FuzzBench Fork for Triereme Evaluation

September 9, 2024

Revision: v3.fuzzbench.marine
Name of node : nodefuzz
Paper : Triereme: Speeding up hybrid fuzzing through efficient query scheduling

- Log into Sphere portal
- Create a new experiment
- Create a new xdc
- In the model editor type :

```
from mergexp import *

# Create a network topology object. This network will automatically
# add IP addresses to all node interfaces and configure static routes
# between all experiment nodes.
net = Network('fuzzbench', addressing==ipv4, routing==static)

# Creating the node.
n=net.node("nodefuzz",proc.cores>=64, image=="2004", memory.capacity>=gb(64))

# Making the experiment runnable.
experiment(net)
```

- Compile code
- Push code
- Make reservation
- Activate
- Attach on xdc
- Go on Jupyter interface (see xdc)

On Jupyter, open terminal and do :

```
#log in merge
mrg login
#connect to xdc
su - marine
#ssh to node
ssh nodefuzz
```

```
#install git
sudo apt-get update
sudo apt install git
#clone git
git clone https://github.com/vusec/fuzzbench-triereme.git
```

Preparation

```
sudo apt-get update
sudo apt-get install software-properties-common

#Install Docker
sudo apt update
sudo apt install apt-transport-https ca-certificates curl software-properties-common
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update
sudo apt install docker-ce docker-ce-cli containerd.io
#Permission for user
sudo usermod -aG docker $USER
#here :
sudo usermod -aG docker marine
logout #to take effect
login


#Install Make
sudo apt-get install build-essential

#Install Python3.10
sudo add-apt-repository ppa:deadsnakes/ppa
sudo apt install python3.10 python3.10-dev python3.10-venv libpq-dev
#Configure Python 3.10 by default :
sudo update-alternatives --install /usr/bin/python3 python3 /usr/bin/python3.10 1

```

```
#Install pip

wget https://bootstrap.pypa.io/get-pip.py
python3.10 get-pip.py

#Make sure you have acess to everything
nano ~/.bashrc
#add this line at the end
export PATH=$PATH:/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/marine/.local/bin
#apply change
source ~/.bashrc

#Install requirements
cd fuzzbench-triereme
chmod +x requirements.txt
python3.10 -m pip install -r requirements.txt


#You can verify that your local setup is working correctly by running the presubmit checks.
make presubmit
#Couldn't solve other error
```

Running experiment

Config file :

```
  GNU nano 4.8                  config_file
# The number of trials of a fuzzer-benchmark pair.
trials: 2

# The amount of time in seconds that each trial is run for.
# 23 hours = 23 * 60 * 60 = 82800
max_total_time: 60

# The location of the docker registry.
# FIXME: Support custom docker registry.
# See https://github.com/google/fuzzbench/issues/777
docker_registry: gcr.io/fuzzbench

# The local experiment folder that will store most of the experiment data.
# Please use an absolute path.
experiment_filestore: /home/marine/fuzzbench-triereme/experiment-data

# The local report folder where HTML reports and summary data will be stored.
# Please use an absolute path.
```

```
report_filestore: /home/marine/fuzzbench-triereme/report-data

# Flag that indicates this is a local experiment.
local_experiment: true
```

```
config_file=./config_file

export test="test-1"
#benchmarks used in paper
code_coverage_benchmarks=(curl_curl_fuzzer_http
   freetype2_ftfuzzer harfbuzz_hb-shape-fuzzer libjpeg
   -turbo_libjpeg_turbo_fuzzer
   libpng_libpng_read_fuzzer libxml2_xml
   mbedtls_fuzz_dtlsclient  openssl_x509 openthread_ot
   -ip6-send-fuzzer  proj4_proj_crs_to_crs_fuzzer
   vorbis_decode_fuzzer woff2_convert_woff2ttf_fuzzer
   zlib_zlib_uncompress_fuzzer)


PYTHONPATH=. python3.10 experiment/run_experiment.py
    -c $config_file   -e $test   --concurrent-builds 2
      --runners-cpus 32   --measurers-cpus 32   --
   fuzzers       aflplusplus_cmplog_forkmode
   symcc_libafl_single       triereme_linear_single
       triereme_trie_single   --benchmarks "${
   code_coverage_benchmarks[1]}"
```

Couldn't solve all remaining errors and couldn't run script. Maybe I forgot to put some of the commands I ran since i tried lots of things.