as}, 0, 0, 0, 0, 0, 0) \\ W_{ss} = (0, 0, 0, W_1^{ss}, W_2^{ss}, W_3^{ss}, 0, 0, 0) \\ W_{ds} = (0, 0, 0, 0, 0, 0, W_1^{ds}, W_2^{ds}, W_3^{ds}) \end{cases} \quad (7)$$

由指标层权重矩阵获得指标层对准则层的权重矩阵 W_{zz} , 具体公式如下。

$$W_{zz} = (W_{as}^T, W_{ss}^T, W_{ds}^T)^T \quad (8)$$

获得准则层对目标层的权重矩阵和指标层对准则层的权重矩阵后, 即可计算综合权重矩阵 W 。

$$W = W_c^T \times W_{zz} \quad (9)$$

获得综合权重后, 通过漏洞评估获得各项指标的评分, 即可计算整车脆弱性指标 S_c 。漏洞评估规则是如果该项指标能被漏洞影响则取该漏洞评分, 被多个漏洞影响则取最高分值。各项指标的取值向量为 $Z=(Z_1, Z_2, \dots, Z_9)$, S_c 的计算公式如下。

$$S_c = Z \times W^T \quad (10)$$

获得的整车脆弱性指标范围是从 0 到 10, 数值越大说明整车安全性越低, 安全隐患越大。

3 基于非线性回归的公式参数拟合

各项指标权值的选取参考 CVSS 和 Ur-Rehman 等^[7-8]在工控系统中模型的权值, 模型公式是参考 CVSS 的计算公式, 来自工控系统和传统网络的指标权值和针对传统网络的计算公式并不能体现智能汽车漏洞的特点。因此, 参考 CVSS 建立思路, 使用智能汽车漏洞数据对公式进行拟合。为了简化问题, 使用 CVSS 原本的公式不变, 仅对其中参数进行调整。于是, 本文模型结合机器学习采用非线性回归的方法对 CVSS 公式中的权值进行调整。

3.1 模型建立

对收集到的智能汽车漏洞进行专家评分, 获得严重等级和评分, 然后使用机器学习方式对参数进行拟合, 参数拟合的过程可以建模为非线性回归的过程。

$$y = f(X; w, b) \quad (11)$$

本文将式(1)~式(6)作为模型 f , 选择式(2)和式(3)中系数[7.08, 7.53, 3.24, 7.57]位置所在参数, 加上式(1)中的偏差 0.2, 共 5 个待训练参数。

模型的输入为漏洞的各项指标 X , 当前权值 w 和当前偏差 b 。 w 和 b 的初始值取[6.42, 7.52, 3.25,

8.22]和 0, 该初始值下的模型公式是 CVSS 的原始公式。模型的输出即对于当前漏洞输入的各项指标 X 所对应的预测评分 y 。

智能汽车漏洞数据是收集的不同车型、车内组件和芯片的漏洞, 数据集大小为 223, 将存在异常值以及缺失值的数据去除之后数据集大小为 219, 获得输入特征和标签, 以 CVE-2020-29440 为例, 数据格式为[0.55, 0.77, 0.85, 0.85, 6.42, 0, 0.56, 0, 0.56, 0, 0.56, 0.97, 8.5]。模型输出为评分预测值 y , 输入特征有 11 个, 具体为攻击向量 av 、攻击复杂度 ac 、权限要求 pr 、用户交互 ui 、影响范围 s 、机密性 c 、完整性 i 、可用性 a 、财产安全 pl 、隐私安全 ps 、功能安全 f 和生命安全 hsi 。其中, 影响范围 s 对应的数值 6.42 仅作为范围是否改变的标识, 不参与训练。

损失函数和优化函数的定义如下。损失函数用来评价当前参数下预测值和真实值之间的差距, 优化函数需要利用损失值对模型参数进行优化, 以达到更低的损失值, 获得更好的拟合效果。这里使用均方误差函数进行损失计算, 优化函数使用 Adam 函数。

