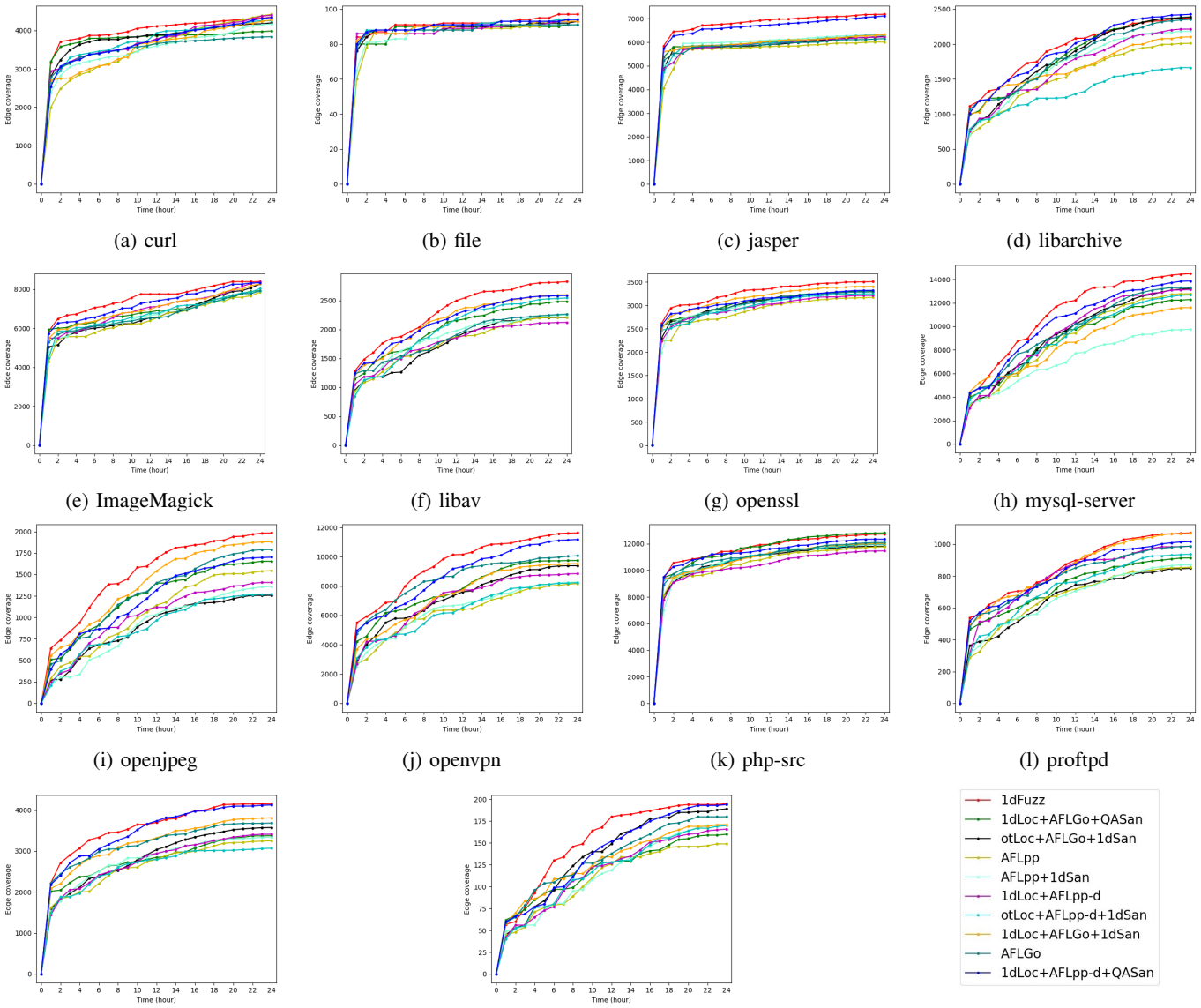
1dFuzz: External Tables and Figures



(a) curl (b) file (c) jasper (d) libarchive

(e) ImageMagick (f) libav (g) openssl (h) mysql-server

(i) openjpeg (j) openvpn (k) php-src (l) proftpd

(m) qpdf (n) zlib

Fig. 1: Edge coverage for different fuzzing schemes on the rest 14 projects in 24h in three trials.

