Honggfuzz

List

Honggfuzz

- **Honggfuzz는 google에서 관리하는 프로젝트입니다.**
- **Honggfuzz는 멀티 스레드와 멀티 프로세스를 사용합니다.**
  - 그렇기 때문에 fuzzer를 여러 개 복사할 필요가 없습니다.
  - Honggfuzz는 사용 가능한 모든 CPU 코어 이용할 수 있습니다.
  - Honggfuzz는 스레드 간에 Corpus 파일을 공유 합니다.
- **Honggfuzz는 OpenSSL에서 중요한 취약성을 발견하였습니다.**
  - Fix Use After Free for large message sizes (CVE-2016-6309)
- **Honggfuzz는 낮은 수준의 인터페이스를 사용하여 프로세스를 모니터링 합니다.**
  - 이로 인해 Honggfuzz는 다른 fuzzer들과 달리 숨겨진 신호를 발견하고 보고 합니다.
- **Honggfuzz는 간단한 Corpus를 전달하고, 피드백 기반의 커버리지 메트릭스를 활용하여 확장하는 방식으로 동작합니다.**
- **Honggfuzz는 하드웨어 기반, 소프트웨어 기반의 다른 퍼저의 구동을 지원합니다.**
  - software-based: libfuzzer, afl
  - hardware-based: branch/instruction counting, Intel BTS, Intel PT
  - Feedback-driven fuzzing
- Honggfuzz는 "liubfuzz/PULIBROOzza.a"를 사용하여 지속적인 퍼지 모드를 지원합니다.
- **Honggfuzz는 원격 / 독립 실행형 프로세스를 오랜 시간동안 원할하게 fuzz 할 수 있습니다.**
  - Can fuzz remote/standalone long-lasting processes
- **Honggfuzz는 다음과 같은 환경에서 동작합니다.**

OS	Status	Notes
GNU/Linux	Works	ptrace() API (x86, x86-64 disassembly support)
FreeBSD	Works	POSIX signal interface
Mac OS X	Works	POSIX signal interface/Mac OS X crash reports (x86-64/x86 disassembly support)
Android	Works	ptrace() API (x86, x86-64 disassembly support)
MS Windows	Works	POSIX signal interface via CygWin
Other Unices	Depends*	POSIX signal interface

Install

Build honggfuzz

```
$ sudo apt-get update
$ sudo apt-get install clang-5.0
$ sudo apt-get install binutils-dev
$ sudo apt-get install libunwind8-dev or libunwind-dev
$ git clone https://github.com/google/honggfuzz.git
$ cd honggfuzz
$ make
$ ./honggfuzz
```

Usage

command

```
$./honggfuzz [options] -- path_to_command [args]
```

Usage

- https://github.com/google/honggfuzz/blob/master/docs/USAGE.md

Example(Fuzzing OpenSSL)

- honggfuzz에서 제공하는 example을 이용해 설명하며, 대상은 OpenSSL 입니다.
  - 해당 예제에서는 libFuzzer도 이용하고 있기 때문에 libFuzzer의 설치도 필요합니다.

Command

```
$ cd honggfuzz/example/openssl/
```

- 우선 아래 2파일에서 Honggfuzz 가 설치된 경로를 재설정이 필요합니다.

compile_hfuzz_openssl_master.sh

```
export CC="honggfuzz path"/hfuzz_cc/hfuzz-clang
```

make.sh

```
HFUZZ_SRC = "honggfuzz path"
```

- 다음과 같이 open-ssl 소스를 다운받아 빌드합니다.

Build open-ssl(ASAN, libFuzzer,)

```
$ git clone --depth=1 https://github.com/openssl/openssl.git
$ mv openssl openssl-master
$ cd openssl-master/
$ ./config
$ ~/Fuzz/honggfuzz/examples/openssl/compile_hfuzz_openssl_master.sh
```

- 다음과 같이 honggfuzz에서 제공되는 corpus를 이용해 fuzz을 진행합니다.

Run honggfuzz

```
lazenca0x0@ubuntu:~/Fuzz/honggfuzz/examples/openssl$ ~/Fuzz/honggfuzz/honggfuzz -f corpus_server/ -P -- ./stdin.
openssl-master.address.server

PID: 6978, inputDir 'corpus_server/', nullifyStdio: true, fuzzStdin: false, saveUnique: true, mutationsPerRun:
6, externalCommand: 'NULL', runEndTime: 0 tmOut: 10, mutationsMax: 0, threads.threadsMax: 1, fileExtn: 'fuzz',
ASLimit: 0x0(MiB), RSSLimit: 0x0, DATALimit: 0x0, fuzzExe: './stdin.openssl-master.address.server', fuzzedPid:
0, monitorSIGABRT: 'true'

[2017-12-04T19:41:58-0800][W][6978] files_readFileToBufMax():50 Couldn't open '/sys/bus/event_source/devices
/intel_pt/type' for R/O: No such file or directory

[2017-12-04T19:41:58-0800][W][6978] files_readFileToBufMax():50 Couldn't open '/sys/bus/event_source/devices
/intel_bts/type' for R/O: No such file or directory
Entering phase 1/2: Dry Run

--------------------------- [ HONGGFUZZ / v1.2 ] -----------------------------
  Iterations : 23687 [23.69k]
       Phase : Dynamic Main (2/2)
    Run Time : 0 hrs 8 min 22 sec
   Input Dir : [1606] 'corpus_server/'
  Fuzzed Cmd : './stdin.openssl-master.address.server'
     Threads : 1, CPUs: 1, CPU%: 100% (100%/CPU)
       Speed : 35/sec (avg: 47)
     Crashes : 0 (unique: 0, blacklist: 0, verified: 0)
    Timeouts : 0 [10 sec.]
 Corpus Size : 1, max file size: 131072
    Coverage : edge: 4801 pc: 107 cmp: 58613
--------------------------------- [ LOGS ] ----------------------------------
Persistent mode: Launched new persistent PID: 30653
[2017-12-04T19:50:19-0800][W][6979] arch_checkWait():314 Persistent mode: PID 30653 exited with status: EXITED,
exit code: 0
Persistent mode: Launched new persistent PID: 30654
[2017-12-04T19:50:19-0800][W][6979] arch_checkWait():314 Persistent mode: PID 30654 exited with status: EXITED,
exit code: 0
Persistent mode: Launched new persistent PID: 30655
```

- **honggfuzz에서는** openssl **이외에도 다양한 예제들을 제공하고 있습니다.**

Example

- https://github.com/google/honggfuzz/tree/master/examples

Related site

- http://honggfuzz.com/
- https://github.com/google/honggfuzz