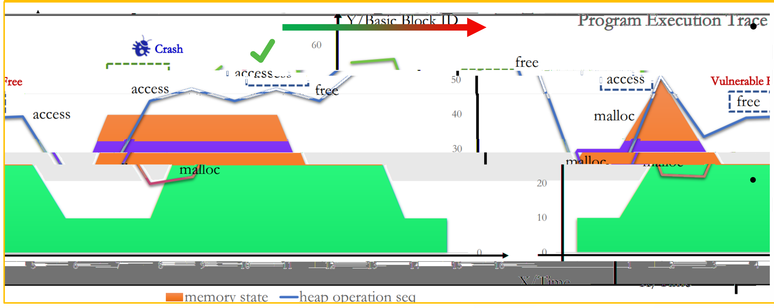
HTFuzz: Heap Operation Sequence Sensitive Fuzzing

ASE 2022 CCF-A

Yuanping Yu*, Xiangkun Jia*, Yuwei Liu, Yanhao Wang, Qian Sang,
Chao Zhang and Purui Su (✉ xiangkun@iscas.ac.cn)

https://github.com/TCA-ISCAS/HTFuzz.git



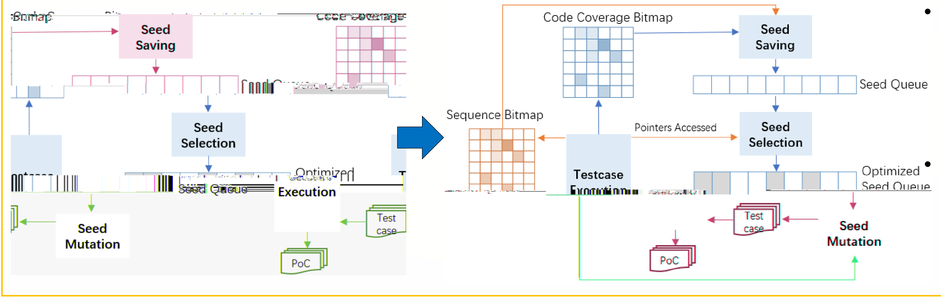
Double-Free
Dereference

Use-After-free,
Null Pointer

/ /

Coverage

Feedback
AFL

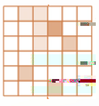


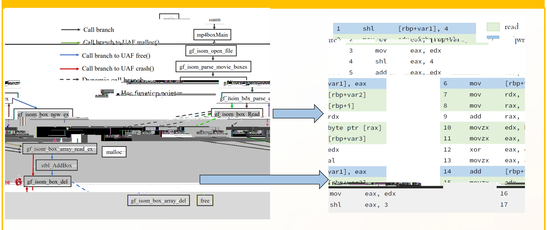
…-> malloc (Size) -> malloc (Size)-> access (Ptr, Size) -> free (Ptr) -> free (Ptr) -> access (Ptr, Size) -> malloc (Size) -> access (Ptr, Size) -> access (Ptr, Size) -> free (Ptr) ->…

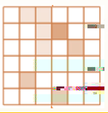
1, 1, *access*, 0, 0, *access*, 1, *access*, *access*, 0

[0, 1, 1] [1, 0, 0] [0, 0, 1] [0, 0, 1]

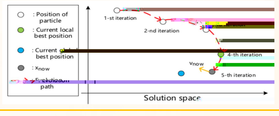
[3] [4] [1] [1]



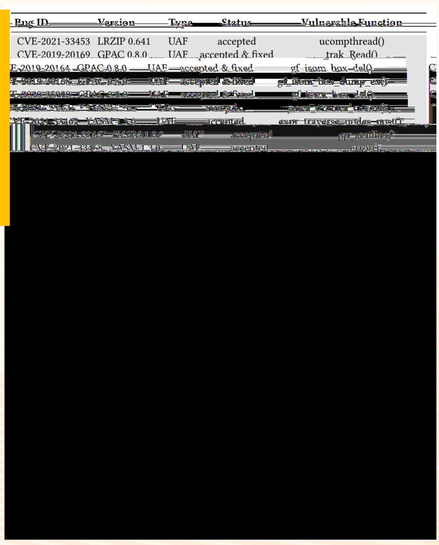




Effector map



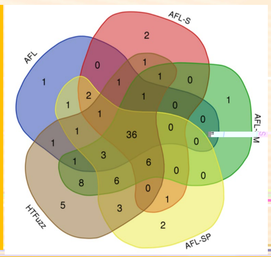
: Optimize Mutation Scheduling for Fuzzers



	HTFuzz	AFL	Memlock	AFL-sen-ma	AFL-sen-mw
0day	37-**32**-0	24-22-0	9-7-0	9-9-0	9-9-0
0day-non-CVE	-	3-0-0	3-0-0	-	-
1day	55-**42**-0	37-26-4	29-20-2	16-12-0	11-9-0
Sum	92-**74**-0	64-48-4	41-27-2	25-21-0	20-18-0

	PathAFL	Tofuzz	MOPT	Angora	Ankou
0day	21-18-0	20-18-0	21-19-0	8-8-0	26-22-0
0day-non-CVE	2-0-0	1-0-0	-	3-2-2	6-1-1
1day	28-23-4	30-20-2	46-32-1	27-25-10	49-36-2
Sum	51-41-4	51-38-2	67-51-1	42-37-14	81-59-3

X-Y-Z, X , Y ,Z HTFuzz



AFL baseline AFL-S Seq Bitmap AFL-SP AFL-S

AFL-SM AFL-S MOPT HTFuzz