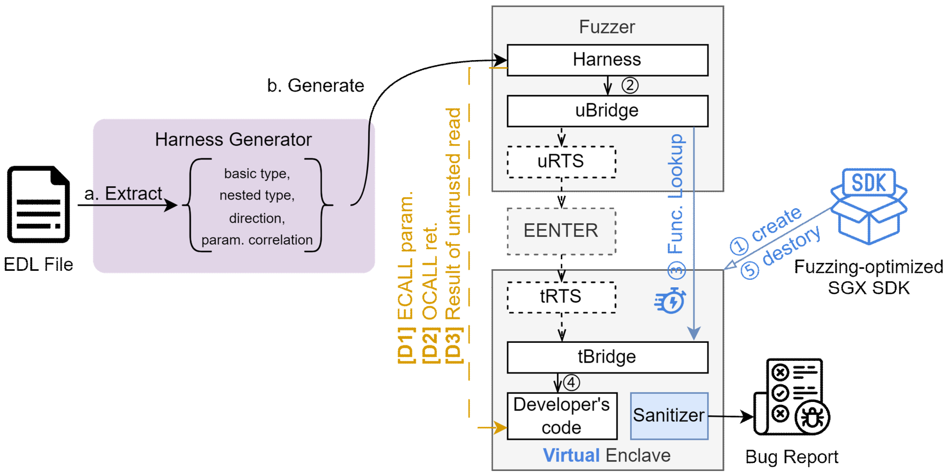
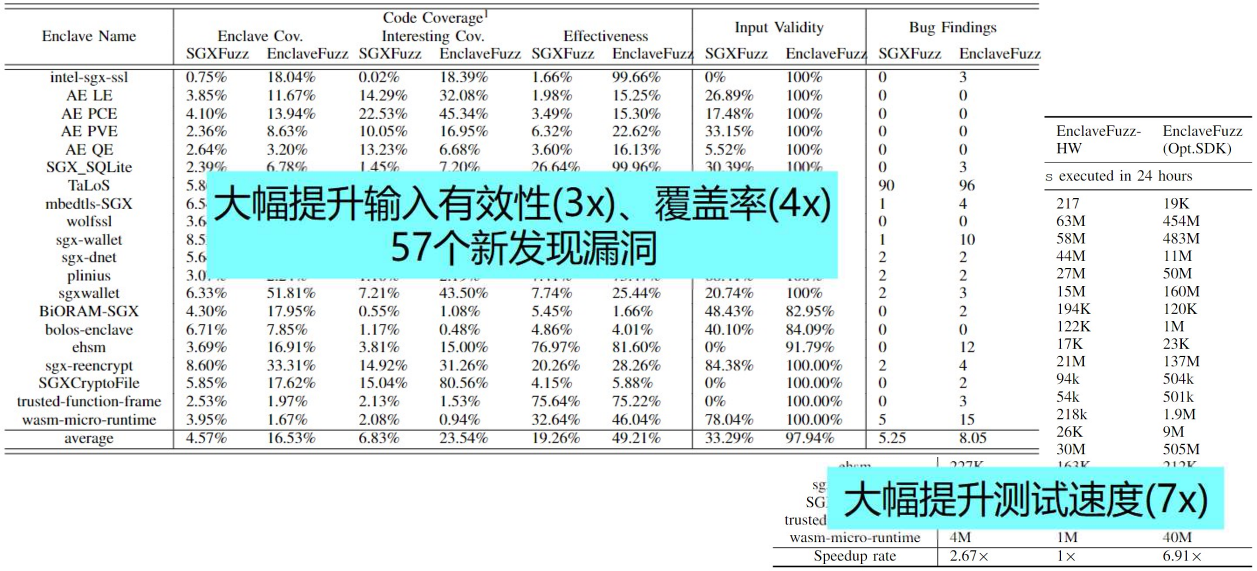
知识驱动：SGX模型

- **多维度结构化且高效的针对SGX应用的模糊测试框架: EnclaveFuzz**
  - ➢ 问题: Enclave固有的输入检查影响测试有效性，繁重的生命周期管理影响测试速度，此外缺乏漏洞检测策略适应SGX场景下威胁模型的转变。
  - ➢ insight：接口描述可助输入构建，压缩非必要执行流程可加速测试，新威胁模型下易发TOCTOU等值得关注。
    - 输入：解析接口描述，扩展不可信内存维度；速度：去除独立内存及上下文切换；Sanitizer：基础版上复用影子表并追踪Load指令以识别出利用不可信内存绕过检查的TOCTOU等。





Enclave Name	Code Coverage[1]						Input Validity		Bug Findings	
	Enclave Cov.		Interesting Cov.		Effectiveness					
	SGXFuzz	EnclaveFuzz	SGXFuzz	EnclaveFuzz	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	2.39%	6.78%	1.45%	7.20%	26.64%	99.96%	30.39%	100%	0	3
TaLoS	5.8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	90	96
mbedtls-SGX	6.5	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	4
wolfssl	3.6	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	0	0
sgx-wallet	8.5	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1	10
sgx-dnet	5.6	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	2	2
plinius	3.0	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	2	2
sgxwallet	6.33%	51.81%	7.21%	43.50%	7.74%	25.44%	20.74%	100%	2	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
ehsm	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
SGXCryptoFile	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
wasm-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)、覆盖率(4x)
57个新发现漏洞

		EnclaveFuzz-HW	EnclaveFuzz (Opt.SDK)
s executed in 24 hours			
		217	19K
		63M	454M
		58M	483M
		44M	11M
		27M	50M
		15M	160M
		194K	120K
		122K	1M
		17K	23K
		21M	137M
		94k	504k
		54k	501k
		218k	1.9M
		26K	9M
		30M	505M
ehsm	227K	163K	212K
sg	[illegible]	[illegible]	[illegible]
SG	[illegible]	[illegible]	[illegible]
trusted	[illegible]	[illegible]	[illegible]
wasm-micro-runtime	4M	1M	40M
Speedup rate	2.67×	1×	6.91×

大幅提升测试速度(7x)

“EnclaveFuzz: Finding Vulnerabilities in SGX Applications” *NDSS 2024*