

# 基于大语言模型指导的内核定向模糊测试探索

Towards Large Language Model guided Kernel Direct Fuzzing

李颢, 苑照月, 张镇铎, 孙有程, 张立军

28th International Conference on Fundamental Approaches to Software Engineering (ETAPS FASE)

主要联系人: 李颢 邮箱: lixie19@ios.ac.cn

## 研究背景

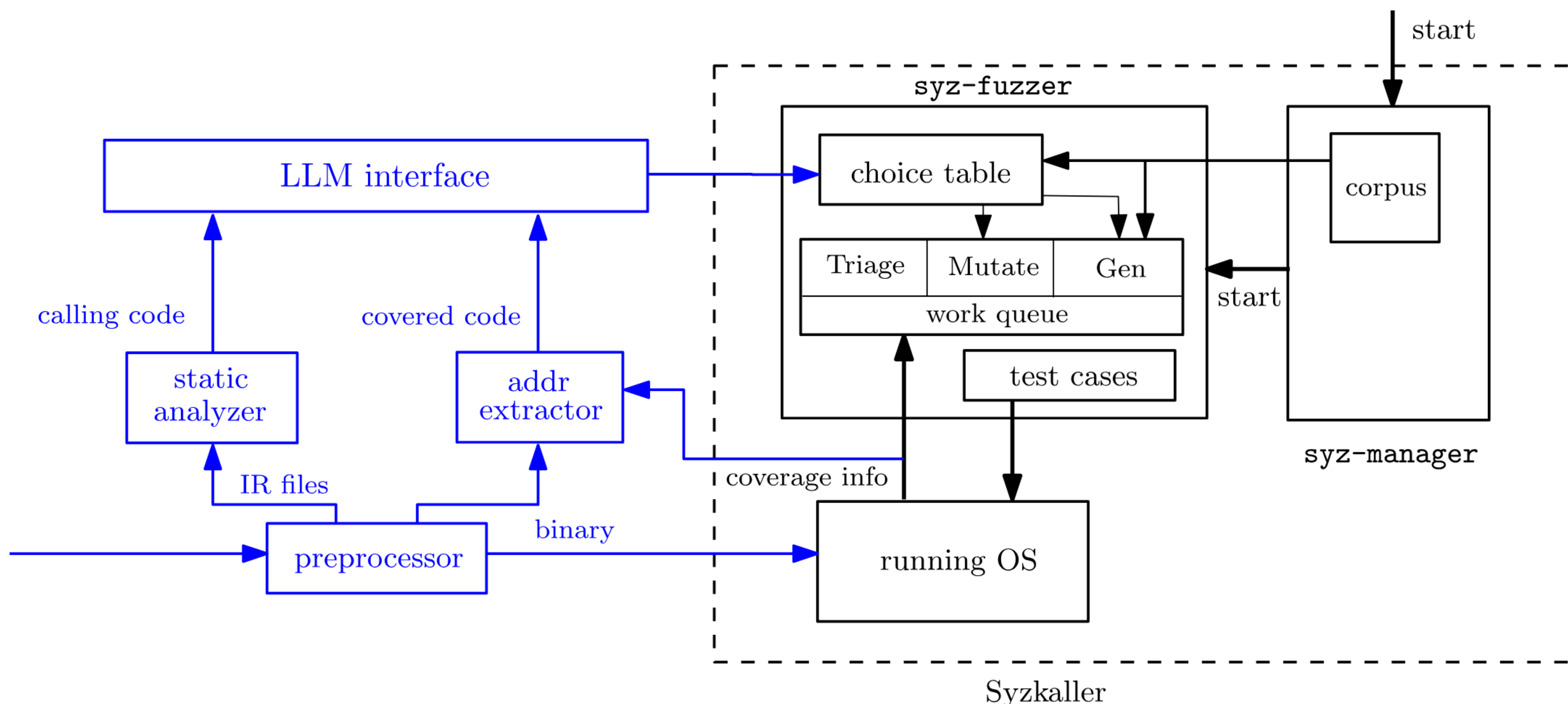
操作系统内核复杂且频繁更新, 传统模糊测试难以高效覆盖

- 传统内核模糊测试工具如 Syzkaller 能有效发现漏洞, 但难以深入覆盖复杂代码路径。
- 定向内核模糊测试针对特定关键区域, 能够更高效地应对内核的快速迭代。
- 大型语言模型 (LLM) 具备强大的代码理解能力, 为模糊测试的智能引导提供了新的可能。