3.2 模型训练与训练结果

设置学习率 lr 为 0.001, $epoch$ 为 100, Adam 算法的 $\beta_1=0.9$, $\beta_2=0.999$, $\epsilon=1 \times 10^{-8}$ 。

训练完成之后, 模型已经收敛, 损失函数的损失值变化小于 0.000 1, 并且漏洞严重等级准确率达到 80%以上。漏洞严重等级准确率是通过在当前参数下预测值 y 和专家评分的真实值标签落在相同的严重等级区间内的样本计算得到的, 训练结果如表 5 所示。

表 5 模型训练结果
Table 5 Results of the model training

参数	数值
损失值	0.298 290
严重等级准确率	0.831 050 22
w	7.077 953
	7.524 998 7
	3.233 344 67
	7.561 943 5
b	0.198 000 04

4 实验测试与结果分析

为了测试本文提出漏洞评分方法的有效性,选取智能汽车领域的 10 个典型漏洞进行分析测试,从漏洞评分的合理性以及漏洞评分的分布两个方面来评价所提算法的效果。并且在本节最后应用层次分析法对特斯拉 Model X 进行整车脆弱性评估。

验证有效性所选 10 个典型漏洞的简要描述如表 6 所示。

4.1 漏洞评分分析

如表 7、表 8 所示,给出所选漏洞在 VSMIV 评分模型下的漏洞各指标取值,使用表中的权值,代入 VSMIV 公式即可得到每个漏洞的评分分值。

具体分值如表 9 所示,其中除了由 VSMIV 评分获得漏洞评分外,还包括通用漏洞评分系统 CVSS、基于 CVSS 的工控网络评分系统 CVSS_{IOT}^[7-8]。CVSS_{IOT} 是在 CVSS 基础上兼容工业控制系统并做优化得到的评分模型,是基于 CVSS 面向其他环境下拓展的比较有代表性的模型。

表 6 漏洞描述
Table 6 Description of vulnerabilities

CVE 漏洞编号	漏洞描述	漏洞影响后果
CVE-2016-2354	蓝牙不用 PIN 码就可以配对,远端未授权攻击者可以发送任意 CAN 消息	影响车辆刹车和驾驶功能
CVE-2017-14937	消息处理函数存在权限提升漏洞,攻击者可以注入恶意命令	安全气囊在正常状态下爆开,引发事故
CVE-2017-9647	TCU 模块中代码对未知输入处理不当,可能造成内存损坏	自动变速箱异常,影响驾驶功能
CVE-2018-18071	人车交互 App 应用存在弱密码验证漏洞,可被中间人攻击	车主信息遭到泄露,远程控制车辆
CVE-2018-18203	车载信息娱乐系统中未签名文件系统映像可以通过有效性检查,更新机制可能使攻击者重写其固件	攻击者作为根用户执行恶意代码或安装恶意软件
CVE-2018-9318	车载信息娱乐系统对未知输入处理不当,攻击者可通过代码注入提升权限	引起信息泄露和恶意报文注入
CVE-2019-12797	蓝牙 PIN 模块存在固定管理员凭证,远端未授权攻击者可以绕过身份认证	蓝牙信息泄露,可向 OBD 发送任意命令
CVE-2019-13582	Wi-Fi 模块对未知输入处理不当,可能造成内存损坏	Wi-Fi 模块被植入恶意代码或受到拒绝服务攻击
CVE-2019-9493	人车交互 App 应用存在固定管理员凭证,远端未授权攻击者可以发送命令查询数据	车辆位置信息被盗取,获得对车辆的物理访问
CVE-2019-9977	车载信息娱乐系统对未知输入处理不当,攻击者可通过代码注入提升权限	车载信息娱乐系统被控制,功能出现异常并可能在 CAN 总线中发包

