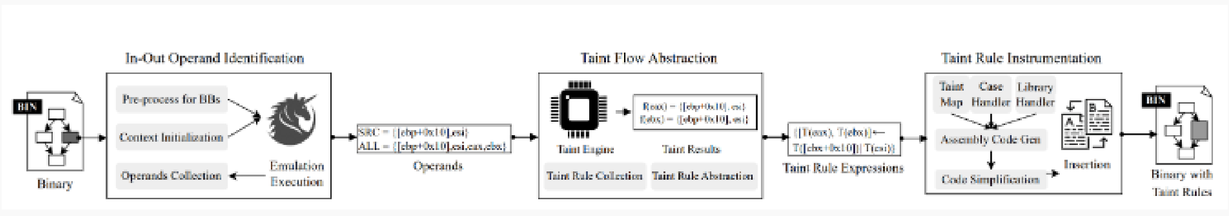
软件所在漏洞挖掘与分析方面取得系列进展

文章来源： | 发布时间：2023-10-09 | 【打印】 【关闭】

软件所可信计算与信息保障实验室软件智能分析团队，聚焦数据流分析及应用，解决了现实场景中复杂软件漏洞挖掘与分析的系列关键难题，多篇成果论文被领域顶会录用。

论文*AirTaint: Making Dynamic Taint Analysis Faster and Easier*被IEEE S&P 2024录用，第一作者为博士生桑倩。论文针对指令级污点传播规则冗余及冗余插桩引入的额外开销等问题，提出将指令级污点传播计算提升到基本块级，并利用汇编指令层静态插装代替动态插装实现的方案。

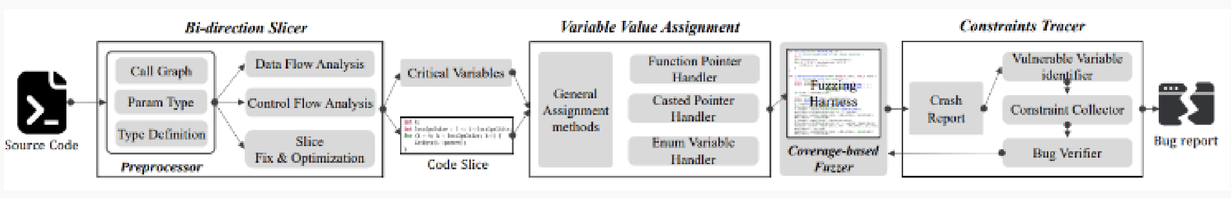
团队设计实现原型工具AirTaint，重点解决了基本块级污点传播规则快速提取、内存操作数的处理、精准插装优化等关键难题。经实验评估，AirTaint分析效率相比于libdft、SelectiveTaint、TaintRabbit最大可提升931.0x、5.97x、328.3x，能够准确地检测不同指令架构（X86、X86-64）、不同类型（Buffer Overflow、UAF等）的漏洞触发情况。



AirTaint框架结构

论文*AFGEN: Whole-Function Fuzzing for Applications and Libraries*被IEEE S&P 2024录用，第一作者为博士生刘昱玮。针对现实场景中模糊测试代码覆盖率实际值低的问题，论文提出“全函数模糊测试”的概念，即对任意函数（特别是容易出现问题的函数）直接进行模糊测试，提升了深层次代码的漏洞挖掘能力；同时提出反馈式“片段测试代码”（类似FuzzDriver）修正和验证方法，有效降低了直接模糊测试带来的误报问题。

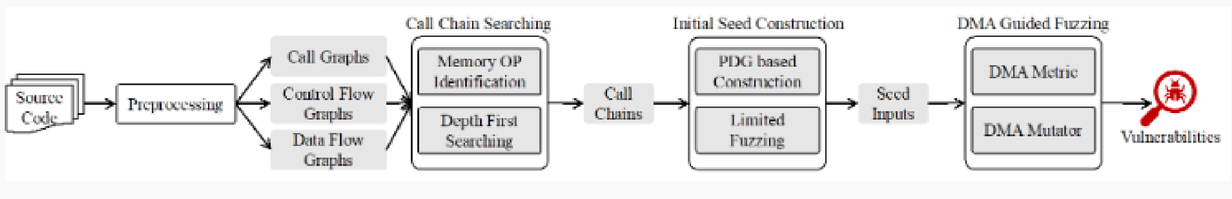
研究团队设计实现原型工具AFGen，重点解决了“片段测试代码”生成中的数据依赖、数值初始化来源和漏洞触发路径约束问题。基于AFGen的全函数模糊测试实验发现了24个0day，漏洞挖掘效果明显优于通用模糊测试工具AFL、AFL++和定向模糊测试工具AFLGo、Parmesan、Beacon，Fuzz Driver生成效果也明显优于Google的同类型工具FUDGE。



AFGen框架结构

论文*VD-GUARD: DMA Guided Fuzzing for Hypervisor Virtual Device*被IEEE/ACM ASE 2023录用，第一作者为博士生刘昱玮。DMA访问是一类特殊但广泛应用的数据传递方式，近几年发现的虚拟设备漏洞中近80%的漏洞和DMA访问相关。DMA数据访问过程是从虚拟设备初始化到虚拟设备调用与回调函数、再到DMA操作具体实施函数的操作序列。论文认为，通过识别该操作序列并作为模糊测试的反馈，可以增强对不同DMA访问代码和逻辑状态的探索，进而发现更多DMA相关的虚拟设备漏洞。

研究团队设计实现原型工具VD-GUARD，首先通过对QEMU等被测虚拟机源代码的预处理确定DMA相关的调用路径，然后根据触发DMA调用路径构造初始化种子，再根据DMA访问的触发情况进行模糊测试反馈。经实验评估，VD-GUARD发现了4个0day漏洞，相比于最新的虚拟设备模糊测试工具MorPhuzz可以发现更多漏洞。



VD-GUARD框架结构

论文*One Simple API Can Cause Hundreds of Bugs: An Analysis of Refcounting Bugs in All Modern Linux Kernels*被SOSP 2023录用，第一作者为和亮研究员。论文认为，Linux Kernel代码中存在很多UAF漏洞的主要成因之一是引用计数错误。为进一步解释引用计数错误的产生原因并更好地指导内核代码开发，研究团队对Linux Kernel中的引用计数错误（数据来源于2005年-2022年753个版本，包括超100万次提交记录）进行收集，统计分析了引用计数错误的安全危害、错误分布和修复情况，并从漏洞潜在的安全影响角度分类总结出四大类引用计数错误发生的根本原因。

研究团队进一步设计实现了基于静态语义模板的漏洞主动挖掘工具，在新版本Linux Kernel中发现bug 351个，其中已确认240个，相关补丁已被合并至主线版本。该论文还公开了容易发生引用计数错误的API调用等。

Subsystem	New Bugs	Impacts			Status		#FP
		Leak	UAF	NPD	#CFM	#PR	
arch	156	135	18	3	91	0	1
drivers	182	149	29	4	137	2	4
include	2	2	0	0	2	0	0
net	2	1	1	0	1	1	0
sound	9	9	0	0	9	0	0
Total	351	296	48	7	240	3	5

bug发现情况统计

软件所可信计算与信息保障实验室苏璞睿研究员带领的软件智能分析团队，长期专注于软件漏洞分析与防治研究，相关工作得到了国家自然科学基金重点项目、国家重点研发计划项目、中国科学院先导项目等科研任务的支持，团队中多名青年骨干入选中国科学院青年创新促进会。