**项目名称：**面向智能网联汽车的开源软件供应链安全关键技术及应用

**提名奖项等级：**天津市科学技术进步奖二等奖

**主要完成单位: 南开大学、中汽智联技术有限公司、上海交通大学、天津大学、中汽数据（天津）有限公司**

**完成人：**陈森、宁玉桥、范玲玲、郭振、朱浩瑾、刘哲理、王海均、王俊杰

**提名单位：南开大学**

**项目简介：**

本项目以开发出适用于智能网联汽车的开源软件供应链的组件及版本识别与漏洞检测工具为首要目标，旨在通过广泛收集智能网联汽车系统的开源软件供应链信息，深入研究组件特征提取与匹配、组件版本语义差异、漏洞语义信息多维特征建模、漏洞特征提取与匹配、汽车软件环境仿真和动态插桩验证等技术，提升高质量漏洞挖掘能力和自动化工具扫描的准确率，实现漏洞扫描准确率90%以上，超过主流同类国际产品，打破国外技术垄断，不断为汽车行业安全风险感知赋能，并在行业广泛推广和应用，产生显著的经济社会效益。

**创新点：**

（1）针对智能网联汽车第三方开源组件识别准确率低的行业共性问题，提出了智能网联汽车系统软件二进制程序区域分割方法，构建了细粒度二进制抽象语法树结构，填补了行业针对智能网联汽车系统软件第三方组件语义特征设计的空白，突破了基于二进制抽象语法树的高精度第三方开源组件识别技术。

（2）针对智能网联汽车开源软件供应链冗长复杂导致的版本交叉混乱问题，提出了基于组件函数关系的第三方开源组件版本语义差异性建模和基于漏洞语义信息的多维特征建模方法，通过融合组件版本语义差异信息和漏洞语义信息，解决了智能网联汽车多系统，多架构的第三方组件版本及供应链漏洞检测问题，研发了智能网联汽车开源软件供应链漏洞检测平台。

（3）针对开源软件供应链漏洞在智能网联实车端验证环境搭建困难、验证效率低的问题，研发了智能网联汽车软硬件融合一体化仿真技术，建成了兼容RH850、TRICORE、ARM、MIPS、PowerPC等多系统架构的智能网联汽车系统虚拟化仿真漏洞验证平台，突破了基于内存状态和执行逻辑监控的定制化动态插桩技术，有效克服了传统依赖实车和人工调试方式所面临的资源受限与低效难题。

**主要技术支撑材料：**

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 附件类型 | 论文（专著）名称/刊名/作者 | 年卷页码 |
| 1 | 论文 | Does the Vulnerability Threaten Our Projects? Automated Vulnerable API Detection for Third-Party Libraries/IEEE Transactions on Software Engineering/Fangyuan Zhang, Lingling Fan, Sen Chen, Miaoying Cai, Sihan Xu, Lida Zhao | 2024年50卷2906-2920页 |
| 2 | 论文 | DeepSuite: A Test Suite Optimizer for Autonomous Vehicles/IEEE Transactions on Intelligent Transportation Systems/Sihan Xu, Zhiyu Wang, Lingling Fan, Xiangrui Cai, Hua Ji, Siau-Cheng Khoo, Brij Bhooshan Gupta | 2022年23卷9506-9517页 |
| 3 | 论文 | Scene-Driven Exploration and GUI Modeling for Android Apps/2023 38th IEEE/ACM International Conference on Automated Software Engineering/Xiangyu Zhang, Lingling fan, Sen Chen, Yucheng Su, Boyuan Li | - |
| 4 | 论文 | Aligning Core Aspects: Improving Vulnerability Proof-of-Concepts via Cross-Source Insights/Proceedings of the 33rd ACM International Conference on the Foundations of Software Engineering/Lingxiao Wang, Wenjing Dang, Mengyao Zhang, Yue Wang, Xianzong Wu, Sen Chen | - |
| 5 | 论文 | Storydroid: Automated generation of storyboard for android apps/2019 IEEE/ACM 41st International Conference on Software Engineering/Sen Chen, Lingling Fan, Chunyang Chen, Ting Su, Wenhe Li, Yang Liu, Lihua Xu | - |
| 6 | 论文 | A Large-Scale Empirical Study on Industrial Fake Apps/ACM 41st International Conference on Software Engineering/Chongbin Tang, Sen Chen, Lingling Fan, Lihua Xu, Yang Liu, Zhushou Tang and Liang Dou | - |
| 7 | 论文 | SMPCache: Towards More Efficient SQL Queries in Multi-Party Collaborative Data Analysis/IEEE Transactions on Knowledge and Data Engineering/Junjian Shi, Ye Han, Xiaojie Guo, Zekun Fei, Zheli Liu, Siyi Lv | 2025年37卷2111-2125页 |
| 8 | 论文 | TensorJSFuzz: Effective Testing of Web-Based Deep Learning Frameworks via Input-Constraint Extraction/The 2025 ACM Web Conference/Lili Quan, Xiaofei Xie, Qianyu Guo, Lingxiao Jiang, Sen Chen, Junjie Wang, and Xiaohong Li | - |
| 1 | 发明专利 | 一种车联网供应链安全漏洞预警方法、系统和存储介质/马超，于龙海，宁玉桥，张巧，霍全瑞，薛世豪 | ZL202311384484.X2024/4/9 |
| 2 | 发明专利 | 汽车固件的安全漏洞检测方法、设备和存储介质/张亚楠，马超，宁玉桥，于龙海，边臣雅，霍全瑞，薛世豪 | ZL202310212730.7 |
| 3 | 发明专利 | 基于车联网漏洞数据的预测方法、设备和存储介质/马超，宁玉桥，李宝田，薛世豪，郭振，张亚楠，吴青洋 | ZL202211263921.8 |
| 4 | 发明专利 | 一种基于POC载荷库的漏洞扫描工具增强方法和系统/张亚楠，马超，沈诗雯，宁玉桥，郭振，边臣雅，薛世豪 | ZL202310777007.3 |
| 5 | 发明专利 | 基于静态和动态结合的漏洞验证方法、设备和介质/张亚楠，宁玉桥，马超，郭振，刘畑灵，张巧，边臣雅 | ZL202310504413.2 |
| 6 | 发明专利 | 一种汽车信息安全测试用例的构建和提取方法/刘畑灵，张亚楠，马超，宁玉桥，郭振，王海均，于明明 | ZL202310670875.1 |
| 7 | 发明专利 | 基于JAVA函数调用序列的高精度第三方库漏洞模块检测方法/范玲玲，张方缘，齐向东，应志军，张健，徐思涵 | ZL202210173072.0 |
| 8 | 发明专利 | 车用CAN总线注入攻击异常检测方法及系统/朱浩瑾，胡浩天，孟岩 | ZL202210817913.7 |
| 9 | 计算机软件著作权 | CyberSploit漏洞PoC检索平台1.0 | 2024SR1084479 |
| 10 | 计算机软件著作权 | Completion漏洞PoC信息融合平台1.0 | 2025SR0871063 |