



200-ЛЕТИЮ СО ДНЯ РОЖДЕНИЯ А.Ф.МОЖАЙСКОГО
И 70-ЛЕТИЮ СО ДНЯ ПРИСВОЕНИЯ АКАДЕМИИ ЕГО ИМЕНИ
ПОСВЯЩАЕТСЯ

ДЕНЬ ИННОВАЦИЙ

МЕТОДИКА ДИНАМИЧЕСКОГО АНАЛИЗА ИСПОЛНЯЕМЫХ ФАЙЛОВ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ



process timing	overall results
run time : 2 days, 16 hrs, 19 min, 19 sec	cycles done : 130
last new find : 0 days, 0 hrs, 0 min, 34 sec	corpus count : 7111
last saved crash : none seen yet	saved crashes : 0
last saved hang : none seen yet	saved hangs : 5
cycle progress	map coverage
now processing : 3825.0 (53.8%)	map density : 2.01% / 15.24%
runs timed out : 0 (0.00%)	count coverage : 5.34 bits/tuple
stage progress	findings in depth
now trying : trim 8/8	favorable items : 1345 (18.91%)
stage execs : 25/229 (10.92%)	new edges on : 1818 (25.57%)
total execs : 105M	total crashes : 0 (0 saved)
exec speed : 151.1/sec	total touts : 26 (0 saved)
fuzzing strategy yields	item geometry
bit flips : 0/478k, 0/478k, 0/478k	levels : 10
byte flips : 0/59.9k, 0/59.9k, 0/59.9k	pending : 6759
arithmetics : 0/4.19M, 0/8.38M, 0/8.38M	pend fav : 1031
known ints : 0/538k, 0/2.27M, 0/3.35M	own finds : 499
dictionary : 0/0, 0/0, 0/0, 0/0	imported : 890
havoc/splice : 28/94.4k, 0/0	stability : 91.16%
py/custom/rq : unused, unused, unused, unused	
trim/eff : 0.04%/204k, 100.00%	[cpu000: 37%]
strategy: explore	state: in progress

КРАТКОЕ ОПИСАНИЕ:

Назначение: проект направлен на решение актуальной научно-технической (практической) задачи, заключающееся в разработке системы динамического анализа исполняемых файлов с помощью методов машинного обучения, обеспечивающей повышение эффективности выявления ошибок в исполняемых файлах.

ОСНОВНЫЕ ТТХ:

Основные тактико-технические характеристики: Созданный в рамках реализации проекта экспериментальный образец основан на 6 моделях, реализованных с применением машинного обучения

для генерации входных данных тестируемого программного обеспечения:

1. Модель LSTM_PLUGIN;
2. Модель GRU_PLUGIN;
3. Модель DQN_PLUGIN;
4. Модель CUSTOM_PLUGIN;
5. Модель SIMPLE_CHUNK_REPLACE;
6. Модель SOFTMAX_BANDIT_PLUGIN.

ОТЛИЧИТЕЛЬНЫЕ СПОСОБНОСТИ (НОВИЗНА):

Экспериментальный образец в сравнении с существующими аналогами выгодно отличается тем, что формирование входных тестовых данных для тестирования программного обеспечения основывается не на классическом полном переборе или шаблонном подходе, а на основе методов машинного обучения.

АВТОРСКИЙ КОЛЛЕКТИВ:

Бирюков Денис Николаевич, Руссу Валерий Юрьевич,
Яроцкий Глеб Дмитриевич

