个人简历

王 珏

生日：1993 年 11 月 14 日

电话：+86 15950580128

微信：skull591

邮箱：juewang591@gmail.com

QQ: 382340878

主页：http://cv.juewang.info/

工作经历

- **2022.08-至今** **华为-2012 实验室-软件工程应用技术实验室** **高级工程师 A**
  - **负责 fuzzing 测试前沿技术研究，优化产品线开发者 fuzzing 测试效果**
    - 深入评估比较现有 fuzzing 技术，发现现有技术效果仍不够理想，无法替代人工测试与代码审核，且现有技术无普适最优，各有优劣；
    - 针对上述发现，开展 **ensemble fuzzing 前沿技术研究**，提出创新的自研新技术，包含基于强化学习的动态资源调度算法与多维度收益衡量的种子共享技术，实验评估相比目前顶尖技术提升效果明显，并在真实世界开源项目上挖掘包含多个 CVE 的缺陷；**学术成果目前投稿 CCF-A 类会议**；
  - **构建系统评估 fuzzing 技术测试效果方法**
    - 业界一般通过一组已知缺陷的发掘效果与代码覆盖率评估，由于缺陷的稀疏性与覆盖率的低信息性，无法全面评估 fuzzing 技术测试效果；
    - **形成一套系统评估 fuzzing 技术测试效果的方法**，包括一组被测程序集（包含 16 个程序中超过 300 个缺陷），一组 fuzzing 测试路障数据集（难以被已有顶尖 fuzzing 技术覆盖的代码块），及一个 fuzz 测试效果自动评估工具；
    - 采用**危险性代码导向的 fuzzing 测试评估标准**，借助静态分析工具、地址消毒器、机器学习技术分析被测程序，预测与漏洞相关函数，使用 fuzzing 测试中这些函数的覆盖率作为效果指标之一，结合代码覆盖率、漏洞触发情况、fuzzing 路障克服情况、综合评估 fuzzing 技术测试效果；
  - **搭建面向全公司产品线的开发者 fuzzing 测试平台**
    - 平台对标 Google OSS-Fuzz，实现项目代码 24 小时看护、异步多测试任务调度、多 fuzzing 引擎插件级插拔与 ensemble 集成测试、post-fuzzing 分析（缺陷定位、去重、效果评估等）；
    - **负责平台核心关键技术部分**：（1）对业界顶尖 Fuzzing 技术深入分析比较，优选 fuzzing 引擎加入平台引擎池；（2）将自研 ensemble fuzzing 技术落入平台，实现多容器、多引擎协作 fuzzing 测试，且实现不同容器可按照参数配置优化不同测试效果指标；及（3）设计统一 fuzzing 引擎抽象接口，实现 fuzzing 引擎插件式插拔使用，确保平台高可扩展性；
    - 参与平台前后端架构设计、异步多测试任务调度方法设计，实现项目代码 24 小时看护、自动拉取、异步测试、及报告反馈

教育背景

- **2016.09-2022.06** **南京大学-计算机科学与技术系** **博士**
  - 导师：吕建教授（中科院院士），马晓星教授（国家杰青），许畅教授（长江学者），蒋炎岩讲师
  - 毕业论文题目：Automatically Detecting Deep Logic Bugs in Mobile Applications
- **2012.09-2016.06** **南京大学-计算机科学与技术系** **本科**
  - 入选“教育部拔尖创新人才培养试验计划”计算机科学拔尖班学习 4 年：以计算机问题求解为核心，开展计算机专业人才创新能力培养
- **2019.09-2021.01** **苏黎世联邦理工学院(ETHZ)-计算机科学学院** **博士联合培养**
  - 导师：Zhendong Su 教授（欧洲科学院院士）

获得荣誉

- 2022 年华为优秀新员工
- 2022 年度南京大学优秀毕业生（研究生）
- 2020 年度华为奖学金，2019 年度中汇信息奖学金，2017 年度华为奖学金，2016 年度校长奖学金
- 2016 年度南京大学优秀毕业生(本科)