表 7 漏洞可行性指标权值
Table 7 Weight of vulnerability exploitability index

漏洞名称	攻击向量	攻击复杂度	权限要求	用户交互	影响范围
CVE-2016-2354	0.62	0.77	0.27	0.85	C
CVE-2017-14937	0.62	0.44	0.62	0.85	U
CVE-2017-9647	0.44	0.77	0.62	0.85	C
CVE-2018-18071	0.85	0.77	0.27	0.85	U
CVE-2018-18203	0.44	0.44	0.27	0.85	U
CVE-2018-9318	0.62	0.77	0.27	0.85	U
CVE-2019-12797	0.85	0.77	0.27	0.85	C
CVE-2019-13582	0.85	0.77	0.27	0.85	U
CVE-2019-9493	0.85	0.77	0.27	0.85	U
CVE-2019-9977	0.85	0.77	0.27	0.62	C

表 8 漏洞影响指标权值
Table 8 Weight of vulnerability impact index

漏洞名称	机密性	完整性	可用性	生命安全	财产安全	隐私安全	功能安全
CVE-2016-2354	0.56	0.56	0.56	0.97	0.56	0.56	0.56
CVE-2017-14937	0.56	0	0	0.97	0.44	0	0.44
CVE-2017-9647	0.56	0.56	0.56	0.97	0.44	0.44	0.56
CVE-2018-18071	0.56	0	0	0	0.56	0.56	0
CVE-2018-18203	0.56	0.56	0.56	0.44	0.44	0.56	0.56
CVE-2018-9318	0.56	0.56	0.56	0	0	0.56	0.44
CVE-2019-12797	0.56	0.56	0.56	0.97	0	0	0.56
CVE-2019-13582	0.56	0.56	0.56	0	0.44	0.44	0.56
CVE-2019-9493	0.56	0.56	0.56	0	0.56	0.56	0
CVE-2019-9977	0.56	0.56	0.56	0.97	0.44	0.56	0.56

表 9 CVSS、CVSS_{IoT} 与 VSMIV 评分比较
Table 9 Comparison of CVSS, CVSS_{IoT} and VSMIV

漏洞编号	CVSS	CVSS _{IoT}	VSMIV
CVE-2016-2354	8.8	7.9	9.7
CVE-2017-14937	4.7	6.9	7.0
CVE-2017-9647	6.6	8.5	7.7
CVE-2018-18071	7.5	4.9	8.9
CVE-2018-18203	6.4	6.3	7.2
CVE-2018-9318	9.8	7.2	9.2
CVE-2019-12797	9.8	8.3	10.0
CVE-2019-13582	9.8	7.2	9.5
CVE-2019-9493	9.8	7.2	9.9
CVE-2019-9977	8.8	7.9	9.7

由具体漏洞描述可知,属于传统安全漏洞,而且不涉及车辆驾驶功能和威胁人身安全的漏洞有:编号为 CVE-2018-18203 的固件升级漏洞,编号为 CVE-2018-9318 的提权漏洞,可以导致恶意代码注入和 Wi-Fi 拒绝服务的漏洞 CVE-2019-13582。VSMIV 对于此类漏洞评分稍有降低,而对于涉及车辆驾驶功能和威胁人身安全的漏洞评分,比 CVSS 评分高。

(1) VSMIV 对于传统安全漏洞的评分

如表 9 所示,VSMIV 对于此类传统漏洞评分整体有降低,而且在合理的范围内,如漏洞 CVE-2019-13582 和漏洞 CVE-2018-9318 分别由 9.8 下降到 9.5 和 9.2。漏洞 CVE-2018-9318 评分下降的原因是在新增的评价指标中不会损害人身

安全和造成严重的经济损失,仅会对隐私指标造成影响,导致信息泄露。另外,其中评分上升的特例是漏洞 CVE-2018-18203,其评分 7.2 相比 CVSS 评分 6.4 有所提升,是因为该漏洞位于车载信息娱乐系统,属于关键系统漏洞。

