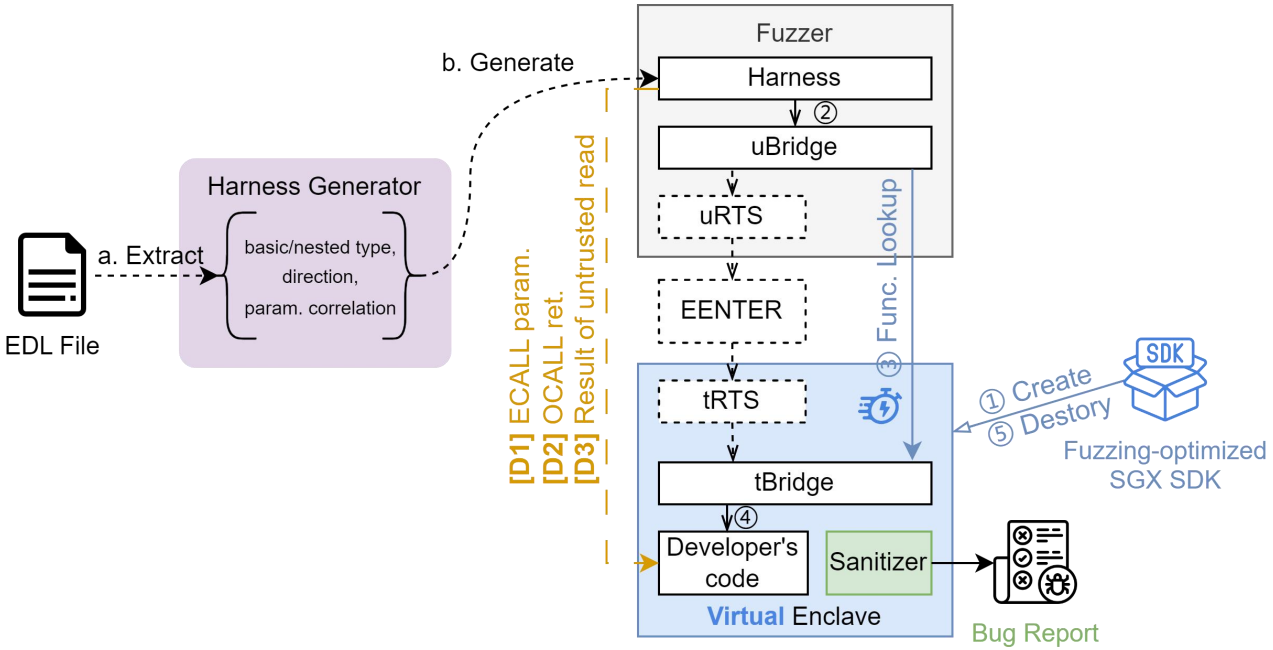
知识驱动：SGX模型

- **针对SGX应用的多维度结构化输入及威胁模型意识的模糊测试框架: EnclaveFuzz**
  - 问题: Enclave基础输入检查影响测试有效性，缺乏适应SGX威胁模型的漏洞检测方法，SGX隔离环境管理影响测试速度。
  - Insight：接口描述可助输入构建，漏洞检测对可信/不可信内存敏感，去SGX隔离环境下测试。
    - 输入：解析接口描述，发现潜在漏洞时测试不可信内存访问；Sanitizer：识别可信内存检测内存安全破坏，识别不可信内存以动静态结合检测TOCTOU；速度：去除SGX独立内存及上下文切换，复用ShadowMap区分Enclave可信内存，硬件复现所挖漏洞。



Enclave Name	Code Coverage[1] Enclave Cov. SGXFuzz	Enclave Cov. EnclaveFuzz	Interesting Cov. SGXFuzz	Interesting Cov. EnclaveFuzz	Effectiveness SGXFuzz	Effectiveness EnclaveFuzz	Input Validity SGXFuzz	Input Validity EnclaveFuzz	Bug Findings SGXFuzz	Bug Findings 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										3
TaLoS										96
mbedtls-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
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

共挖掘162个漏洞
大幅提升输入有效性(3x)和覆盖率(4x)

bolos-enclave	96M	30M	505M
wasm-micro-runtime	4M	1M	40M
Speedup rate	2.67×	1×	6.91×

大幅提升测试速度(7x)