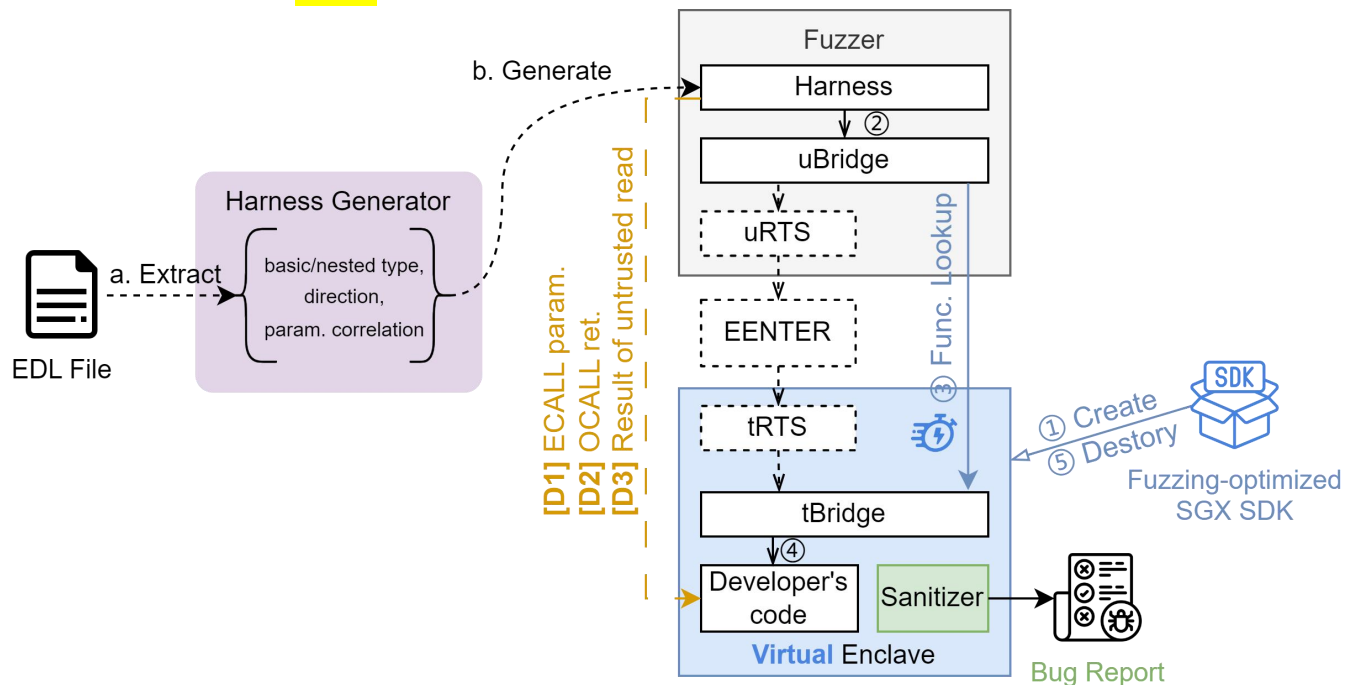


- 问题: Enclave基础输入检查影响测试有效性, 缺乏针对SGX威胁模型的漏洞检测方法, 繁重生命周期管理影响测试速度。
- Insight: 接口描述可助输入构建, 新威胁模型下TOCTOU等值得关注, 压缩非必要执行流程可加速测试。
 - 输入: 解析接口描述, 低开销扩展不可信内存维度; Sanitizer: 动静态结合检测潜在TOCTOU, 选择性修改不可信内存破坏一致性; 速度: 去除独立内存及上下文切换构建虚拟Enclave, 复用ShadowMap区分Enclave内外内存, 所挖漏洞硬件版可复现。



Enclave Name	Code Coverage ¹				Effectiveness		Input Validity		Bug Findings	
	Enclave Cov.		Interesting Cov.		SGXFuzz	EnclaveFuzz	SGXFuzz	EnclaveFuzz	SGXFuzz	EnclaveFuzz
intel-sgx-ssl	0.75%	18.04%	0.02%	18.39%	1.66%	99.66%	0%	100%	0	3
AE LE	3.85%	11.67%	14.29%	32.08%	1.98%	15.25%	26.89%	100%	0	0
AE PCE	4.10%	13.94%	22.53%	45.34%	3.49%	15.30%	17.48%	100%	0	0
AE PVE	2.36%	8.63%	10.05%	16.95%	6.32%	22.62%	33.15%	100%	0	0
AE QE	2.64%	3.20%	13.23%	6.68%	3.60%	16.13%	5.52%	100%	0	0
SGX_SQLite	2.30%	5.20%	1.45%	7.20%	26.64%	98.06%	20.20%	100%	0	3
TaLoS										96
mbdttls-SGX										4
wolfssl										0
sgx-wallet										10
sgx-dnet										2
plinius										2
sgxwallet										3
BiORAM-SGX	4.30%	17.95%	0.55%	1.08%	5.45%	1.66%	48.43%	82.95%	0	2
bolos-enclave	6.71%	7.85%	1.17%	0.48%	4.86%	4.01%	40.10%	84.09%	0	0
chsm	3.69%	16.91%	3.81%	15.00%	76.97%	81.60%	0%	91.79%	0	12
sgx-reencrypt	8.60%	33.31%	14.92%	31.26%	20.26%	28.26%	84.38%	100.00%	2	4
SGXCryptoPile	5.85%	17.62%	15.04%	80.56%	4.15%	5.88%	0%	100.00%	0	2
trusted-function-frame	2.53%	1.97%	2.13%	1.53%	75.64%	75.22%	0%	100.00%	0	3
wasn-micro-runtime	3.95%	1.67%	2.08%	0.94%	32.64%	46.04%	78.04%	100.00%	5	15
average	4.57%	16.53%	6.83%	23.54%	19.26%	49.21%	33.29%	97.94%	5.25	8.05

大幅提升输入有效性(3x)和覆盖率(4x)
共挖掘162个漏洞

	1M	20K	50M
BIORAM-SGX	96M	30M	505M
bolos-enclave	227K	163K	212K
cherry			
大幅提升测试速度(7x)			
wasn-micro-runtime	4M	1M	40M
Speedup rate	2.67x	1x	6.91x

大幅提升测试速度(7x)