ISCAS 中国科学院软件研究所学术年会’2021
暨计算机科学国家重点实验室开放周

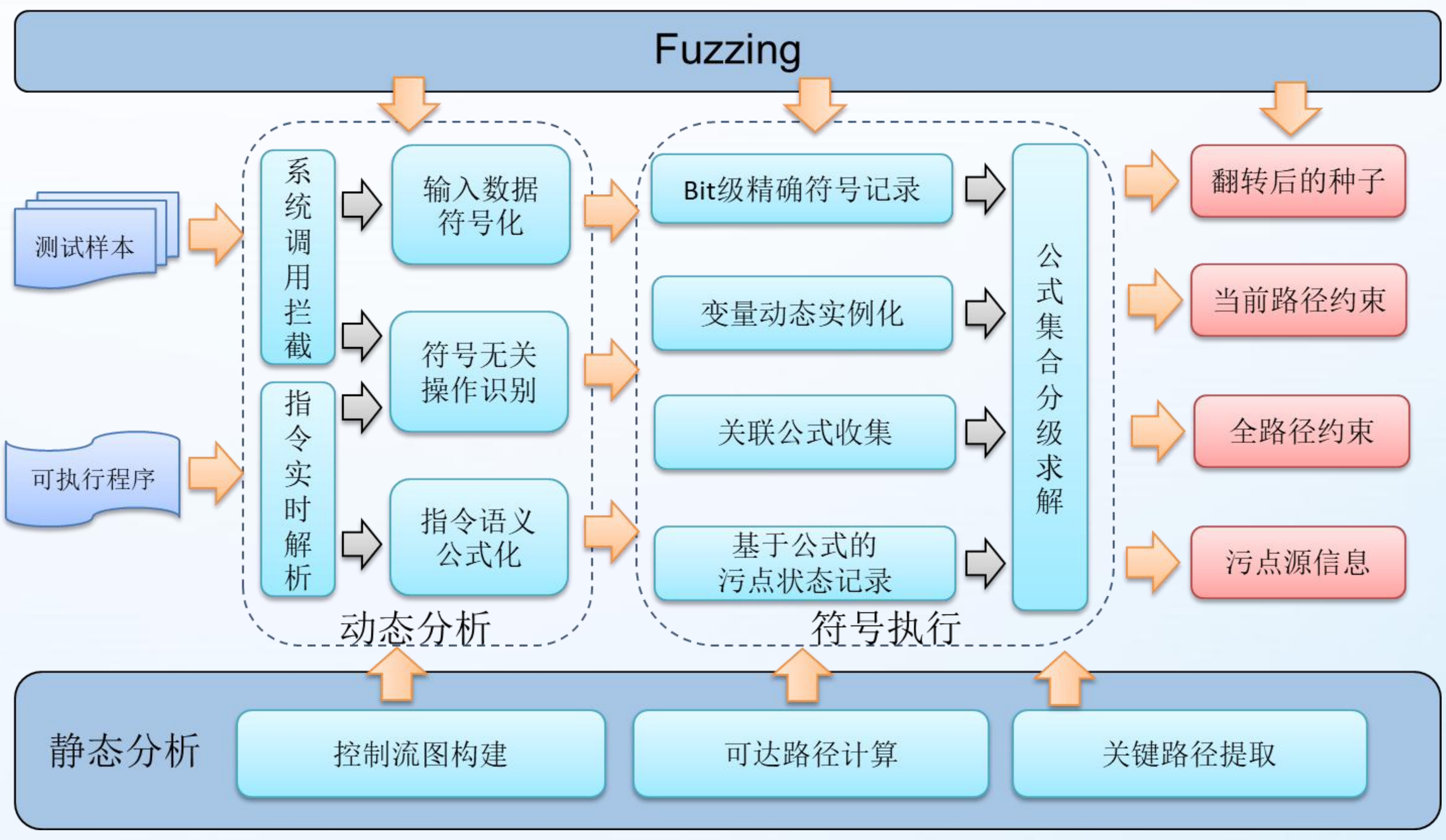
工具系统

AOTA-SSym:基于关键路径条件的导向性Fuzzing系统

杨轶、苏璞睿
{yangyi, purui}@iscas.ac.cn
13581793536, 13910088471

AOTA-SSym （Application Oriented Taint Analysis & Selected Symbolic Execution）系统针对现有模糊测试工作中面临的问题研发。主要包括：1）使用盲目数据变换，难以有效导向目标路径；2）少数系统引入符号执行，但表达与推导过程精度不足，误差较大；2）符号执行过程基于中间语言实现符号化解析，冗余度高、分析效率低； 4）路径翻转的求解过程依赖于全路径约束，易被非必经节点产生的约束干扰。

我们提出了基于关键路径的Fuzzing方法，仅关注程序中可能将路径导向偏离目标的分支条件；提出二进制指令语义直接解析、符号无关指令识别方法，动态忽略了80%以上符号无关指令，有效提高系统效率；提出了基于公式的污点状态记录方法，在不增加复杂度的条件下，同时实现符号执行与污点传播，提高了系统分析能力；提出了基于全路径约束、当前路径约束的分级求解方法，消除了非必经节点约束干扰，有效提高了路径翻转能力。


Fuzzing
测试样本
可执行程序
系统调用拦截
指令实时解析
输入数据符号化
符号无关操作识别
指令语义公式化
动态分析
Bit级精确符号记录
变量动态实例化
关联公式收集
基于公式的污点状态记录
公式集合分级求解
符号执行
翻转后的种子
当前路径约束
全路径约束
污点源信息
静态分析
控制流图构建
可达路径计算
关键路径提取

系统主要包括程序预处理、控制依赖分析、输入数据符号化、关联逻辑公式收集、公式集合分级求解、符号数据源回溯等功能，具备针对Linux、Windows等操作系统上的大型应用软件的动态逆向分析能力。系统具有如下的技术特性：

- 基于bit级符号化表示与求解，分析精度高；
- 结合符号执行精确翻转关键路径，降低符号执行的复杂度；
- 支持命令行参数、文件、网络输入变量符号化，数据获取能力强；
- 支持Intel x86/x64指令集，支持Acrobat PDF、OpenSSH等大型可执行程序分析；
- 全约束求解与简化约束求解分级实现，不受前序路径中非必要约束干扰。

该系统目前已经应用于漏洞挖掘，在3天内发现了objdump、libjpeg、libpng等广泛使用的应用和程序库中的96个未知错误。