## 研究目标和难点

- 利用 LLM 对内核代码进行分析, 提升对于目标函数及邻近区域的覆盖率和快速覆盖效率。
- 结合静态分析和动态反馈, 实现模糊测试过程中的测试用例生成策略的智能化调整。
- 与已有的SOTA工具相结合。

## 方法架构



基于已有的内核模糊测试Syzkaller, 提出我们的工具框架SyzAgent, 其主要包括以下几个模块:

- 静态分析模块:** 提取内核调用路径, 确定目标函数相关代码。
- 大语言模型接口:** 基于代码和测试反馈生成系统调用入口指导信息。
- 模糊测试引擎 (Syzkaller):** 结合 LLM 指导进行测试用例生成和变异, 测试过程中收集能够触碰 (Hit) 到目标函数邻近区域的测试用例。
- 反馈循环:** 根据测试情况和收集的测试用例动态调整测试用例生成策略, 持续优化覆盖。

## 实验评估

### 实验设置

- 数据集收集:** 从Linux内核中选取了27个当前LLM提示词限制下能够处理的目标函数
- 每个目标函数进行Syzkaller和SyzAgent分别重复3次2小时的模糊测试

### 实验结果

- 在27个目标函数测试中, 67%案例覆盖率提升显著, 如表1所示。
- 在6个例子上, 出现了突破传统Syzkaller覆盖瓶颈的现象, 例如图1所示。
- 对比Syzdirect, LLM方法在系统调用识别方面表现优异。
- SyzAgent工具链接:  
<https://github.com/SpencerL-Y/SyzAgent>

ID	Target Function	Dist.	SYZAGENT Hit %			Syzkaller Hit %			Avg. Diff
			Run 1	Run 2	Run 3	Run 1	Run 2	Run 3	
1	ksys_semctl	1	28.27	28.89	31.8	3.8	5.15	1.11	26.3
2	__sys_setfsgid	1	19.1	13.89	9.45	0.0	0.03	0.0	14.14
3	do_sched_yield	1	25.15	26.32	41.7	20.57	30.14	26.86	5.2
4	vm_acct_memory	2	32.4	28.82	32.84	22.12	17.83	15.27	12.95
5	__shmem_file_setup	2	8.82	7.32	7.81	3.79	6.49	4.93	2.91
6	io_register_iowq_m...	2	22.05	15.63	18.26	1.02	3.28	2.59	16.35
7	__anon_inode_getfile	2	30.47	30.38	30.65	9.97	11.89	11.68	19.32
8	copy_faxattr_from...	3	56.8	56.99	54.75	51.0	49.34	50.1	6.03
9	__io_uring_add...	3	36.02	34.97	28.0	8.9	2.65	11.76	25.23
10	keyring_ptr_to_key	3	30.26	21.64	23.95	6.58	2.48	6.47	20.11
11	mnt_get_writers	3	77.1	73.33	75.44	67.6	73.84	80.1	1.44
12	futex_requeue_pi...	3	0.92	0.0	0.0	2.94	0.31	2.0	-1.44
13	wait_for_device_probe	4	0.33	0.31	0.12	0.35	0.14	0.13	0.05
14	memcpy_to_page	4	24.07	29.73	34.0	7.1	9.02	0.0	23.89
15	kiimage_is_dest...	5	1.74	7.69	8.05	0.0	0.06	0.66	5.59
16	find_lock_entries	5	40.68	37.72	33.88	38.28	34.67	39.23	0.03
17	fsnotify_data_sb	5	58.2	57.33	61.22	55.73	55.72	60.94	1.45
18	security_inode_set...	5	12.02	10.74	12.86	3.39	4.78	3.61	7.94
19	free_partitions	6	13.48	21.94	14.57	28.17	24.73	25.97	-9.63
20	bpf_prog_free	6	0.56	5.12	3.68	1.25	1.5	3.37	1.08
21	locks_delete_glob...	6	0.59	0.58	0.0	0.73	0.04	0.56	-0.05
22	pmd_none_or_clear_bad	7	12.92	11.3	16.47	14.72	19.68	18.11	-3.94
23	__submit_bio_noac...	7	31.89	21.5	19.88	20.09	28.69	27.06	-0.86
24	srcu_read_lock_nm...	7	19.89	45.15	26.51	23.62	25.22	20.31	7.47
25	trace_wbc_writepage	8	1.82	0.81	3.03	0.79	1.71	0.6	0.85
26	sk_set_bit	8	8.21	10.61	6.48	3.09	3.23	6.61	4.12
27	sidtab_search_core	8	76.48	77.85	75.68	73.14	76.26	73.34	2.42