(2) VSMIV 对于涉及车辆驾驶功能和人身安全漏洞的评分

车载信息娱乐系统相关的漏洞在本文模型下的评分较 CVSS 中的评分多数提升了一个威胁等级。车载信息娱乐系统被控制执行任意命令,在车辆系统中会引起比传统 IT 系统更为严重的后果,部分车载信息娱乐系统甚至可以直接与 CAN 总线通信。因此,车载信息娱乐系统属于能够影响到车辆驾驶功能和人身安全的关键系统,该系统相关的漏洞具有更高的危害,应该得到更高的评分,最终 VSMIV 评分的结果与预测一致。

除了车载信息娱乐系统相关漏洞,涉及驾驶功能的漏洞和能够控制 CAN 总线的漏洞普遍比 CVSS 给出的评分高。

(3) CVSS_{IoT} 对于传统安全漏洞的评分

CVSS_{IoT} 模型对于此类 4 个传统安全漏洞的评分,普遍下降且下降幅度较大,该模型将漏洞对人身安全的威胁纳入考查指标,然而此类 4 个漏洞均不涉及威胁生命安全。虽然不涉及生命安全,但是可以给攻击者后续攻击提供良好的信息支撑或立足点。因此,该模型评分给出的漏洞评分过低,无法正常体现漏洞的危害性。

(4) CVSS_{IOT} 对于汽车安全漏洞的评分

除属于传统安全的4个漏洞之外,其余漏洞相较于 CVSS 评分均有不同程度的上升。而在 CVSS_{IOT} 模型下的评分则是普遍下降,其中漏洞 CVE-2018-18071, CVSS_{IOT} 模型仅能根据漏洞造成的隐私泄露来评价该漏洞,无法评价远程控制车辆可能造成的危害,因此对于该漏洞的评分由 CVSS 的 7.5 降到 4.9。CVE-2017-14937 和 CVE-2017-9647 评分则有所上升,具体原因是两漏洞原始评分均较低,但都与人身安全相关,故该模型给出了相比 CVSS 较高的评分。

(5) 评分整体稳定性

整体来看, CVSS_{IOT} 能够在一定限度上评价汽车漏洞的威胁,但是由于其评价指标过于单一,导致该指标会大幅影响到漏洞的评分,相比本文模型, CVSS_{IOT} 评分与 CVSS 评分总体差距较大,无法保证评分的相对稳定性。本文模型新增的生命安全、财产安全、隐私安全和功能安全指标可以将多个因素考虑在内,更加合理地评价汽车漏洞可能对智能汽车或相关人员造成的影响,并且能够保证评分与 CVSS 评分的相对稳定性。

4.2 漏洞评分分布与多样性分析

除漏洞评分比较外,本文还进行了模型分布的统计与比较,将所有不同的指标权值组合输入模型,使用 Python 和 pyecharts 将模型的输出进行结果统计和分布曲线绘制,得到了 CVSS、CVSS_{IOT} 和 VSMIV 的模型分布图,如图 7~图 9 所示,通过模型分布图,可以更好地比较模型的分布情况。

与 CVSS 的特征分布相比, VSMIV 模型具有更好的稳定性,相邻分布之间的变化更为平缓,且特征曲线相较 CVSS 更贴近正态分布,可以更好地刻画漏洞分布情况:分布平缓连续可以有效避免过多极端值的出现,分布近似正态离散更能客观有效地区分不同漏洞的严重性^[17]。并且,在 CVSS 的分布中,评分为 0 的情况远多于其他情况,与之相比, VSMIV 并没有此种情况的出现。与 CVSS_{IOT} 相比, VSMIV 的数值分布更为平滑,而 CVSS_{IOT} 的评分相邻数值存在较大差距,部分取值出现次数少,使相似漏洞容易产生相同的漏洞评分。