TABLE I: Fuzzing results of the `1dLoc` Group, where we compare `1dLoc` with another patch locator.

Group	Solution				Patch	Target	Crash						Average
	ID	Locator	Fuzzer	Sanitizer	Distance	Number	Total	ratio	iB+TCS	ratio	iB+nTCS	nB	Time
1dLoc	4	/	AFLpp	1dSan	c	242	**36**	0.38	**34**	0.40	0	2	**6h12m**
	5	otLoc	AFLpp-d	1dSan	c	242	67	0.71	61	0.73	5	1	4h49m
	6	1dLoc	AFLGo	1dSan	c	242	44	0.46	39	0.46	3	2	5h22m
	7	otLoc	AFLGo	1dSan	c	242	39	0.41	35	0.42	3	1	5h48m
	3	**1dLoc**	**AFLpp-d**	**1dSan**	**c**	**242**	**95**	**1.00**	**84**	**1.00**	**7**	**4**	**4h27m**
Best Improvement							2.64x		2.47x				1.39x

Patch distance *c*: there is only one commit gap between the pre-patch and post-patch binaries. *iB*: crash hits target patch in benchmark. *nB*: newly found crash not in benchmark. *TCS*: crash conforms to the TCS feature. *nTCS*: otherwise. Average Time: average time to first generated PoC.

TABLE II: Fuzzing results of the `1dSan` Group, where we compare `1dSan` with another sanitizer.

Group	Solution				Patch	Target	Vulnerabilities						Average
	ID	Locator	Fuzzer	Sanitizer	Distance	Number	Total	ratio	iB+TCS	ratio	iB+nTCS	nB	Time
1dSan	8	1dLoc	AFLpp-d	/	c	242	69	0.73	63	0.75	6	3	5h17m
	9	1dLoc	AFLpp-d	QASan	c	242	72	0.76	60	0.71	7	5	5h51m
	6	1dLoc	AFLGo	1dSan	c	242	44	0.46	39	0.46	3	2	5h22m
	10	1dLoc	AFLGo	QASan	c	242	**38**	0.40	**31**	0.37	5	2	**6h09m**
	3	**1dLoc**	**AFLpp-d**	**1dSan**	**c**	**242**	**95**	**1.00**	**84**	**1.00**	**7**	**4**	**4h27m**
Best Improvement							2.50x		2.71x				1.38x

Patch distance *c*: there is only one commit gap between the pre-patch and post-patch binaries. *iB*: crash hits target patch in benchmark. *nB*: newly found crash not in benchmark. *TCS*: crash conforms to the TCS feature. *nTCS*: otherwise. Average Time: average time to first generated PoC.

TABLE III: Fuzzing results of the `distance` Group, where we change the distance between pre- and post-patch binaries.

Group	Solution				Patch	Target	Crash						Average
	ID	Locator	Fuzzer	Sanitizer	Distance	Number	Total	ratio	iB+TCS	ratio	iB+nTCS	nB	Time
distance	11	1dLoc	AFLpp-d	1dSan	m	242	**48**	0.51	**40**	0.48	4	4	**7h33m**
	3	**1dLoc**	**AFLpp-d**	**1dSan**	**c**	**242**	**95**	**1.00**	**84**	**1.00**	**7**	**4**	**4h27m**
Best Improvement							1.98x		2.10x				1.70x

Patch distance *c*: only one commit gap between the pre- and post- patch binaries, *m*: one minor version gap. *iB*: crash hits patch in benchmark. *nB*: newly found crash not in benchmark. *TCS*: crash conforms to the TCS feature. *nTCS*: otherwise. Average Time: average time to first generated PoC.