表1

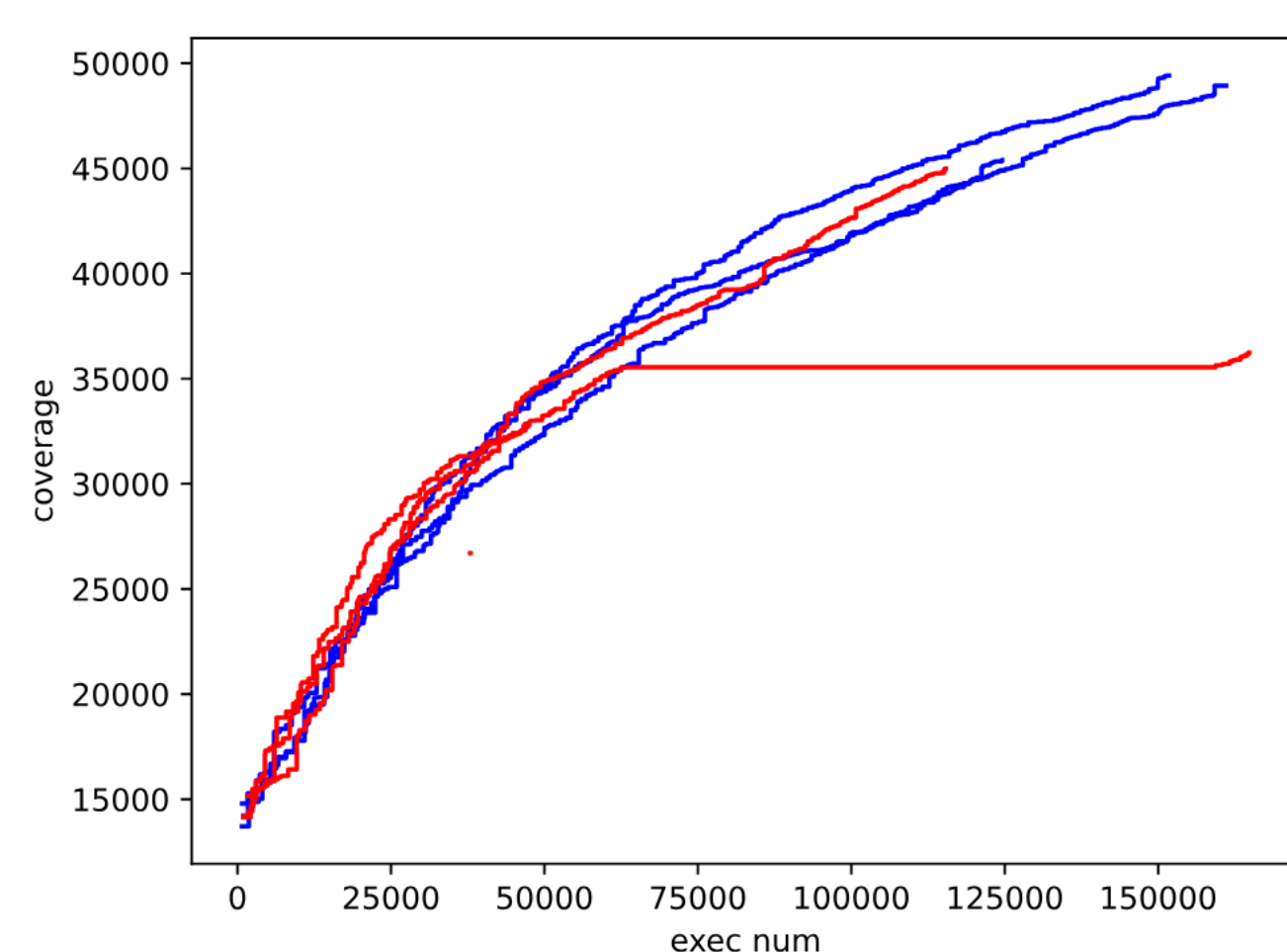


图1