科研成果

目前共发表论文 10 余篇，包括 CCF-A 类会议/期刊 6 篇，CCF-B 类会议/期刊 4 篇，主要关注于**智能手机应用缺陷检测与质量保障**，其中第一作者论文 4 篇（包括 2 篇 CCF-A 类，1 篇 CCF-B 类）。部分重要论文如下：

- **ComboDroid: Generating high-quality test inputs for Android apps via use case combinations**
  - **2020 ICSE (CCF-A)：第一作者**
  - 分析 Android 应用执行不同功能时的数据依赖关系，生成多样化数据流的，能够探索应用深层状态的测试输入
  - 文章的工具整理公开，通过会议的 Artifact Evaluation，被授予 Available 徽章
- **Detecting non-crashing functional bugs in Android apps via deep-state differential analysis**
  - **2022 ESEC/FSE 2022: 第一作者**
  - 化用 bugs as deviant behaviors 思想，自动识别被触发的 Android 应用非崩溃功能性缺陷
  - 文章工具整理公开，通过会议的 Artifact Evaluation，被授予 Available 徽章
- **AATT+: Effectively manifesting concurrency bugs in Android apps**
  - **2018 SCP (CCF-B 期刊)：第一作者**
  - 分析 Android 应用并发执行时线程间数据依赖关系，同步生成测试输入与线程调度，以触发潜在并发缺陷
- **Benchmarking automated GUI testing for Android against real-world bugs**
  - **2021 ESEC/FSE (CCF-A)**
  - 首个基于真实世界 Android 应用缺陷的 benchmark，对已有自动测试输入生成工具进行系统比较与分析
  - 包含种类丰富，能有效检验工具效果的真实世界应用与缺陷，已与工业界深入合作，协助提升内部工具效果
- **Property-based fuzzing for finding data manipulation errors in Android apps**
  - **2023 ISSTA (CCF-A)**
  - 通过组合相关的数据修改操作并验证其是否保留正确的 property，自动检测 Android 应用中的数据修改错误
- **An empirical study of functional bugs in Android apps**
  - **2023 ESEC/FSE (CCF-A)**
  - 首个针对 Android 应用非崩溃功能缺陷的实证研究，建立包含 399 个真实世界缺陷实例的数据集，并分析其症状、根因、修复方法等各方面特征
- **Fully automated functional fuzzing of Android apps for detecting non-crashing logic bugs**
  - **2021 SPLASH/OOPSLA (CCF-A)**
  - 基于 independent view property，无需人工提供 oracle，自动检测应用非崩溃功能性缺陷
- **Droidleaks: A comprehensive database of resource leaks in android apps**
  - **2019 EMSE (CCF-B 期刊)**
  - 首个 Android 应用真实资源泄露缺陷数据集，包含 32 个真实世界应用中近 300 个资源泄露缺陷
  - 基于该数据集，对已有静态资源泄露检测工具进行系统比较与分析
- **Android 应用测试输入自动生成技术**
  - **2019 中国科学：信息科学 (CCF-A 中文期刊)**
  - 提出对 Android 应用测试输入自动生成技术的统一描述框架，从三个维度系统描述每个技术，并在同一框架下，系统分析比较现有技术，讨论现有技术不足及未来发展契机

个人能力

科研兴趣

- 关注于软件测试、Android 应用缺陷检测及质量保障等方向

智能手机平台

- 熟悉 Android 应用编写与测试工具，熟悉 Android 系统架构及 Framework 层代码，熟练使用 Soot、Xposed、Jacoco 等 Android 应用分析及插装工具、熟悉 Stoat、APE 等学术界顶尖自动测试工具代码

编程语言

- 熟悉 Java、Kotlin、python、C/C++等主流编程语言

语言能力：

- 较好的英语写作及交流能力，可独立进行英语学术写作；通过托福考试，获得 102 分