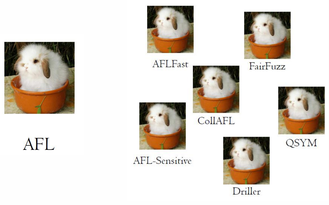
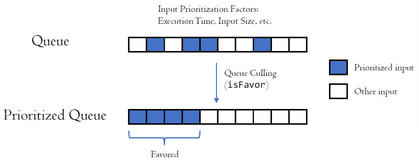
Not All Coverage Measurements Are Equal
Fuzzing by Coverage Accounting for Input Prioritization
（基于覆盖率审计的模糊测试优化，NDSS 2020）

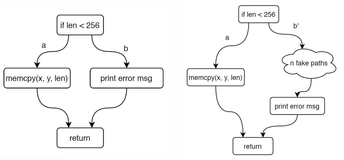
YanhaoWang, Xiangkun Jia, Yuwei Liu, Kyle Zeng,
Tiffany Bao, DinghaoWu, and Purui Su* (ISCAS, PSU, ASU)
作者联系方式：xiangkun@iscas.ac.cn，purui@iscas.ac.cn
开源工具地址：https://github.com/TortoiseFuzz/TortoiseFuzz



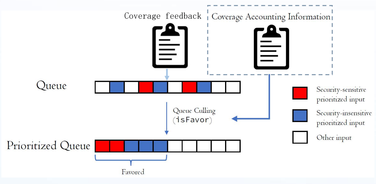
近些年基于AFL （American Fuzzy Lop，美国垂耳兔）形成了一系列的改进工具。



AFL**增加了覆盖率反馈**，通过维护了一个测试用例队列保留能够引起路径变化的测试用例，并对其中更有潜力的测试用例赋予高优先级。



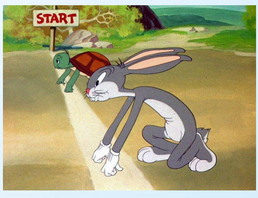
代码覆盖率反馈并不是完美的。比如AFL并不区分左图更具危险性的a分支；也会陷入右图b'的伪造分支中。可见，**对于不同路径应该进行区分并倾向于危险性更高的路径。**



我们增加了覆盖率审计信息，包括危险函数信息（函数级）、复杂代码结构信息（基本块级）和敏感指令信息（指令级），用于挑选更有潜力的测试用例。

Program	Version	ID	Vulnerability Type	New
exiv2	0.26	CVE-2018-16336	heap-buffer-overflow	✓
		CVE-2018-17229	heap-buffer-overflow	✓
		CVE-2018-17230	heap-buffer-overflow	✓
		issue_400	heap-buffer-overflow	✓
		issue_460	stack-buffer-overflow	-
		CVE-2017-11336	heap-buffer-overflow	-
		CVE-2017-11337	invalid free	-
		CVE-2017-11339	heap-buffer-overflow	-
		CVE-2017-14857	invalid free	-
		CVE-2017-14858	heap-buffer-overflow	-
		CVE-2017-14861	stack-buffer-overflow	-
		CVE-2017-14865	heap-buffer-overflow	-
		CVE-2017-14866	heap-buffer-overflow	-
		CVE-2017-17669	heap-buffer-overflow	-
		issue_170	heap-buffer-overflow	-
		CVE-2018-10999	heap-buffer-overflow	-
new_exiv2	0.26	CVE-2018-17229	heap-buffer-overflow	✓
		CVE-2018-17230	heap-buffer-overflow	✓
		CVE-2017-14865	heap-buffer-overflow	-
		CVE-2017-14866	heap-buffer-overflow	-
		CVE-2017-14858	heap-buffer-overflow	-
exiv2_9_17	0.26	CVE-2018-17282	null pointer dereference	✓
nasm	2.14rc4	CVE-2018-8882	stack-buffer-under-read	-
		CVE-2018-8883	stack-buffer-over-read	-
		CVE-2018-16517	null pointer dereference	-
		CVE-2018-19209	null pointer dereference	-
		CVE-2018-19213	memory leaks	-
gpac	0.7.1	CVE-2019-20165	null pointer dereference	✓
		CVE-2019-20169	heap-use-after-free	✓
		CVE-2018-21017	memory leaks	✓
		CVE-2018-21015	Segment Fault	✓
		CVE-2018-21016	heap-buffer-overflow	✓
		issue_1340	heap-use-after-free	-
		issue_1264	heap-buffer-overflow	-
		CVE-2018-13005	heap-buffer-over-read	-
		issue_1077	heap-use-after-free	-
		issue_1090	double-free	-
libtiff	4.0.9	CVE-2018-15209	heap-buffer-overflow	✓
		CVE-2018-16335	heap-buffer-over-read	✓
liblouis	3.7.0	CVE-2018-11440	stack-buffer-overflow	-
		issue_315	memory leaks	-
ngiflib	0.4	issue_10	stack-buffer-overflow	✓
		CVE-2019-16346	heap-buffer-overflow	✓
		CVE-2019-16347	heap-buffer-overflow	✓
		CVE-2018-11575	stack-buffer-overflow	-
		CVE-2018-11576	heap-buffer-over-read	-
libming	0_4_8	CVE-2018-13066 (2 similar crashes)	memory leaks	-
catdoc	0_95	crash	memory leaks	-
		crash	Segment Fault	-
		CVE-2017-11110	heap-buffer-underflow	-
tcpreplay	4.3	CVE-2018-20552	heap-buffer-overflow	✓
		CVE-2018-20553	heap-buffer-overflow	✓
flvmeta	1.2.1	issue_13	null pointer dereference	✓
		issue_12	heap-buffer-overflow	-

我们的工具命名为**TortoiseFuzz**，取自“龟兔赛跑”的故事，希望我们的“乌龟”能够跑赢这些“美国垂耳兔”。



我们共发现了**20个0day漏洞**（如左图）。在30款真实程序组成的测试集上和6款最近的模糊测试工具进行了对比。结果显示，我们的工具在**漏洞挖掘数量方面**（下方左图）、**内存消耗方面**（下方中图）**和Anti-Fuzzing技术对抗方面**（下方右图）**具有明显优势。**