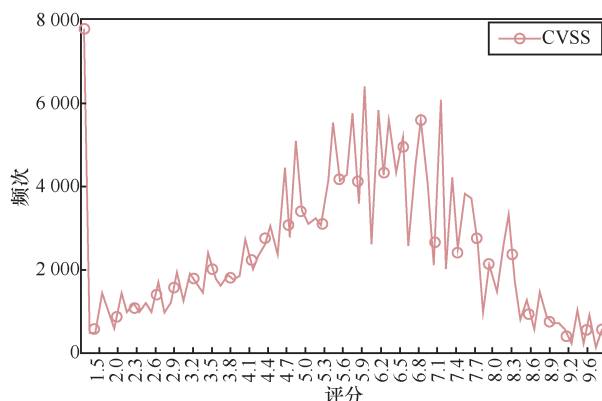


图7 CVSS 模型分布
Figure 7 CVSS model distribution

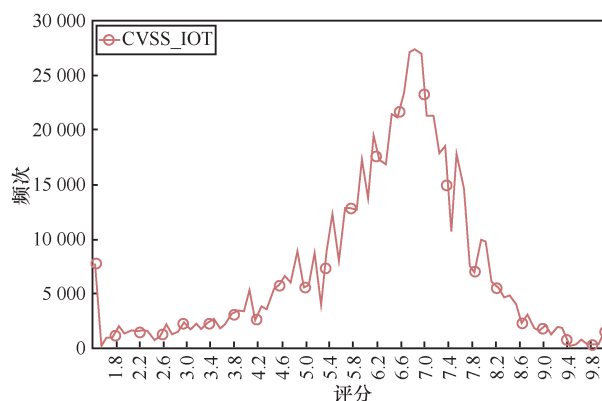


图8 CVSS_{IOT} 模型分布
Figure 8 CVSS_{IOT} model distribution

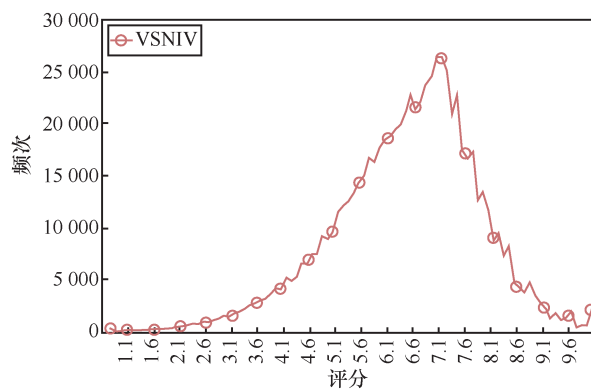


图9 VSMIV 模型分布
Figure 9 VSMIV model distribution

漏洞本身具有复杂性和多样性,评分系统拥有良好的评分多样性,可以使评分系统更好地评价漏洞特点^[6,18-19]。VSMIV、CVSS 和 CVSS_{IOT} 的评分结果是有限的,不同的评分指标组合可能产生相同的评分结果,评分结果共有 101 种可能取值,范围从 0 到 10 且最小步长是 0.1。评分多样性是统计评分系统所有可能的评分结果,可能

取值数量越接近 101, 则认为评分多样性越好。如表 10 所示, 在评分多样性方面, VSMIV 可能取值数量为 94, CVSS 的取值数量为 84, 而 CVSS_{IoT} 的取值数量是 87。这表明 VSMIV 的系统多样性取值优于 CVSS 和 CVSS_{IoT} 的系统多样性, VSMIV 可以更好地表达不同漏洞的严重程度。

表 10 系统分布多样性
Table 10 Diversity of model distribution

评分系统	系统分布多样性
CVSS	84
CVSS _{IoT}	87
VSMIV	94

基于评分模型特征分布曲线和评分多样性, 可以得出本文提出的评分模型对于汽车漏洞的特征表达和刻画能力高于 CVSS 版本和 CVSS_{IoT} 模型。

4.3 整车脆弱性评估实例

本节将基于 2.3 节中给出的判断矩阵和式(7)~式(10), 使用层次分析法对特斯拉 Model X 进行整车脆弱性的评估。通过判断矩阵和式(7)~式(9), 得到各项指标的综合权重 W 。特斯拉 Model X 上存在的漏洞与本文模型下的评分如表 11 所示。

表 11 特斯拉 Model X 漏洞的 VSMIV 评分
Table 11 Vulnerability score of Tesla Model X in VSMIV

