ISCAS 中国科学院软件研究所学术年会'2022
暨计算机科学国家重点实验室开放周
学术论文

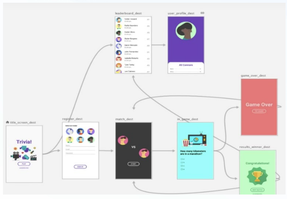
ICCBot: 高效的Android ICC 解析工具

ICCBot: Fragment-Aware and Context-Sensitive ICC Resolution for Android Applications. ICSE 2022, Demo Track.

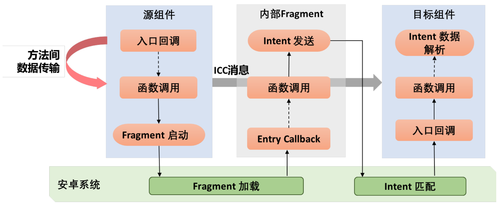
燕季薇(yanjw@ios.ac.cn)，张世新，刘烨庞，严俊，张健
软件工程技术研究开发中心

很多大型框架都提供了组件/模块化的设计，组件负责**单一职责**。

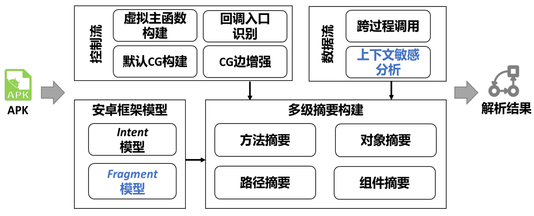
不同组件通过收发满足特定规范消息实现**组件间通讯(ICC)**，框架层隐藏了真实的函数调用行为。



ICC消息的**建模和提取**是安卓框架下应用控制流、数据流恢复的重要一环，对上层应用的分析和测试具有重要意义。

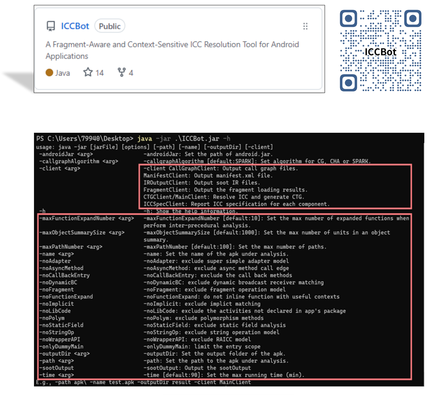


ICC发送&接收过程



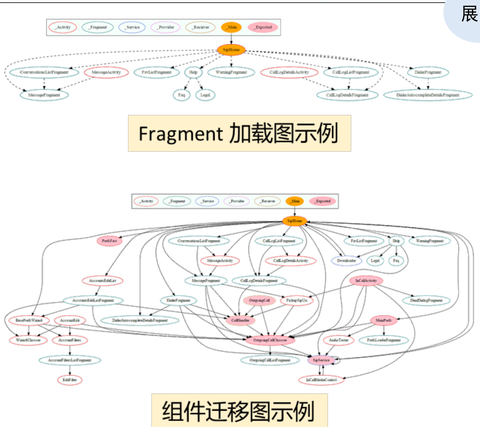
ICCBot设计架构

工具



ICCBot 运行界面

展示



实验验证

正确的ICC数量最多，误报最少

- 在三个手工构造的**Benchmark**上的准确性比较

Benchmark	#Ground-Truth	IC3		IC3-DialDroid		Gator		ICCBot	
		#TP	#FP	#TP	#FP	#TP	#FP	#TP	#FP
DroidBench	12	8	0	8	0	7	1	10	0
ICC-Bench	26	10	0	23	0	4	0	26	0
ICCBotBench	11	7	3	10	24	7	3	11	0
Sum	49	25	3	41	24	18	4	47	0

两种策略辅助ICC识别的效果

- 在**2,000**个真实应用上的识别数量比较

Tool	#Success	$Time_{succ}$	#ICC
IC3	1,719	57s	10,860
IC3-DialDroid	1,851	115s	8,601
Gator	1,882	20s	27,297
ICCBot	2,000	54s	28,584