漏洞	评分
CVE-2020-29440	8.4
CVE-2020-29439	6.9
CVE-2020-29438	7.6
CVE-2019-13582	9.5
CVE-2019-13581	8.8

根据上述 CVE 漏洞, 对特斯拉 Model X 进行漏洞评估, 获得该车型的各项指标得分如表 12 所示。漏洞评估规则是如果该项指标能被漏洞影响则取该漏洞评分, 被多个漏洞影响则取最高分值。

使用式(10)对指标向量 Z 和指标综合权重 W 进行计算, 即可得出特斯拉 Model X 的整车脆弱性 S_c 为 8.6, 表明该车型安全性存在较大隐患。

表 12 特斯拉 Model X 各项指标得分与权重
Table 12 Score and weight of Tesla Model X

准则层	指标层	脆弱性得分	指标综合权重
攻击面	物理访问	8.4	0.201 049 27
	近距离访问	9.5	0.100 472 68
	远距离访问	0	0.029 695 03
系统安全	权限提升	9.5	0.063 118 5
	命令执行	9.5	0.100 084 31
	行为控制	8.4	0.386 003 52
数据安全	数据保密性	9.5	0.064 447 19
	数据完整性	9.5	0.035 545 17
	数据可用性	9.5	0.019 584 36

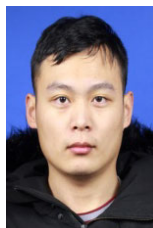
5 结束语

本文提出的面向智能汽车的信息安全漏洞评分方法, 建立了基于生命安全、财产安全、隐私安全和功能安全的漏洞影响计算模型, 并且根据智能汽车特点优化了漏洞可行性计算模型中的攻击向量和攻击复杂度指标, 很好地解决了基于信息安全三要素的 CVSS 无法合理评价智能汽车漏洞严重性的问题。与典型的 CVSS 相比, VSMIV 漏洞评分能够评价漏洞对车辆功能造成的影响, 判断漏洞是否会导致功能受损或者车辆异常行为等问题; 生命安全指标能够直接判断漏洞是否会对人员生命安全造成威胁以及何种程度的威胁; 此外, 添加了财产损失相关的指标, 因此漏洞评分能在一定程度上反映该漏洞可能对资产所有者造成的财产损失。并且, 本文提出的基于非线性回归的方法拟合了在现有指标权值上的公式参数, 使该模型能够更好地表示和刻画智能汽车漏洞。实验测试结果显示, 对于相同的汽车漏洞, VSMIV 漏洞评分更为合理, 并且模型相较于 CVSS 评分系统具有更好的多样性, 相邻评分之间的分布变化更为稳定连续。与 CVSS_{IoT} 相比, VSMIV 采取的评分指标更加丰富, 评分稳定性与多样性也更好。因此, VSMIV 评分模型可以更为合理地进行漏洞威胁评级。基于本文模型给出的漏洞评分, 对特斯拉 Model X 应用层次分析法得到该车型的整车脆弱性评分, 为系统管理人员更清晰地认知整车安全状况和漏洞修复提供了有效参考。

参考文献:

- [1] 田野. 11 部门联合发布《智能汽车创新发展战略》[J]. 智能网联汽车, 2020(2): 6-7.
TIAN Y. 11 departments jointly released intelligent vehicle innovation and development strategy[J]. Intelligent Connected Vehicles, 2020(2): 6-7.
- [2] ZHAO F, HUANG H Q, JIN H, et al. A hybrid ranking approach to estimate vulnerability for dynamic attacks[J]. Computers & Mathematics with Applications, 2011, 62(12): 4308-4321.
- [3] KERAMATI M. New vulnerability scoring system for dynamic security evaluation[C]//Proceedings of 2016 8th International Symposium on Telecommunications (IST). 2016: 746-751.
- [4] 李舟, 唐聪, 胡建斌, 等. 面向 SaaS 云平台的安全漏洞评分方法研究[J]. 通信学报, 2016, 37(8): 157-166.
LI Z, TANG C, HU J B, et al. Vulnerabilities scoring approach for cloud SaaS[J]. Journal on Communications, 2016, 37(8): 157-166.
- [5] LIU Q X, ZHANG Y Q. VRSS: a new system for rating and scoring vulnerabilities[J]. Computer Communications, 2011, 34(3): 264-273.
- [6] SPANOS G, SIOZIOU A, ANGELIS L. WIVSS: a new methodology for scoring information systems vulnerabilities[C]//Proceedings of the 17th Panhellenic Conference on Informatics. 2013: 83-90.
- [7] UR-REHMAN A, GONDAL I, KAMRUZZAMAN J, et al. Vulnerability modelling for hybrid IT systems[C]//Proceedings of 2019 IEEE International Conference on Industrial Technology. 2019: 1186-1191.
- [8] UR-REHMAN A, GONDAL I, KAMRUZZAMAN J, et al. Vulnerability modelling for hybrid industrial control system networks[J]. Journal of Grid Computing, 2020, 18(4): 863-878.
- [9] BOZORGI M, SAUL L K, SAVAGE S, et al. Beyond heuristics: learning to classify vulnerabilities and predict exploits[C]//Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining. 2010: 105-114.
- [10] ISO 26262. Road vehicles-functional safety[S]. 2011.
- [11] EVITA. E-safety vehicle intrusion protected applications[S]. 2011.
- [12] LE V H, DEN-HARTOG J, ZANNONE N. Security and privacy for innovative automotive applications: a survey[J]. Computer Communications, 2018, 132: 17-41.
- [13] 郭亚军. 综合评价理论与方法[M]. 北京: 科学出版社, 2002.
GUO Y J. Theory and method of comprehensive evaluation[M]. Beijing: Science Press, 2002.
- [14] 刘琼. 基于层次分析法的风险评估系统的研究与设计[D]. 西安: 西安电子科技大学, 2009.
LIU Q. Study and design of the risk assessment system based on analytic hierarchy process[D]. Xi'an: Xidian University, 2009.
- [15] ZHANG Y J, DENG X Y, WEI D J, et al. Assessment of E-commerce security using AHP and evidential reasoning[J]. Expert Systems with Applications, 2012, 39(3): 3611-3623.
- [16] 陈秀真, 吴越, 李建华. 车载信息系统的的功能测评体系及方法[J]. 信息安全学报, 2017, 2(2): 15-23.
CHEN X Z, WU Y, LI J H. System and approach of security testing and evaluation for invehicle information systems[J]. Journal of Cyber Security, 2017, 2(2): 15-23.
- [17] WANG R Y, GAO L, SUN Q, et al. An improved CVSS-based vulnerability scoring mechanism[C]//Proceedings of 2011 Third International Conference on Multimedia Information Networking and Security. 2011: 352-355.
- [18] MELL P, SCARFONE K. Improving the common vulnerability scoring system[J]. IET Information Security, 2007, 1(3): 119.
- [19] 谢丽霞, 徐伟华. 改进漏洞基础评分指标权重分配方法[J]. 计算机应用, 2017, 37(6): 1630-1635.
XIE L X, XU W H. Improved weight distribution method of vulnerability basic scoring index[J]. Journal of Computer Applications, 2017, 37(6): 1630-1635.

[作者简介]



于海洋 (1996-), 男, 山东泰安人, 上海交通大学硕士生, 主要研究方向为车联网信息安全、网络安全。



陈秀真 (1977-), 女, 山东聊城人, 博士, 上海交通大学副教授, 主要研究方向为车联网信息安全、网络信息系统安全检测与评估、社交网络大数据分析。



马进 (1977-), 女, 山东滕州人, 博士, 上海交通大学高级工程师, 主要研究方向为大数据与人工智能应用、车联网信息安全、网络空间安全综合管理新技术。



周志洪 (1979-), 男, 江西九江人, 上海交通大学讲师, 主要研究方向为密码应用、安全测评、车联网安全。



侯书凝 (1998-), 女, 江西抚州人, 上海交通大学硕士生, 主要研究方向为车联网信息安全。